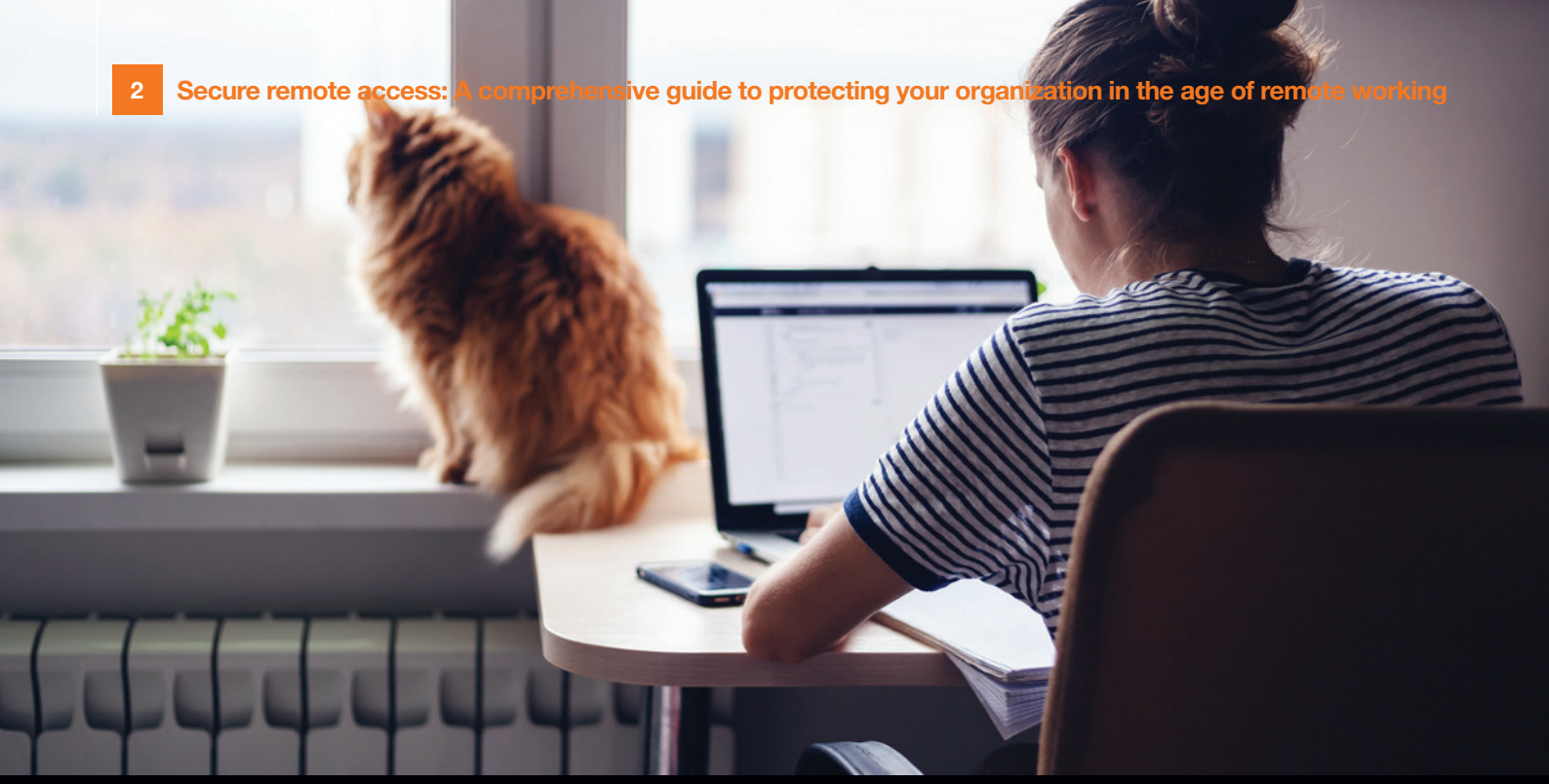
Orange
Cyberdefense

Securing your remote workers

A comprehensive guide to protecting your organization in the age of remote working



Introduction

Almost overnight, the COVID-19 pandemic and resultant global lockdowns have made remote work the new norm for many businesses. IT managers and network administrators scrambled to introduce new architectures or roll out new capabilities to adapt to the violent new reality of an entire workforce suddenly requiring remote access to enterprise systems. By all accounts, the IT sector handled it all very well.

There's probably no going back, however. As subsequent waves of infection crisscross the globe, travel restrictions remain in place, and families adapt to the idea of a "home office', there is every chance that remote work will continue on a significant scale for the foreseeable future.

Statistics show that virtual work or remote work is something that businesses have accepted and some fully embraced[1]. According to an Owl Labs study, some workers have indicated that they will prefer jobs that offer remote work over jobs that do not[2].

Contents

Long-term growth

An Ipsos poll of early 2012 showed that telecommuting or telework was a growing trend back then[3]. Some business leaders disagreed with that view. In 2013 Yahoo decided to cancel telecommuting to improve company productivity in support of a struggling business[4]. The perceived benefit of being in physical proximity and managing staff in person were prioritized over the agility and flexibility of allowing employees to work remotely.

Contrary to that, other business leaders saw telecommuting as a perk to lure talent away from the competition[5]. A poll conducted by Gallup in 2017 showed that American companies that encouraged telecommuting had better chances of retaining staff or hiring new staff[6]. A flexible work schedule and allowing staff to manage their work hours can lead to improved productivity, but this all depends on the type of work involved.

New management skills are needed in the post-COVID era to ensure that employees meet timelines and that productivity is measured transparently[7]. A Harvard Business Review (HBR) article claims that businesses that manage scarce time, talent, and energy are 40% more productive than other businesses[8]. The same HBR article observes that companies collaborating effectively before COVID-19 have remained productive during the disruptions. The same companies are estimated to have increased productivity by as much as 5% during these times. The HBR article also states that the inverse is true for companies that struggled with collaboration before the lockdowns and stay-at-home instructions.

The mass "Work From Anywhere" (WFA) movement of early 2020 was made possible with much better communication infrastructure backed by the growth of cloud-hosted solutions[9]. Cloud-based Office productivity solutions such as Microsoft's Office365 and Google's Workspace (formerly G-Suite) made the shift to a more extensive remote work possible[10], [11]. The COVID-19 pandemic played an instrumental role in forcing digital transformation onto business leaders[12].

A challenge in the early part of the 2020 lockdown was implementing or scaling the equipment that enabled remote work[13]. This scramble to work remotely and get it done as soon as possible could have resulted in some technical and security shortcuts[14]. There are plenty of risks, as highlighted by the Telework guide published by CISA[15].

Focus on security

Having dealt with the urgent requirement to facilitate remote work, therefore, the time has now come to (re)consider the security implications of this new reality and take account of any compromises we may have had to make to simply "stay online"[16].

We have written this solution paper to address these vital security issues. It will primarily focus on the intractable fact that the user's connectivity to the internet, and therefore to our business networks, is facilitated by their home internet router. However, this essential component of the enterprise connectivity stack is not under our direct control and therefore needs to be considered "untrusted" at best or "malicious" at worst.

How do we ensure the security of the remote workforce in the light of insecure home network routers? And what role do secure remote access or virtual private network (VPN) technologies play in mitigating potential threats that may arise because our users are connected from home?

At a time when more people are connecting and working remotely from free or home Wi-Fi networks than at any time before, it is essential that the primary technology we use to facilitate this securely – typically enterprise secure remote access products – should offer security how and when we expect. We believe this calls for a review by businesses and their vendors of the contemporary threat model for remote workers and the appropriate application of security technologies as a part of the response to these threats.

"A Harvard Business Review (HBR) article claims that businesses that manage scarce time, talent, and energy are 40% more productive than other businesses[8]."

The paper is presented in support of Orange Cyberdefense's work in preparation for talks given at Black Hat USA 2020 and RSA Conference 2021.

In the Black Hat talk, we examined the weakness of secure remote access technologies when presented with a captive portal scenario. The RSA Conference talk followed a similar vein. We evaluated the risks presented by compromised home routers and how an attacker could use what we learned from the Black Hat talk to launch attacks against devices in a compromised home router setting. We demonstrated that patient attackers could compromise secure remote access technologies using novel and known techniques.

This paper aims to outline a holistic strategy complemented by a comprehensive set of technical controls. It can be used to achieve an appropriate level of security for home users in the face of a diverse group of old and new threats.

On solutions

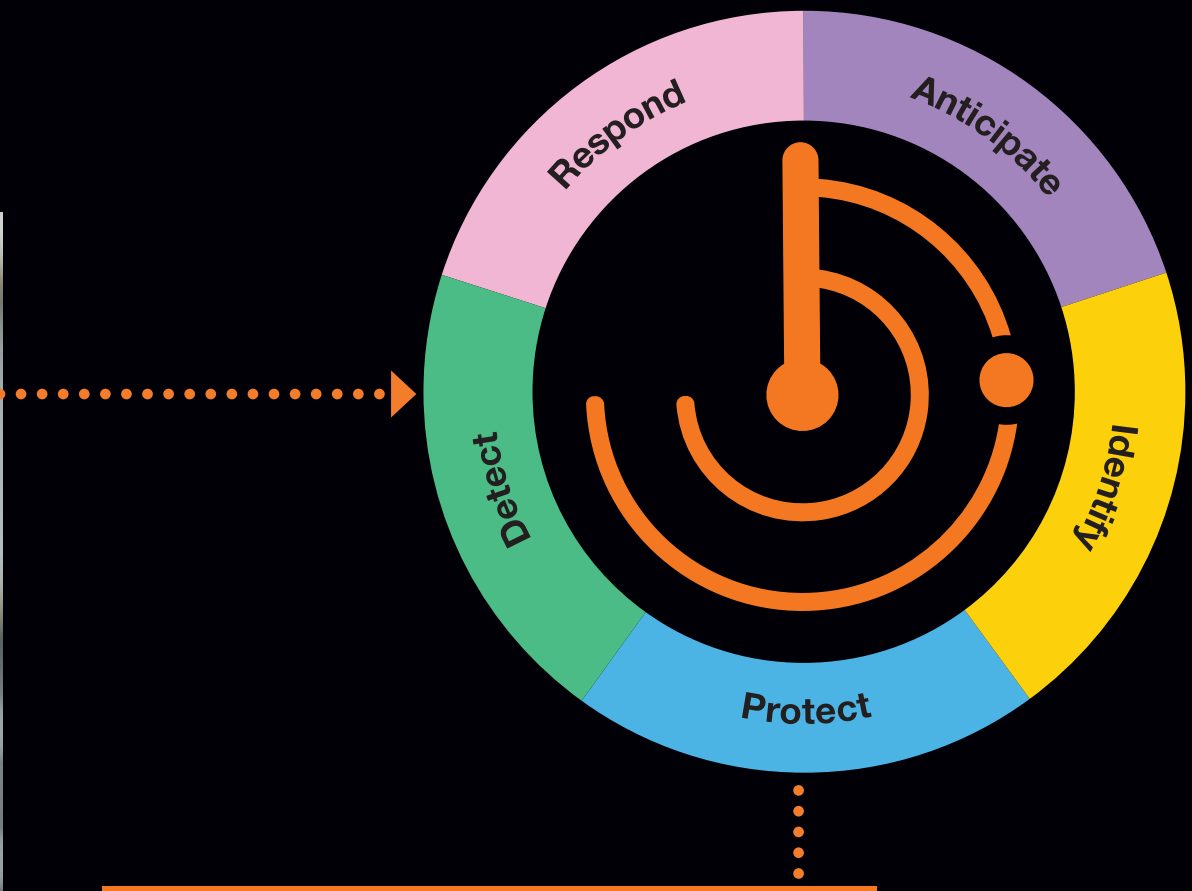
We all know there is no one-size-fits-all solution. We aim to provide general guidance to initiate an internal process that will help IT administrators and security staff find solutions that best fit each respective organization's needs and unique situation.

The threat model for staff working from home may be different from the traditional mobile workers' threat model, but this will depend on the general security philosophy being applied. We believe it reasonable to apply the same threat model for both, though we have even less control over the infrastructure we use for mobile workers. One could argue that traveling staff may be exposed to a more varied threat landscape and may encounter threats more frequently. Much will depend on the results of a risk assessment for each scenario.

A cybersecurity framework

The US National Institute of Science and Technology (NIST) has developed a Cybersecurity Framework[17] as guidance for organizations to better manage and reduce their cybersecurity risk. The NIST framework is widely referenced and applied. It describes five different functions: identify, protect, detect, respond and recover.

At Orange Cyberdefense we have adopted a modified version of the NIST framework that maps to our own capabilities. We have also introduced a function that is not sufficiently clear in the NIST model, namely "Anticipate". We will use this extended version of the NIST framework to help you structure and evaluate your response to the cyber extortion threat. As such our report is structured around the following five functions groups.



1. **Anticipate** the latest cyber threats and prevent digital risk
2. **Identify** your critical assets, data and vulnerabilities to prepare your security strategy
3. **Protect** your organization with the right technology and skills and
4. **Detect** cyber attacks through analysis of alerts and behaviors
5. **Respond** to cyber attacks with proper containment and remediation plans

Has the threat landscape changed due to the COVID-19 crisis?

Not really. The tactics, techniques, and procedures used by attackers remained fundamentally unchanged during the examined period. Our research shows that the lockdown in response to the COVID-19 pandemic had a marginal impact on the volume and intensity of attacks. In the article titled Hidden impact of COVID, published in our Security Navigator 2021 report, we note that attackers pivoted quickly to use COVID-19 as a lure, but this lasted only a short time, before attackers moved on to other themes.

We found that attacks targeting people (e.g. phishing, watering hole and scams) have been featuring more often than the year preceding the pandemic but did not make the news more often during, or because of, the COVID-19 lockdown period. We saw that COVID-19-related social engineering attacks spiked in Q2 of 2020 and then dropped off in Q3, while other significant security events involving 'the human' remained constant for that period.

In our 2021 Security Navigator report, we suggest that at the peak of the crisis in March 2020, there were 17 different countries under lockdown in our area of operations. We note that the total volume of incidents we processed dropped by 12% by the time the lockdowns started getting lifted significantly in May.

As businesses in Europe returned to "normal" again in June, incidents increased by 15%, only to fall again during the European holiday period in July and August. The impact of the pandemic on business activity is notable. According to data from the UK's Office for National Statistics, only 66% of UK businesses were trading during one period in June, and 30% of the UK workforce was on furlough leave during the same period. These two figures had reduced to 47% and 9% respectively by September.

The impact of these meta factors on incident volumes is not always immediately apparent, however. For example, after a period of leave, we see an increase in failed login activity that may appear malicious but then actually isn't. We also observed a reduced appetite to make changes during lockdown, resulting in significantly fewer AD changes or privilege escalation incidents.

Risk of remote working

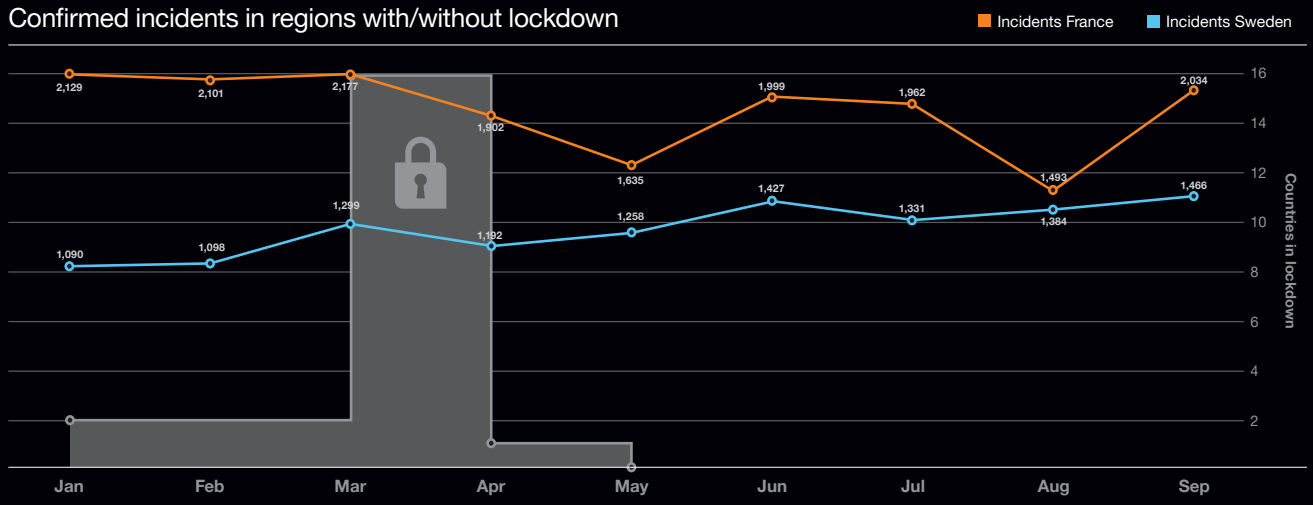
It is vital to focus on the impact of the crisis on the systemic factors, and the first that comes to my mind is the massive adoption of remote working, secured by remote access technologies.

What we see is that there are a myriad security issues with home routers and Wi-Fi connections. Even if they integrate a part of security by design, they still need to be patched and configured correctly, which is, unfortunately, not always the case.

Our research shows that a compromised home router changes the threat model. A home router, Wi-Fi access point, or any IoT device for that matter, is typically a powerful, fully functional Linux computer. It is connected to the same LAN as the user's endpoint and is being "trusted" by the endpoint in several ways. For example, the home router controls or influences network configuration (IP address, routes, DNS settings, network boot settings), web content, connectivity, and more. This puts a malicious or untrusted router in a powerful position in relation to the endpoint.

Lockdown effects on incident count

Confirmed incidents in regions with/without lockdown



In France, where lockdown was in effect from mid-March to mid-April, incident volumes decreased by an astounding 30% between March and May. However, in Sweden, where there was no general lockdown, volumes only decreased by a total of 3%, after dipping by 8% in April.

VPNs and secure remote access: a note on terminology

There is a tricky issue of semantics that we need to address right up front. This paper discusses some of the security properties of a class of technologies we will refer to primarily as “virtual private networks” or VPN. As our business is a significant seller and implementer of security technologies, we feel it is fair to say that this term accurately captures the class of tooling we are exploring. Indeed, it is used by some of the vendors we examine to describe themselves.

The term VPN is used much more broadly than this, however. It expands to (and even originates in) enterprise networking constructs like site-to-site links and MPLS “virtual private LAN” and “virtual private routed network”, services amongst others. Our research and this paper do not examine the technologies deployed under this broader definition of the term VPN.

Another term used to describe the technologies we’re discussing is “secure remote access” or “remote access security”. Once again, this term is widely used to describe the technologies we’re talking about here (often also by the vendors themselves) and stretches to encompass a different class of technologies (e.g. the popular Teamviewer) used to remotely access desktops directly over a network. Again, this latter group is not what we are discussing here.

This paper uses the terms virtual private network and secure remote access to describe technologies that allow a remote user on an endpoint device like a laptop or tablet to connect into a corporate environment over an untrusted network like the internet. They do this by enforcing authentication and creating an encrypted virtual tunnel between an agent on the computer and a gateway deployed on the network’s perimeter.

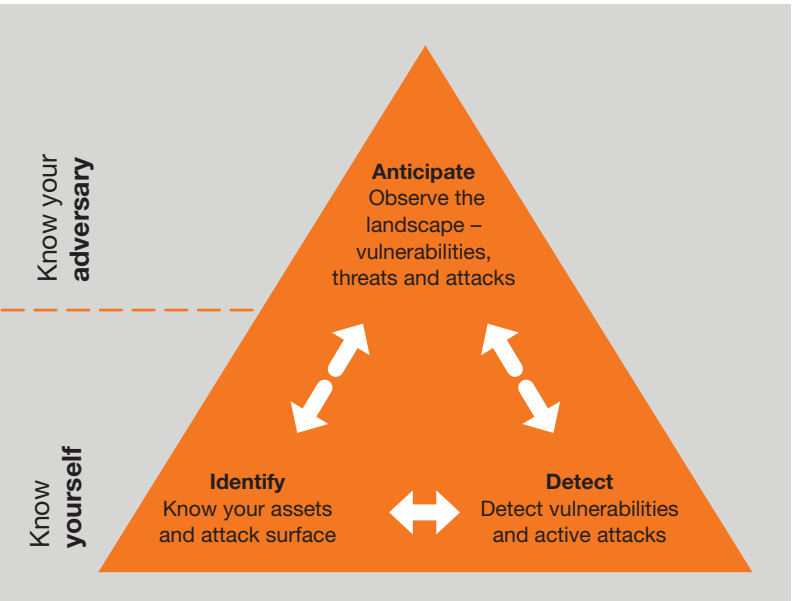
Anticipate

Anticipate the latest cyber threats and minimize digital risk

Intelligence-led security is the collection, validation, aggregation, correlation and analysis of both internal and external data. It enables you to understand risks, identify threat actors, discover attacks underway, and understand the motivations, methods and actions of likely adversaries. Ultimately, it allows limited security resources to be invested where they will have the most impact. This kind of pro-active, intelligence-led approach is as essential to the security of remote workers in other security domains.

By anticipating that you might be a victim and understanding what forms an attack might take, you can assess your readiness and prepare accordingly. A real-time perception of the changing threat landscape – vulnerabilities, tools, techniques, and other relevant factors – can help you to adjust your tactics and apply your resources where they will have the most impact.

For example, we know that our remote workers will connect to an untrusted network to access the internet. These users will likely use Wi-Fi to do so, and we saw this trend increase during the first wave of the COVID-19 pandemic[18].



The mid to late 2000s saw wide adoption of Wi-Fi technology. The first-generation Wi-Fi solutions were rather naïve given what we know today. Since then, several attacks against wireless technologies have been published[19]. Even newer technologies such as WPA3 have been found to contain vulnerabilities[20]. **Not only are Wi-Fi protocols fraught with vulnerabilities, but the devices that offer internet or local LAN access through Wi-Fi are riddled with unpatched vulnerabilities[21].**

In response to this risk, businesses have traditionally deployed technologies such as secure remote access to provide adequate confidentiality and integrity, while ensuring remote users are correctly authenticated before allowing them onto the internal network.

Your preparation should include keeping abreast of developments and new techniques being used by attackers to breach networks. By taking an intelligence-led approach to security, you can better understand the current climate regarding attacker tactics, techniques and procedures (TTPs), and what steps can be taken to counter them. This allows you to focus your resources on the areas that will provide the most reward in terms of detection and prevention capabilities.

Vulnerability management and threat detection, in particular, need to be led by relevant intelligence.

Scanning, SIEM, EDR and IDS tools will no doubt be updated at some point to test for relevant indicators of compromise (assuming you have sufficient telemetry). However, you'll want to assume that the attacker is already active in your environment. You will need to understand how to search for indicators of compromise after the fact. Such indicators need to be broader than just the traditional markers like file hashes and IP addresses provided to you in threat intelligence feeds. Attackers are clever at hiding in normal traffic and behaviors.

Prepare your people

Ongoing user awareness training can also benefit from ongoing intelligence. Put training and testing based on real and current threats in place to provide your employees with the tools they need to identify attempted phishing emails, social engineering attempts or other markers of a possible attack.

Agility is key

Systems are fallible and nothing is perfectly secure. New attacks emerge all the time because of design flaws, programming errors, and incorrectly used or misconfigured technology. Attackers know how to identify these mistakes and will take advantage of such an opportunity.

A “hacker disclosure culture” is mostly seen as a positive means of sharing information about vulnerabilities and detailed proof-of-concept exploits can be used to test systems to verify impact. This is true if it is done in a thoughtful and responsible manner.

Clearly attackers do not subscribe to this ethical approach to vulnerability disclosure and actively seek vulnerabilities to exploit without cooperating with vendors. This is further fueled by the zero-day exploit market that seeks to purchase working exploits to repackage and combine into offensive tools that are sold to anyone with a large enough budget.

An intelligence-led philosophy offers the practitioner the benefit of dealing with new situations by continuously collecting, analyzing, processing, and responding to new information. Military strategist and US Air Force Colonel John Boyd developed a process for this called the OODA loop[23]. OODA is an acronym for “observe, orient, decide, and act”. Each facet provides output that is used as input by the next facet, thus a feedback loop is created. These concepts can be put into practice in the context of cyber security.

The observe phase involves monitoring changes in the threat landscape, as well as identifying vulnerabilities and identifying anomalous activity inside your organization. The orient phase considers how this new information relates to what is happening in your organization. The decide phase requires one to select a strategy based on the information gathered and the given situation. Finally, the act phase is where you execute your decision and use any new learnings to improve the systems and processes.

Since this is a loop, the cycle never stops. In practice, there will be several parallel OODA loop instances based on activities performed by staff. Do not think of an OODA loop as one big loop but rather multiple active parallel processes.

Document your incident response plan

Another key component is establishing a documented incident response process that all employees are aware of and know how to initiate. It should be based on an appreciation of other victims' experiences and tested against real-world case studies, using tabletop exercises and targeted red team exercises, for example. You may also want to keep hard copies of these processes readily available in case they are compromised in an attack. These processes must be regularly tested and updated to ensure they stay relevant to the business and address any new threats or risks.

Understand that the plan needs work for remote workers as well. This means that investigating or remediating an incident may need to play out remotely. Some staff may not be tech-savvy, thus relying on them to perform certain tasks may be unrealistic. Other considerations include remote connectivity constrained by bandwidth speed, latency, or data usage limits.

Be realistic

Understand that staff probably have used work equipment for personal purposes or accessed work resources with personal devices. Neither case is ideal, but understanding that this will happen will allow for a complete playbook and incident response plan.

Staff will probably share the local network with other untrusted devices such as another family member's mobile device, a spouse's work device, and a variety of IoT devices.

Attackers are opportunistic

Despite the prevailing wisdom, it's probably unlikely that incidents occur because an organization was explicitly targeted. It's most likely that attackers will stumble upon a vulnerable device or service, or an exposed remote access service. Going after low-hanging fruit such as brute-forcing credentials or scanning for unpatched services with known exploits are much more likely to be used against an organization.

For this stage of the cyber framework, the implication here is that you need to be more concerned about general patterns and trends in attack techniques than gathering specific intelligence regarding campaigns targeting you directly.

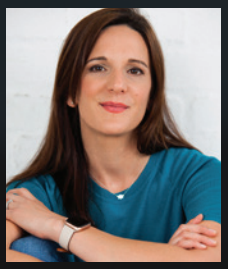
Practice how they'll play

Theory is good but it must be put to the test. Your response plan should be based on current intelligence regarding how remote users are being compromised or leveraged to compromise the enterprise, but your plan needs to be tested against these "intelligence-led" scenarios. You will need to test your remediation and recovery plans, with an emphasis on supporting remote workers. You need to identify and simulate specific, contemporary scenarios that take your remote worker architecture, business assets, risk appetite and key technologies into account. For some of these exercises, you should assume that a breach of your perimeter has already occurred.

Not everything has to be technically demonstrated, however. For example, it is safe to assume that an IoT device on the local network is compromised and can be used to attack your device. Working with this assumption, you can now practice your response to a scenario like this based on the real-world experiences of others.

The key to successful security awareness education

We asked Anna Collard, SVP Content Strategy & Evangelist at KnowBe4 AFRICA, to describe the keys points involved in preparing a successful user security awareness program.



1. Get active executive involvement

You need executive involvement that goes way beyond sponsorship or budget approval for the campaign. Your executives need to be the face of your campaign, because people look at what their leaders are doing. Get a one-minute video clip of your CxO sharing why security is important to the business and them personally.

2. You can't manage what you can't measure

Create a baseline view of your current status by running a proficiency or security culture assessment and track it every 12 months. This will allow you to showcase improvements. Phish prone percentage (PPP) can help as a tracking metric but can be manipulated by changing phish sophistication levels, so needs to be reported in context.

3. Avoid cognitive overload

Focus on two or three key behaviors and/or messages at a time and repeat these throughout your campaign. Don't throw the whole security book at your people, as the danger is that nothing will stick.

4. Don't do it alone

Work with your marketing, internal comms, HR and compliance teams, amongst others. SANS just published a report saying that at least 2.5 full time employees (FTE) need to be dedicated to a successful security culture program.[22]

5. Make it beautiful

This is the visible face of your department, so make sure your comms are beautiful, simple and impactful. Choose content that is personally relevant and interesting to people (protect your kids, your home etc.).

6. Use a carrot and stick

Combine positive with negative incentives: reward desired behavior such as public shoutouts for someone reporting a nasty phish, or bonus payments for anyone not falling for a simulated phish in a certain timeframe. Negative incentives can include automatic remedial training for clickers, and line manager follow-ups for non-participation.

7. Perform relevant tests

Combine training with frequent and random phish simulations. Doing quarterly phishing is not enough. Everyone in the company should get a randomly-assigned phish every week. This gamifies the experience as every email needs to be scrutinized.

8. Be human

Emotions are powerful engagement techniques, so use them in your content. Tell stories and use humor.

Anticipate checklist

Check	Control	Impact
	Do we have incident response and recovery plans that are built with remote workers in mind?	High
	Do I know who to contact when I need assistance during an incident?	High
	Does my staff known who to contact when they need to report an incident?	High
	Am I aware of the most common vulnerabilities and misconfigurations being deployed by attackers (e.g. credentials stuffing against RDP and VPNs), so that I can identify these in my environment?	High
	Are my staff properly trained to identify and respond to contemporary social engineering techniques?	High
	Am I in a position to understand, learn from, and adapt to the experiences of recent victims in my sector?	Medium
	Do I fully understand the tactics, tools and procedures used by contemporary threat actors targeting home users? Do I have access to the latest threat intelligence that provide me with information on current exploit trends and techniques?	Medium
	Are my IT staff and remote workers properly informed about attacks against remote workers to spot the signs of an attack or compromise in progress?	Medium
	Have I considered my cyber insurance policies considering contemporary intelligence about recent compromises in my area of operations?	Low
	Have I conducted table-top and technical exercises based on understanding how contemporary attacks against remote workers play out?	Low

Identify

Identify your critical assets, data and vulnerabilities to prepare your security strategy

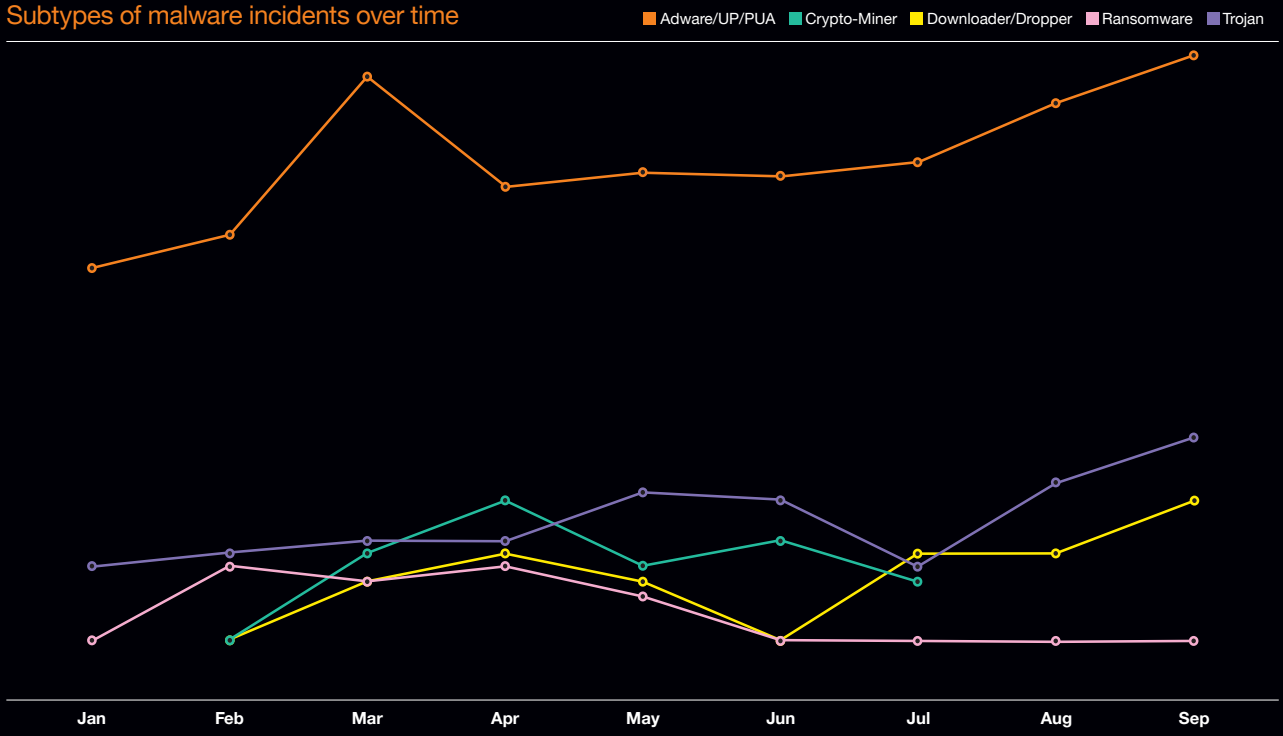
Asset management

You need to identify all hardware and software assets in scope to understand your attack surface. It is essential to get a view from an attacker's perspective. Simply believing that something is out of scope does not mean that an attacker will respect that. This includes remote and mobile workers, cloud-deployed systems, internet-facing systems, security platforms, or anything important for an organization to function.

Allowing users to install any software on their work devices offer great flexibility for staff, but comes with obvious risks. Ideally, you should account for and approve all software present on a host. Depending on how restrictive corporate policies are, it is still wise to scan hosts regularly to determine what software is present and if the appropriate security patches have been installed.

Malware trends

Subtypes of malware incidents over time



In December 2020 we reported a high number of confirmed incidents involving the installation of adware and potentially unwanted programs or applications (PUP). These incidents represent 60% of all confirmed classified malware detections. Most incidents involve users installing unwanted programs or extensions such as zip unpackers, browser add-ons that send user data to external entities, torrent clients, etc. We noted a particular increase in confirmed adware and PUP incidents in March 2020 – during the peak of the first wave of global COVID-19 lockdowns. This is in line with an overall trend we observed, which is a small peak of malware activity in March that is only reached again in late summer, when there is an increase in security incidents and confirmed incidents overall.

One explanation of the March peak could be **that many employees started working from home at this time and felt they needed to install free but unapproved applications as they tried to adjust to the new reality keep up with their normal work activities**. This trend was especially noticeable amongst our small and large organizations.

Determine your threats and risks

Our research shows that readily available security solutions can mitigate most threats that emerge due to remote work. But it is also clear that no single product addresses all the threats. The technologies that **address these threats need to be applied very specifically and configured very carefully**. To truly mitigate all threats may come at a real cost in terms of functionality and useability. Start with understanding your business-specific threats and risk appetite.

This exercise needs to be technical and specific because **our research has shown that details matter**. Such a detailed threat assessment can be achieved via a goal-oriented penetration test or "red team" exercise. With input from product specialists and a robust red team perspective, a thorough threat modeling exercise would be another way to achieve the required view to select appropriate mitigations.

Manage the vulnerabilities attackers will exploit

The **most likely entry points for an attacker involve compromising an end-user via phishing or social engineering**. However, **secure remote access services are also increasingly being accessed or compromised** through password spraying or brute-forcing techniques. Others include exploiting unpatched systems and zero-day vulnerabilities.

These techniques can give attackers a foothold in a network from which to move laterally once inside. Even if a vulnerability is not the initial point of access, local privilege escalation vulnerabilities (PrivEsc) are frequently used to facilitate credential grabbing, malware infection, command & control, lateral movement, service manipulation and ultimately encryption. These **"local" vulnerabilities are often underestimated and overlooked**, yet tackling them can play a major part in managing the eventual impact of an initial compromise.

A robust vulnerability management program must be in place to identify and patch vulnerable systems. This should **cover all internet-facing systems, internal devices, and must be able to include remote workers**. It is also imperative to **include security solutions such as firewalls and secure remote access technologies such as VPNs** in this program. Indeed, of 25 exploits listed in a recent CISA report on the vulnerabilities exploited by state-affiliated cyber actors, six target the kinds of security technologies we use to secure our perimeters and facilitate remote access to our networks.

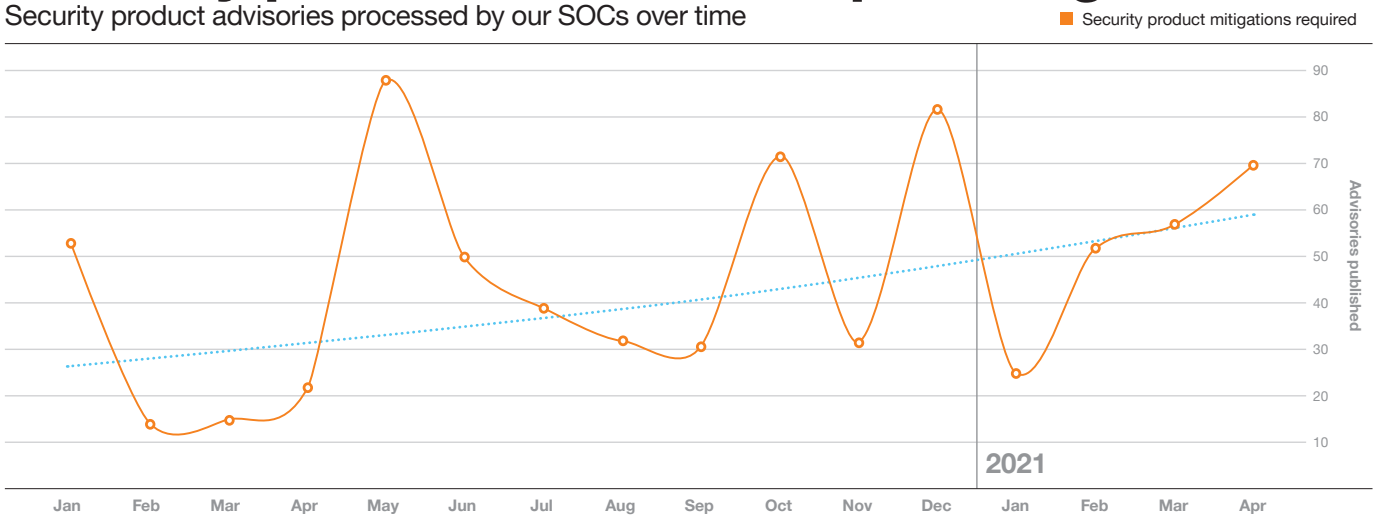
It's clear that the volume of security vulnerabilities in enterprise security and remote access technologies appears to be growing at a noticeable rate, as the chart below from our SOC operations illustrates.

Patch information for vulnerabilities routinely exploited by MSS-affiliated cyber actors

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-5902	Big-IP devices (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT)	F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902
CVE-2019-19781	Citrix Application Delivery Controller Citrix Gateway Citrix SDWAN WANOP	Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 Citrix blog post: security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3 Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0 Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway version 10.5
CVE-2019-11510	Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15	Pulse Secure Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX
CVE-2020-0688	Microsoft Exchange Servers	Microsoft Security Advisory: CVE-2020-0688: Microsoft Exchange Validation Key Remote Code Execution Vulnerability

Security products in need of patching

Security product advisories processed by our SOCs over time



Establishing and maintaining an effective vulnerability management program is something most organizations still find to be a painful and difficult undertaking – especially when considering what can seem to be a flood of new vulnerability disclosures.

The first step in setting up a vulnerability management program is to perform an asset discovery exercise. This will identify the systems deployed in your environment and allow you to maintain an accurate inventory Depending on your environment, hardware can be as important here as software.

An updated asset inventory allows security teams to know if they are impacted when a new zero-day vulnerability or new exploit technique is discovered. Asset inventories must be maintained through dynamic discovery as much as possible to ensure that the information remains relevant. Use automated vulnerability identification with scanning and ensure that it supports end-user platforms for this process to be effective.

Cloud-based vulnerability discovery solutions are best positioned for this type of task as they don't depend on network proximity.

Vulnerability identification processes should probably be "passive". Active scanning over the network is obviously problematic for home user devices, and so businesses are increasingly adopting agent-based solutions that are deployed to the user's desktop directly. This approach has the advantage of reducing the demand on the network and VPN, while providing detailed, continuous inventory, patch, and vulnerability data.

Several vendors are also starting to offer multi-purpose agents that can deploy patches, or even crossover into other realms like malware and attack detection. There are several apparent advantages to centralizing these diverse security controls under one agent, but the key factors to consider are ability to centralize control and telemetry, and the requirement for skills in your team.

Once you have identified these systems, you should assess them to determine the actual risk level for each device or group of devices based on their criticality to the business. This exercise can then be used to prioritize devices when it comes to deploying patches to them.

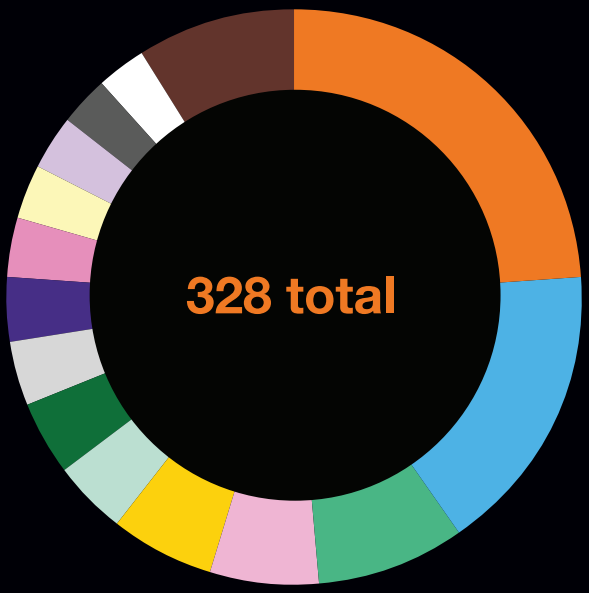
The next step is to regularly run scheduled vulnerability scans against the estate to identify vulnerable assets. The output from these scans should be a report identifying the highest-risk devices based on their criticality rating alongside the risk posed by the vulnerabilities present. **The risk evaluation needs to consider the value and exposure of the asset, the assigned seriousness of the vulnerability, the age of the available patch, and any intelligence about the existence or use of an exploit**. This should then be used to prioritize the remediation of devices by deploying patches automatically or manually as appropriate.

Interactive platforms

Vulnerability scanners and third-party vendors are also increasingly offering sophisticated interactive reporting platforms that layer in asset and risk information and allow for vulnerability scan findings to be organized and interrogated in diverse ways by various stakeholders. This dynamic approach views the vulnerability scan results more as an aggregated dataset to be interrogated than a report that describes a single scan "event".

This approach supports the notion of "intelligence-led" security in that it allows your team to continuously reassess the vulnerability posture in light of new events, rather than having to re-run scans and translate each report in a set of actions. Most modern platforms of this type also provide some level of integration with ticketing and other workflow systems, or provide some workflow management capabilities directly, thus reducing the friction involved in getting remediation actioned.

Don't forget the hardware



	%
Continuous vulnerability management	24.09
Inventory and control of software assets	16.46
Inventory and control of hardware assets	8.23
Account monitoring and control	6.10
Maintenance, monitoring and analysis of audit logs	5.79
Limitation and control of network ports, protocols and services	4.27
Application software security	3.96
Controlled access based on the need to know	3.66
Incident response and management	3.66
Secure configuration for hardware and software on mobile devices, laptops and workstations	3.35
Boundary defense	3.05
Malware defenses	3.05
Data protection	2.74
Email and web browser protections	2.74
Other	8.84

Summary of recommendations made in our World Watch intelligence advisories for Q1 2021

Most of the recommendations emerging from the World Watch security intelligence service we provide fall under the basic CIS controls of inventory and vulnerability management. Moreover, hardware inventory has become more important, growing from 5.9% to 8.3% of all recommendations made during the first quarter of 2021.

There are two approaches to vulnerability scanning, and both need to have a place in your vulnerability management program:

1. Regularly scan and patch to reduce your overall level of risk. Regular vulnerability scanning is analogous to brushing your teeth. You need to perform it regularly and diligently, just to keep abreast of the threat. Of course, the scanning is only as useful as the triage, mitigation, and measuring efforts that emerge from it, but done properly, vulnerability scanning and patching or remediation will put you way ahead of the curve. Regular scanning, even if performed meticulously, is only the beginning though. The threat changes, and we need to respond continuously.

2. Ad-hoc searches for systems with specific vulnerabilities or attributes that are being exploited by attackers. There are thousands of vulnerabilities disclosed each month. For example, between 2018 and 2020 the US National Vulnerability Database officially recorded an average of 1,524 vulnerabilities a month, across 6,744 vendors. And there are likely to be many more we don't know about. Chances are, you won't be able to address them all as quickly as you'd like. But only a fraction of vulnerabilities ever actually get exploited "in the wild". A report from Kenna Security suggested that only 2.6% of 18,000 tracked vulnerabilities were exploited in 2019.[24] With the right intelligence about the severity of specific vulnerabilities, you can adjust patching priorities appropriately. Intelligence has two facets: not only do we need to know what kind of systems to worry about, we also need to identify those systems within our environments. The ability to rapidly perform scans or (preferably) searches across the IT inventory to identify the systems or services most vulnerable to current attack vectors, is the second characteristic of a successful vulnerability management program.

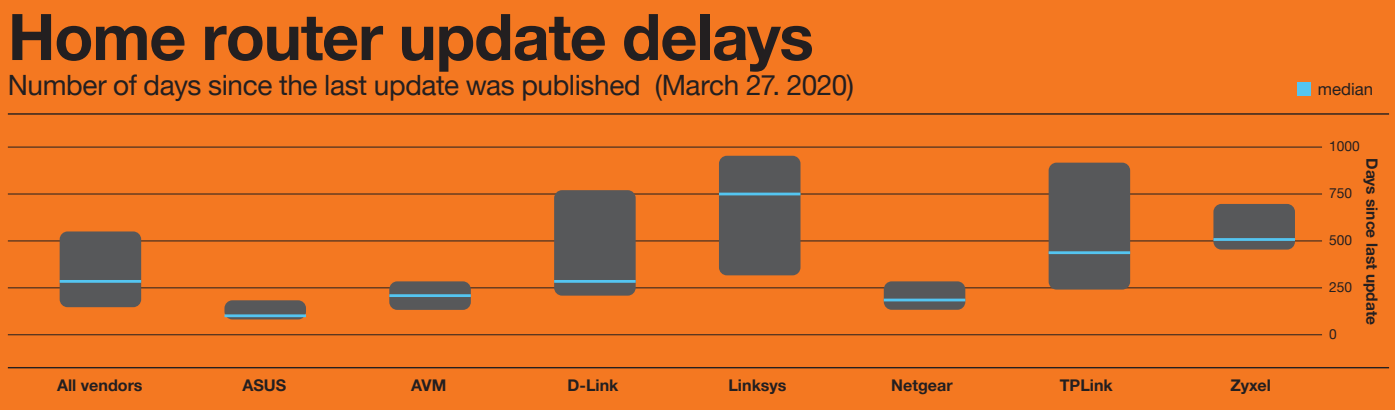
Vulnerability identification must consider all third-party applications and their facets. For example, it is possible to extended or alter the behavior of a web browser through plugins or extensions. Ensure that the asset inventory reflects this and that the vulnerability identification process also covers it. Malicious browser plugins or extensions fall outside this category and must ideally be handled by endpoint protection solutions at the time of installation or activation.

Home network vulnerabilities

In a recent study of the security posture of several home networking vendors, Fraunhofer concluded:

"81 routers got an update within the last 365 days before 27th March 2020. However, **the average number of days since the last update before 27th March 2020 is 378 days**. That means in average devices did not get any security fixes within one year. 22 of 127 devices were not updated within in the last two years. The worst-case was not updated since 1969 days, which means more than five years without security patches".

Our results are alarming. There is no router without flaws: 46 routers did not get any security update within the last year. The boxplot[25] in the figure shows the relative update cycles across the vendors. The blue line depicts the median number of days since all assessed products from that vendor received an update.



Source: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

Staff home routers

Home IoT devices are frequently targeted because these lack adequate security patches, secure configuration settings, or unique credentials. Home routers especially have a bad reputation regarding vulnerability management and what is normally considered secure configuration. In most cases these devices are difficult to patch, primarily because the vendor no longer supports them. You need to either gain a clear understanding of the attack surface and risks that emerge from these devices, or find a way to take them out of the equation so that they're not a concern to you.

Home users may also configure devices to permit potentially dangerous traffic into their network because they wish to expose services, for example, a NAS or security camera system, on their internal network to the internet.

Businesses may want to consider performing vulnerability assessments on their employees' internet routers. These devices could also be included as part of a special asset inventory to track and possibly include as part of the vulnerability management process, but there are obvious challenges to this approach.

The fundamental problem, however, is that these devices are typically owned and controlled by the homeowner or ISP, and not the business, and therefore must be considered fundamentally untrusted.

Unlike other technologies on the internet on the "path" between the user and enterprise network, the home router also has the characteristic of being in direct proximity to the user's endpoint, and indeed exerting significant influence over the behavior of that endpoint via the Dynamic Host Configuration Protocol (DHCP). Our research suggests that control over the home router, and thus DHCP, provides the attacker several opportunities to target the endpoint and the router, many of which are extremely difficult to mitigate.

As the name suggests, DHCP is used to define configuration settings on an endpoint that joins a network, including IP address, DNS, routes and more. While it is possible to layer security over these insecure and untrusted devices, we strongly recommend that businesses consider ways of taking responsibility and control of internet connectivity of their users working from home.

This could potentially be done by offering subsidized connections via mobile (4G/5G) or by providing preconfigured, secured and managed customer premises equipment (CPE) via SD-WAN offerings.

Penetration testing in support of vulnerability management

You should carry out regular penetration testing alongside your vulnerability management program on h**ome worker, internal, internet and cloud environments**. This will help identify any other weaknesses besides vulnerabilities, such as misconfigurations, and test that patches are being successfully deployed.

Penetration testing will also highlight other ways an organization is vulnerable to attack, such as password spraying, or brute-force attacks on systems or services. Internal testing will identify how easy it is for an attacker to elevate privileges and move laterally through your environment.

Practice how they'll play

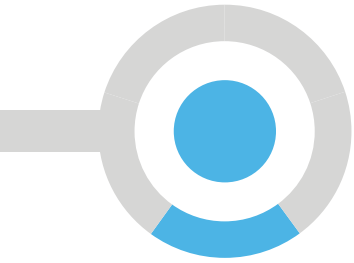
At least some of your testing must be designed to mimic the techniques of contemporary cybercriminals. This includes scoping the tests to incentivize the same aggressive technical and social engineering techniques attackers are currently using. It's no good testing for weaknesses you already know about. **Find and engage with testers you can trust to truly exercise your security technologies and processes using real-world, intelligence-led techniques**.

An emerging approach to penetration testing is called "purple teaming". Derived from the traditional labels of "red hat" and "blue hat", this approach seeks to actively test detection and response capabilities (as well just protection mechanisms). It deliberately involves your security and operations team in the exercise. In a purple team exercise, your security teams are invited to participate in the process and allowed to assess and refine their capabilities with guidance from a battle-tested adversary.

Such real-world testing, by a reputable provider with the required technical bona fides, is an excellent way to understand how badly an attack against home workers might impact your enterprise environment.

Identify checklist

Check	Control	Impact
	Do I have a comprehensive view of my IT assets, particularly of my internet footprint, and what IT systems my users are actually deploying at home, so that all these systems are being considered in my vulnerability management program?	High
	Do I have an effective vulnerability and patch management process that ensures relevant security patches are being identified, triaged, and remediated within an appropriate time?	High
	Am I certain that my vulnerability management program has sufficient scope and covers all the systems an attacker might target, including remote worker PCs, Linux, OSX, appliances, and connected hardware, wherever they may be connected?	High
	Are my SOC and response teams involved in penetration testing exercises to acquire proper “battlefield” experience and practice identifying and responding to a skilled and determined adversary?	High
	Am I aware of third-party tools and applications your remote workers may be getting directly from the internet, because they’re considered necessary for their jobs?	High
	Does my vulnerability management program also incorporate security platforms, and especially remote access, VPNs, and remote desktop environments, which are frequent attack vectors?	High
	Does my vulnerability management program include mobile devices allowed by the corporate BYOD policy?	High
	Does my vulnerability management program consider all internet-facing systems, including those that are used for remote access, and those used as fallback, or apparently deprecated?	Medium
	Am I routinely checking for weak passwords and password reuse issues, which are commonly exploited by cybercriminals?	Medium
	Do I have access to intelligence that informs me when the risk rating for a system, service or vulnerability needs to be re-rated?	Medium
	Can I perform ad-hoc scans or searches to identify systems or services that may have become an attacker vector for criminals?	Medium
	Does my business engage regular penetration tests or red team exercises that emulate the tools and tactics that actual cybercriminals are deploying, and can proceed without excessive limitations or constraints?	Medium
	Do I have a hardware inventory of routers used by remote users, and do we know what their exposed services and the patch level of the devices are?	Low



Protect

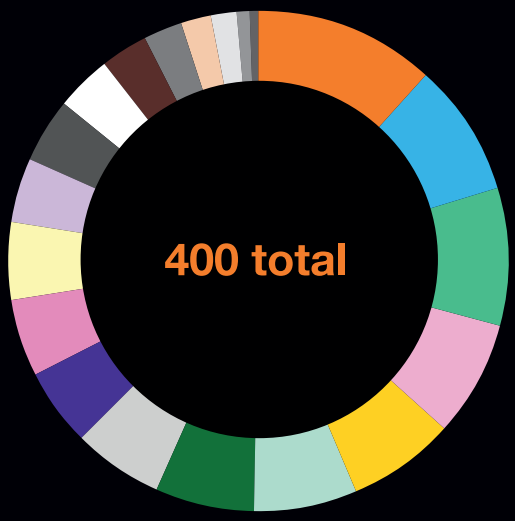
Protect your organization with the right technology and skills.

Don’t depend on your users to detect malicious content

As already noted, **phishing attacks are a key vector for an attacker to gain a foothold in a network**. There is a strong argument that remote workers, operating in isolation and without the opportunity to stroll over to IT or chat at the water cooler are more susceptible than they may otherwise be.

Therefore, a solid email security system must be in place to detect and prevent phishing campaigns and other email-borne threats. An optimal solution is a cloud-based service, as it provides centralized monitoring and control and can scale as required when the need arises. You also benefit from real-time intelligence and protection based on telemetry from the vendors’ customer base.

An analysis of hundreds of incidents handled by our CSIRT in 2020 (about 10% of which were ransomware) shows the distribution of control failures our analysts identified.



	%
Maintenance, monitoring and analysis of audit logs	11.75
Controlled use of administrative privileges	8.75
Limitation and control of network ports, protocols and services	8.75
Continuous vulnerability management	7.50
Account monitoring and control	7.00
Secure configuration for hardware and software on mobile devices, laptops and workstations	6.75
Implement a security awareness and training program	6.25
Malware defenses	5.75
Application software security	5.25
Incident response and management	5.00
Email and web browser protections	4.75
Controlled access based on the need to know	4.25
Penetration tests and red team exercises	4.25
Data protection	3.50
Boundary defense	3.25
Inventory and control of software assets	2.25
Secure configuration for network devices, such as firewalls, routers and switches	2.00
Data recovery capabilities	1.75
Inventory and control of hardware assets	0.75
Wireless Access Control	0.50

“It’s no surprise that phishing attacks related to working from home are increasing given that many countries around the world have seen their employees working from home offices for nearly a year now. Just because employees may be more used to their home office environment, doesn’t mean that they can let their guard down. The bad guys deploy manipulative attacks intended to strike certain emotions to cause end users to skip critical thinking and go straight for that detrimental click.” [26]

Stu Sjouwerman, CEO, KnowBe4

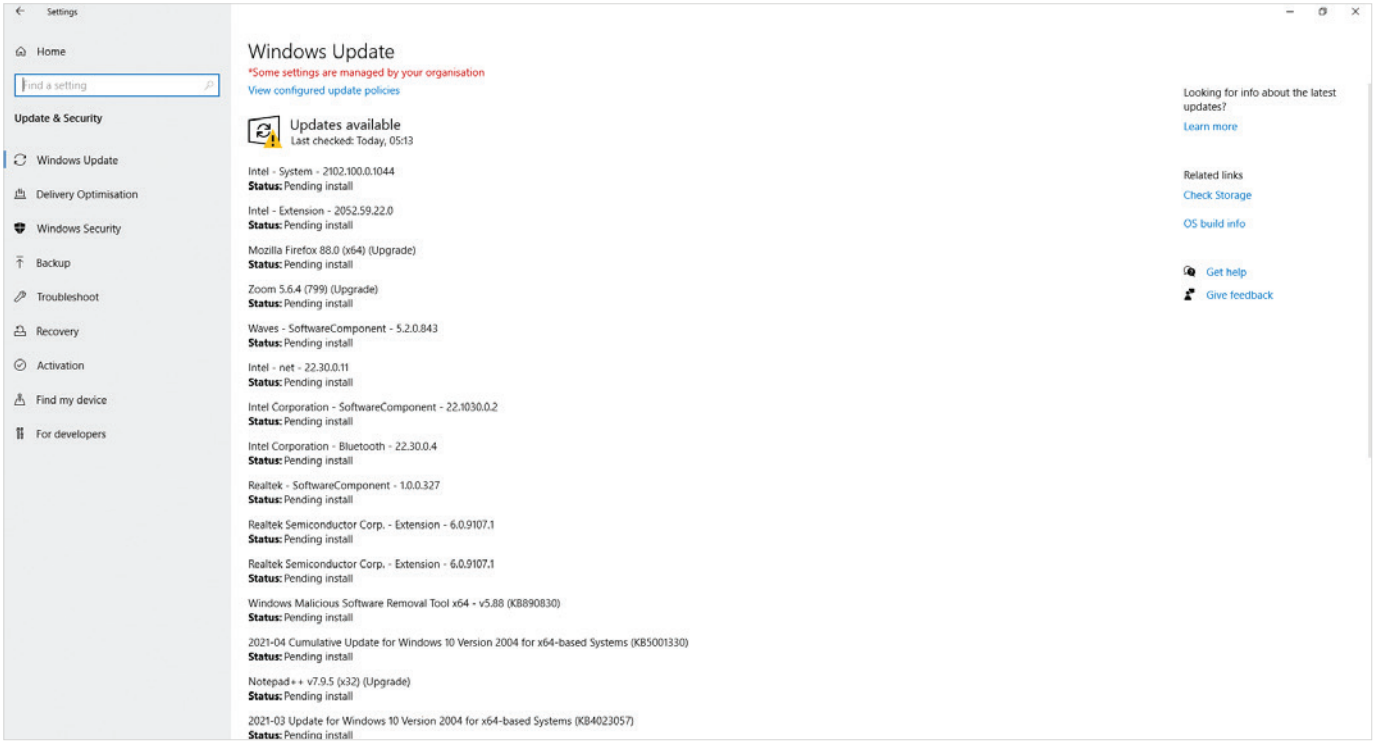
Strong authentication, everywhere that matters

You should enable multifactor authentication (MFA)[27] on all internet-facing services, where feasible. **At the very least, MFA should be implemented on email, VPN and exposed RDP services**. This will then restrict other primary attack vectors, namely password spraying and credential stuffing. SMS multifactor authentication mechanisms should only be used as a last resort and should be moved away from at the earliest opportunity. Instead, use an app-based or token-based one-time password (OTP) solution, as this removes the risks of a SIM-swapping attack being used to intercept the MFA SMS request.

Patch security vulnerabilities

The purpose of vulnerability identification is to know what must be patched. A 2020 Ponemon report indicated that only 21% of respondents in a study of 1848 IT security professionals indicated that their organizations are “highly effective” in patching vulnerabilities. We can conclude that patching is difficult and made more complex by the remote worker dynamic. It’s a challenge we desperately need to tackle.

Patching solutions must be automated to ensure that vulnerabilities can be addressed at scale. It is not practical or feasible to perform manual patching when you have an estate that consists of thousands of machines.



Patching solutions must not tie remote workers to an on-premises solution as this can create a dependency on connectivity solutions like VPNs, which in turn may suffer due to bandwidth limitations. On premises patching solutions may be good for systems located in a data center but is less ideal for remote workers.

Leveraging update services of trusted vendors instead of traditional on premises update services may be better suited for remote workers as bulky update downloads happen directly from the vendors provisioned update service, but may create a visibility problem.

Patch management for remote computers: from the horse's mouth

We asked our own Global Chief Information Security Officer, Richard Jones, for guidance on approaching the issue of vulnerability and patch management for remote workers. This is what he said:.

1. Define standard builds

The first challenge is to ensure that you are working from a limited number of standard builds. Not every desktop can be the same, but you want to restrict the number of different builds down to the smallest possible number.

2. Don't depend on VPN connectivity for deploying or managing patches.

It's unrealistic to assume that remote workers will connect often enough to ensure consistency. You have to find a way to manage and distribute patches via a robust cloud infrastructure without requiring them to connect to a VPN.

3. Use vendor updates where appropriate.

Certain mature user applications can be trusted to push patches automatically, including Microsoft Office, leading browsers, document viewers, and other trusted vendors you chose to approve. Given the growing frequency of software supply chain attacks, you need to carefully assess the security resilience of the vendor and their software update mechanisms before adding them to this list. Vendor updates can be leveraged to do the heavy lifting, you still need to verify that the process is working, and machines are getting updated as expected.

4. Consider the hardware.

Modern attacks frequently target drivers, firmware, and other aspects of computer hardware. Your patch management program also needs to consider how patches for these elements can be identified, tested, and deployed, especially given the risk of an update failing.

5. Ensure that you verify major updates.

You need to assess and prioritize updates, especially for drivers, firmware, and operating systems where an update failure might seriously impact the computer. The risk of disruption needs to be weighed against the security risk the patch is addressing, given what intelligence suggests about the exploitability of the vulnerabilities in question.

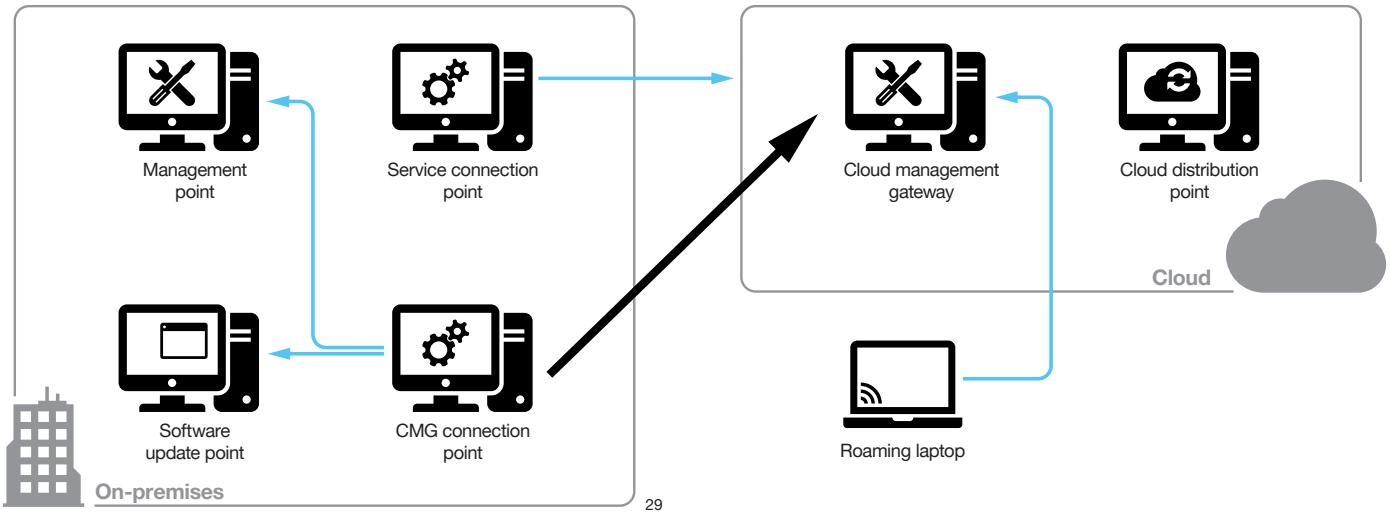
6. Trust but verify.

Whatever approach you take to deploying patches, you need to verify that updates for all applications are properly installed on all the endpoints in your environment, including remote workers.

Choosing the right tools

Microsoft Endpoint Configuration Manager (ECM), previously known as Microsoft System Center Configuration Manager (SCCM), is a systems management software product developed by Microsoft for managing large groups of computers running Windows, Windows Embedded, macOS, Linux or UNIX, as well as various mobile operating systems. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory[28].

ECM is well known and widely deployed, and perfectly suited to managing endpoint software on the enterprise network. In addition, Microsoft offers several technologies intended to help reduce bandwidth and network load to optimize update delivery. Traditionally ECM has been oriented toward on-premise deployments, but options are now available to distribute updates via the Microsoft Content Distribution Network (CDN), which is available on the internet, and therefore negates the need for enterprise network access.



29

In addition to ECM and the Microsoft CDN, some other technologies may be required to complete your capabilities. Firstly, you may want a platform that specializes in managing updates for third-party products, as ECM may not be ideally suited to that. Secondly, you may consider a platform (like the vulnerability management interfaces listed above) that allows you to consolidate data from diverse configuration management databases (CMDB), update, and vulnerability management tools into one consolidated dataset and user interface.

Consolidating all your updates in one platform, like ECM, obviously creates a highly valuable single point of failure. An attacker with sufficient access to this platform would have the ability to deploy any software to any device on your network. Appropriate segmentation, configuration and protection of this infrastructure is therefore paramount.

Patch priority should be determined based on known active threats and updated continuously as the threat landscape changes. An intelligence-led approach as described earlier, will help organize the patch priority.

Rolling out security patches always potentially impacts the system. The worst case is that the update could corrupt the operating system or possibly introduce stability issues. This may be rectified by following a rollback procedure, which could involve activating the procedure to replace or swap out a now defective device. A robust data backup or file storage strategy for remote users will minimize productivity loss in the event of a planned activity. The selected approach must accommodate easy recovery will little end-user involvement and must complement the overall business continuity planning.

Unified endpoint management

Unified endpoint management (UEM) also known as enterprise mobility management is a holistic approach to managing endpoints, including mobile devices previously managed by mobile device management (MDM) solutions. UEM and MDM solutions can be used to assist with policy enforcement, asset inventory management, patch management, vulnerability discovery, and more. Depending on corporate policy, UEM solutions can be configured to prohibit the installation of mobile applications from untrusted sources, control how devices access the internet, what services can run on the device, etc.

MDM solutions must be complemented with mobile threat protection to guard against installed applications being exploited, applications turning rogue, or new malicious applications being installed.

Get the "basics" right

There are also a couple of "basic" security hygiene practices that should be implemented, while these will not prevent an attack, they can help to restrict and contain one, thereby buying time to detect the attack and eradicate it from your network. Primarily they are the principle of least privilege and network segmentation.

Enforce least privilege

Enforcing least privilege revolves around **only giving a user account or process those privileges which are essential to perform its intended function**. This is not always an easy thing to implement and can often result in pushback from some business areas that see it as disruptive. But it's an essential weapon in your armory.

Feedback from our CSIRT tells us that standard users have been given far too much freedom, access, and privilege on devices and network systems in many incidents they attend. An initial first step is ensuring that a user's standard domain account does not have administrative privileges anywhere. This includes locally on a device or at domain admin level. At the very least, if a user requires some form of administrative access, then a separate account should be provided, which gives them that access only while they need it.

Where possible, use a privileged access management (PAM) solution where passwords can be checked out, then checked back in once used and changed. This also extends to a PC's local administrator account. **Every computer's local password should be unique** as this will help prevent lateral movement to other devices if one password is compromised.

Microsoft has provided the Local Administrator Password Solution (LAPS) to help manage this.

The principle of least privilege should not just be limited to the standard Active Directory environment, but should also apply on all systems, services and solutions users access. If a user only requires access to one element of a system, or only needs read-only access, for example, then they should be granted just those permissions and no more.

This can be especially challenging in cloud, multicloud or hybrid cloud environments, but it is all the more necessary. In these environments, you can configure any human or machine identity with thousands of identity and access management (IAM) permissions to access services potentially containing sensitive information. Due to these complexities, it is very easy to unintentionally provide identities with permissions allowing access to services and resources, which they do not require.

The organization must decide if they will provide a local administration account to their users. This runs the risk that users may abuse this account to install of potentially unwanted programs. This approach is still better than assigning administrative privileges to the user's main account and should be used sparingly. Organizations will have to decide which remote users they extend this courtesy to, such as software developers.

Finance staff, for example, are frequently targeted and policy may require that these worker's environments be locked down. As an additional precaution, these staff are not provided accounts with administrative or elevated privileges. Staff with such setups will be required to log support tickets with an IT helpdesk. The IT staff can provide remote assistance using a variety of existing tools.

IT staff can then use LAPS to access the unique password of the administrative account associated with the remote host and perform their support tasks accordingly. Alternatively, support staff can use other support strategies to push software to remote hosts using a preferred mechanism such as Microsoft's Endpoint Configuration Manager.

Segment networks as much as possible

Network segmentation uses the principle of least privilege to only allow the network traffic that needs to get to and from a system so it can operate, while preventing all other traffic. This should begin with basic perimeter security, ensuring that only required systems are exposed to the internet and that they are only exposing the required services.

Comprehensive network segmentation is a general security best practice that will slow down lateral movement after any kind of compromise. In the special case of remote access, this is best achieved by implementing the age-old notion of a 'DMZ':

1. Ensure that a VPN connection only provides network-level access to the specific systems that a given user needs access to, ideally even on a user-by-user basis if possible.

2. Ensure that the systems the VPN does allow access to are themselves segmented from the rest of the network as much as possible to reduce the "blast radius" in the case where a VPN exposed system is compromised.

The idea of reducing the blast radius starts to lead us down the path of "zero-trust" architectures, which we will examine in more detail later.

Deception technologies

One other area that should be explored is the concept of deception technologies, an emerging element of cybersecurity that is gaining significant traction. The tactic of deception is particularly effective against human attackers as they seek to move laterally through a network and usually provides solid evidence of an intrusion.

Deception technology uses traps (decoys) and/or lures mixed among and within existing IT resources designed to tempt an attacker to interact with them. As these traps or lures are not "real" and serve no genuine purpose, any interaction with them by an attacker will generate an alert that can be considered concrete as no one should be interacting with them. These traps or lures, often referred to as canaries, can be in the form of specific files, user accounts or even a host system on the network.

Dominic White is the Ethical Hacking Director at Orange Cyberdefense.

"But that's a noisy, high false-positive alert, so we end up back at needing a blue team to look after the EDR solution data stream. What if instead, we made high quality (i.e. low false positive, low volume) alerting "the basics"? Something the overworked IT/sec manager could use. Which is partly a justification for why deception techniques can and should make up a bigger portion of sec team work earlier on in the strategy than most people typically put it." [30]

This can even be extended to processes running on devices, as **attackers like ransomware actors will try and kill certain processes to disable security products or release files so they can be encrypted**. As these processes are quite well-known, fake processes can be used and if they are detected being stopped then an alert is generated. While all this can be accomplished internally relatively easily, services do exist to automate the creation and management of these canaries. They will make them appear as realistic for your environment as possible as well as catering for more complex scenarios and capabilities.

Used in conjunction with appropriate network segmentation, **host canaries could also be used to help detect VPN compromises**. For example, by placing a simple honeypot in proximity to legitimate VPN-exposed systems, one may be able to detect an attacker that has compromised the VPN or an exposed system and has started reconnaissance prior to attempting lateral movement. Honeypot lures are a high opportunistic detection method, but they come at a very lost cost to acquire, deploy and manage and therefore serve as a powerful extension to your other defenses.

Deception obviously also needs to be paired with effective detection and response capabilities. Deception alerts are infrequent by design, but of very high fidelity. Accordingly, systems and processes must be put in place to ensure that alerts from deception systems are noted and responded to with appropriate urgency.

Understand where data is really stored

Critical business data differs from business to business. For some businesses, it makes sense to have data stored centrally, while in others, it needs to be stored as close as possible to the people working with the data. Understanding how data is consumed and how data is processed is crucial when working with highly regulated data.

The General Data Protect Regulation (GDPR) of the European Union has several requirements about how data is processed, stored, and who is responsible for data at a given point. GDPR also makes provision for data subjects to make requests asking for details on how and why their data is processed. This feature of the GDPR places an additional burden on the data controller as they need to accommodate these requests within a month and normally without any fee [31]. This is but one example of where the data lifecycle is important for continued business operations.

Data classification plays an important role when designing a data management strategy. This helps to design for regulatory requirements and steers role-based access control. All of this is crucial to ensure business continuity.

Attackers know the value of email and that inboxes contain valuable information. Similarly, staff could leak sensitive data through email, either by accident or intentionally. Data loss prevention (DLP) solutions can help by limiting the chance of data being shared with unauthorized parties.

Attackers will also seek out means to access endpoints to use mapped network drives to access files. The lack of adequate permissions on this network-accessible data is generally a problem that attackers love to take advantage of.

Similarly protecting data at rest must be high up on the priority list of any security or IT team. This includes a wide range of controls, from protecting physical backups through to protecting data on remote or mobile devices. Backups in general, are created to help guard against data loss and to recover from an incident. Businesses can invest in offline solutions as well as online or cloud-based solutions. Backup solutions are only as good as the recovery strategy.

Cloud-based backup and data storage solutions make sense for remote workers, but it's important to recognize the risks associated with this. Cloud-based storage solutions offer remote workers the ability to keep data in a location that multiple devices can access. It facilitates easy sharing of data without physically sharing the data or duplicating the data by emailing it as an attachment, for example. Cloud-based file storage could be a challenge for DLP solutions as staff could use any service to upload data. Access to the storage account must be tightly controlled with authentication that relies on several factors.

Devices in the possession of remote workers can be lost or stolen. **Full disk encryption can help to limit access to sensitive or proprietary information when the device is not in control of the designated custodian.**

Any data management strategy that seeks to encompass remote workers needs to be realistic and reflect an empathetic understanding of the worker's actual working environment. People will want to use their mobile phones, access data from personal devices, and transfer large files to third parties. It's crucial to understand and securely accommodate the daily needs of your remote workers or your controls will ultimately be bypassed, and your security strategy will crumble.

Secure exposed infrastructure

In our annual Security Navigator report for 2021 we point out **that many of the "new" threats we observed involved attacks against remote access or perimeter security infrastructure, rather than the endpoint device**. We noted that in conjunction with the increased deployment of security technologies, we also observe an extraordinary increase in reported vulnerabilities for these kinds of systems, including technologies from several leading perimeter security product vendors.

We believe this extraordinary surge in security product vulnerabilities is the function of three factors:

1. The notable success of Pulse Vulnerability, CVE-2019-11510, from May 2020, which has been exploited in several high-profile attacks.
2. The rapid and sometimes reckless adoption or expansion of secure remote access capabilities to accommodate remote workers, which made these technologies a very attractive target.
3. A cascade effect in which the discovery of one vulnerability creates knowledge, experience and ideas, and thus leads to the discovery of different vulnerabilities in the same product, or similar vulnerabilities in different products.

Several of the vulnerabilities recently discovered in perimeter security products have become popular targets for attack by cybercriminals like REvil and have been pivotal in some of the major breaches of the past year. They are also popular with state-backed actors. In a recent advisory released by the US National Security Agency (NSA) titled State-Sponsored Actors Exploit Publicly Known Vulnerabilities, they list the 25 known vulnerabilities in active use by state-sponsored actors. Six of the twenty-five involve perimeter security technologies.

"In a recent advisory released by the US National Security Agency (NSA) titled State-Sponsored Actors Exploit Publicly Known Vulnerabilities, they list the 25 known vulnerabilities in active use by state-sponsored actors. Six of the twenty-five involve perimeter security technologies."

Consider the home router

There is a good chance that staff working remotely will be using their own home wireless routers to access the internet. These home router devices represent a blind spot.

We presented research at Black Hat USA 2020 and RSA Conference 2021 that demonstrates practical threats and how some secure remote access technologies, on their own, cannot adequately deal protect an endpoint.

Remote Access Point (RAP) devices provisioned and managed by the business can help to secure the full communications channnel. This means that mobile devices and laptops can connect to the device using Wi-Fi with strong authentication and data will be tunneled securely to the business.

There are, however, several factors to consider. One is the coverage range of the Wi-Fi device. Poor coverage may inconvenience staff and cause them to use an alternative access point. Another is that all traffic is pushed through the VPN- tunnel which may impact user experience or negatively affect some cloud-based services. This type of solution may "confuse" some services that rely on geographical information to direct users to specific content distribution networks (CDN). It can lead to increased latency and degrade performance of certain collaboration software that depends on video conferencing.

To improve the user experience, the business could sponsor internet access in the form of mobile data. The remote worker will then connect to the trusted mobile router supplied and managed by the company. Secure remote access technologies must still be used to ensure selected traffic to specific services are protected, while exceptions could be introduced for cloud-based services. Microsoft calls this type of tunnel configuration "VPN Forced Tunnel with broad exceptions"[32].

Mobile data may provide freedom of movement benefits, but mobile data services could be unreliable or could become prohibitively expensive, once certain data usage thresholds have been exceeded. This could result in the user falling back to Wi-Fi solutions.

Another option could be for the business to provide a complete solution with fixed-line access, such as fiber to the home (FTTH), with a managed device. This can allow the business to control all aspects of the remote network, including quality of service (QoS). It is also possible to offer guest internet access to remote workers, and this could allow staff partial use of the sponsored solution for personal and home use.

Virtual desktop infrastructure

Virtual desktop infrastructure (VDI) solutions have the benefit of exposing a fully-featured desktop environment to remote staff on their endpoint.

VDI gives administrators the ability to provision and control access to data. In other words, staff can't easily download or extract information to their remote devices. Any data sharing is controlled at the enterprise level. However, it is possible for malicious insiders to take screen captures or photos of displayed information and leak details that way.

User experience on VDI can be negatively impacted by poor network bandwidth or high network latency. This could result in remote staff experiencing disconnects or a slow and sluggish desktop environment.

VPN configuration

In our Black Hat USA 2020 and RSA Conference 2021 talks we highlighted the need to enforce strict VPN configuration that limits the local network interaction of portable computing devices. We referred to this configuration as "lockdown" configuration. It can be thought of as a **hardened configuration state that enables the secure remote access agent on the end-user device to control interaction with the local network until the secure channel has been established.**

The lockdown configuration addresses the dangers of captive portals and Wi-Fi access points that require the guest user to interact with a service before being granted access to the internet. An attacker-controlled captive portal or malicious Wi-Fi access point can launch several attacks against the endpoint in this state. This could result in credential theft or leverage the guest user's browser to gain access to internal networks after the VPN tunnel is established.

7 steps to better VPN configuration

For your VPN configuration, we recommend that you strongly consider the following actions:

1. **Update your VPN software to the latest version.**
2. **Enforce "route precedence" on your endpoint VPN agent.** In other words, ensure that external factors such as DHCP cannot interfere with routes directing traffic through the VPN to your network.
3. **Review the use of "split tunneling".** Microsoft speaks of "Forced Tunnel with exceptions", which is a concept that forces all traffic through the VPN tunnel, except for predefined exceptions.
4. **Control DNS resolution on the endpoint.** Its essential to define the DNS server the endpoint uses and control how host names are resolved, as attackers can abuse DNS to divert traffic and connections.
5. **Fully qualify internal host names.** All host names for internal resources must have the complete domain name suffix. Using resources without that domain suffix can result in attackers abusing the DNS search suffix feature to resolve hosts to IP addresses they control.
6. **Review VPN session time-out settings.** If the VPN tunnel times out without sufficient lockdown settings while the user is away from the computer, it may leave the desktop exposed on a potentially malicious LAN.
7. **Complement VPN by using firewall or endpoint protection to control sensitive outbound connections.** Several of the attacks we've demonstrated involve redirecting traffic destined for the enterprise network to a malicious endpoint located on the LAN or Internet. Use a local host firewall to prevent this.

A key principle of the hardened VPN lockdown configuration is to **prohibit any service or application the portal computing device from interacting with any other device on the local networ**k until the VPN tunnel is properly established. Only the VPN agent may initiate communications and interface with the captive portal web site using a sandbox-protected web browser commonly referred to as a captive portal mini browser (CPMB). **The VPN agent should only allow services or applications to interact with the network once the VPN tunnel has been established and all VPN policies have been applied.**

Route precedence is another essential feature that the VPN agent must enforce. Network routing is an important concept used by VPNs to move traffic securely from the remote site to the corporate network. Technically there is a lot more to it than that, but in essence, network traffic can be directed using the local machine's network routing configuration. The VPN agent can influence this by making temporary configuration changes that will force certain network traffic to flow through it to the peering location.

We've found **that in certain cases, an attacker in control of the Wi-Fi access point can manipulate this routing table by using DHCP to inject custom routes that change how traffic flows**. This means that the attacker can redirect traffic destined for the corporate network to a malicious host, where login credentials could be stolen, for example.

Ensure you control the remote user's DNS server and how host names are resolved. An attacker-controlled access point can manipulate and direct traffic based on what IP addresses are associated with hostnames. Person-in-the-middle[33] attacks can be prevented if applications detect anomalous host certificates, but applications must refuse to continue when an invalid certificate is encountered. **You want to avoid any situation where the user is prompted to make a security decision relating to the certificate's authenticity.**

Do not use unqualified hostnames when configuring resource mappings within your environment. An attacker-controlled access point can use DHCP to manipulate DNS search suffixes that could result in hosts resolving to IPs under the control of the attacker.

The risk regarding VPN session timeout must also be considered in the light of an access point that an attacker may control. Our Black Hat and RSA Conference talks highlight that a **VPN on the endpoint can only offer real security benefits once the VPN tunnel is established**. Some VPN agents offer lockdown features that can make a difference when connecting to malicious access points, even when the VPN is not established. **But when a VPN session times out, the VPN lockdown configuration must kick in to protect the endpoint in its idle state when connected to an access point.**

Businesses must **consider using logging on the endpoint to detect anomalies and known attacks launched over the local network**. Tools such as Sysmon can be used with great effect to identify specific conditions, and EDR can also add a lot of value here. However, you need to consider that the logs need to be communicated with a centrally managed service that has rules defined to trigger alerts when specific log conditions are encountered.

Dual stack IP configurations

Most Windows machines support IPv4 and IPv6 network configurations, and IPv6 is slowly but surely becoming more relevant each year. However, **some security products and configurations do not consider IPv6 and concentrate only on protecting IPv4 networks.**

It is very likely that VPN sessions establish using an IPv4 network, but the IPv6 network stack on the host is also active. **An attacker can abuse the IPv6 network to influence DNS resolutions and network traffic since IPv6 takes precedence over IPv4 on Windows configurations.**

Consider a "zero-trust" approach

The zero-trust security model eliminates implicit trust in any one element, node, or service. Instead it requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

Zero trust is a mindset or a set of principles, it is not a technology. You can never be 100% zero-trust "compliant" or "capable". **Applying the zero-trust philosophy is a journey.**

There are three important principles that the zero-trust model teaches us:

1. **Apply the concept of least privilege.**
2. **Assume that breach is inevitable or has likely already occurred.**
3. **Every transaction must be authenticated and authorized.**

Several vendors have established a presence in this space, and many are positioning themselves as providers of zero-trust solutions. The solutions on offer generally will enable architecture that is aligned with zero-trust core principles. No single technology will grant you zero-trust status, however.

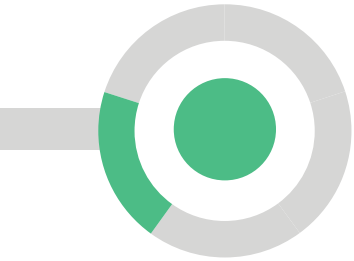
Several vendors also offer innovative zero-trust solutions that allow secure remote access to corporate resources. These resemble VPN-like solutions, but unlike traditional VPN services they do not expose a VPN service at the corporate perimeter. We have seen several reports of VPN appliances that were compromised due to unpatched vulnerabilities or credential compromise[34]. The "application broker" approach uses an intermediary technology to facilitate the reverse connection between the client and the service appears to reduce that risk.

These **zero-trust secure remote access technologies enable businesses to apply the concept of least privilege by only exposing specific applications or services to users**. Users never get access to the network; they only get access to brokered application or service instances. This allows us to segment their applications or services, as the principle of least privilege requires.

Under these configurations, **it also becomes possible to inspect and analyze all network and application transactions**. All activity must be associated with an authorized entity and the policies associated with that entity and application can be tailored to permit or block specific behaviors.

Protect checklist

Check	Control	Impact
	Do I have a system for distributing patches for the operating system and third-party applications on all servers and workstations in my domain, including remote worker endpoints? Does that system support remote workers by operating via the cloud, without a VPN connection being required?	High
	Am I certain I know where all my remote access systems (remote desktop and VPN are), and do I have systems and processes in place to track discover and address vulnerabilities and misconfigurations on these systems?	High
	Do I restrict network-level connections as tightly as possible once a remote worker is connected via the VPN?	High
	Have I aggressively implemented least privilege on all my endpoints, servers, and services, but especially on remote worker endpoints?	High
	Do I have an identity provider that offer a range of compatible multi-factor authentication integrations or solutions? Have I implemented MFA for all users on all my remote access systems?	High
	Do I have an effective content security system that analyzes and filters potentially malicious content from email and from the web? Do these controls apply even for remote workers, and even when they are not connected to the VPN?	High
	Do my remote workers receive regular updates about contemporary phishing and social engineering attacks in an appropriate format? Are they as empowered as possible to detect these kinds of attacks and do they know how to deal with them when they do?	High
	Do I understand what data my remote workers need, where it's located and how they access it? Do I have a data management program and can I assign access to data based on roles and privileges?	High
	Have I considered sponsoring internet access to my remote staff, to take their personal home routers "out of the equation"?	High
	Do I understand what security controls have failed or are lacking when other businesses suffer incidents involving remote workers, and am I confident that my business won't repeat the same mistakes?	Medium
	Does my endpoint solution allow me the ability to protect remote staff that may not always be connected with secure remote access technology?	Medium
	Do I have a finite set of prescribed "builds" for my employee desktops that are flexible enough to meet their needs, but standard enough for me to track my gauge my software exposure and properly test patch rollouts?	Medium
	Do I have a means of validating the patch level on all systems, including remote worker endpoints? Can I cross-reference patch levels with results from vulnerability scans?	Medium
	Have I segmented my internal networks into smaller logical groups with strict controls for specific traffic flowing out of or into the network?	Medium
	Are my business-critical networks and systems protected against distributed denial of service (DDoS) attacks?	Medium
	Do I have a process and platform in place to verify low-level patches before rolling them out to remote workers, to avoid any potential performance issues on their desktops	Low
	Do I have a data loss prevention strategy that can detect data leaving corporate boundaries or data exposed through remote staff?	Low



Detect

Detect cyber-attacks through analysis of alerts and behaviors.

Endpoint protection, detection and response

The most obvious place to detect and disrupt malware and ransom activities is on the endpoint. The growing attack-surface presented by a desktop, its value in terms of data and as a foothold, and users' mistakes have made the endpoint an increasingly popular target.

This has dramatically altered the network security paradigm. Where once it was sufficient to protect only the perimeter of a corporate network, this outdated approach is now no longer enough. Instead, **there must be a new, comprehensive, and ongoing focus on endpoint security**.

Endpoint detection typically takes the form of anti-virus or endpoint protection, detection and response (EDP/R), also known as "next-generation" anti-virus.

The value proposition of endpoint solutions is that they can detect the signatures of malicious files or processes, or even suspicious traffic or other behaviors. They then block the processes from executing and quarantine the suspicious files.

Most EDR work. But some work better than others.

In an experiment performed by our Security Research Center, EDR solutions were chosen and configured using the suggested industry-standard configurations and agents were installed in an up-to-date Windows 10 machine. Samples were run and the outcome evaluated by rThreat, an attack emulation solution. We could track if the file was executed, for how long, and if it was stopped. We tested both known and unknown threats that follow TTP standards, are mapped to the MITRE ATT&CK framework, and tested across the entire kill chain, to reflect authentic APT practices.

EDR 1

18/23 samples failed to execute.

5/23 samples executed for more than 10 seconds, 3 being obfuscated known samples, 2 stopped.

3/23 samples executed successfully and encrypted files, 2 obfuscated known samples and 1 known.

From this we can see that 18 samples were picked up by static analysis and 5 were missed. Of the 5 samples that could execute, 2 were stopped by behavioral analysis and 3 could run successfully.

EDR 2

18/23 samples failed to execute.

5/23 samples executed for more than 10 seconds (all different from EDR 1), all known, all stopped by behavioral analysis.

From this we can see that 18 samples were picked up by static analysis and 5 were missed but picked up by behavioral analysis.

Real-time behavior

Endpoint protection now needs to know how to pick up real-time malicious behavior on an endpoint, instead of just known malicious signatures and heuristics on the file system. This involves the continuous collection and processing of significant amounts of data from an endpoint.

EDRs have moved beyond prevention-only approaches on files to treating a file undetected by AV as unknown. This places the burden on the file to prove that its behavior is benign or not. By collecting the vast amounts of system activities, analysts had the opportunity to observe new malicious techniques, not yet seen in the wild, also known as zero-days. In fact, 77%[35] of successful attacks used fileless malware that older endpoint security tools could not prevent.

Since **fileless malware and similar types of advanced attacks can't be detected with only static rules or signatures**, you need to detect behavior anomalies on the endpoint. This behavior needs to be analyzed and correlated across other endpoints to separate the false positives from the real incidents. Without the right tools and competencies this can require a lot of effort.

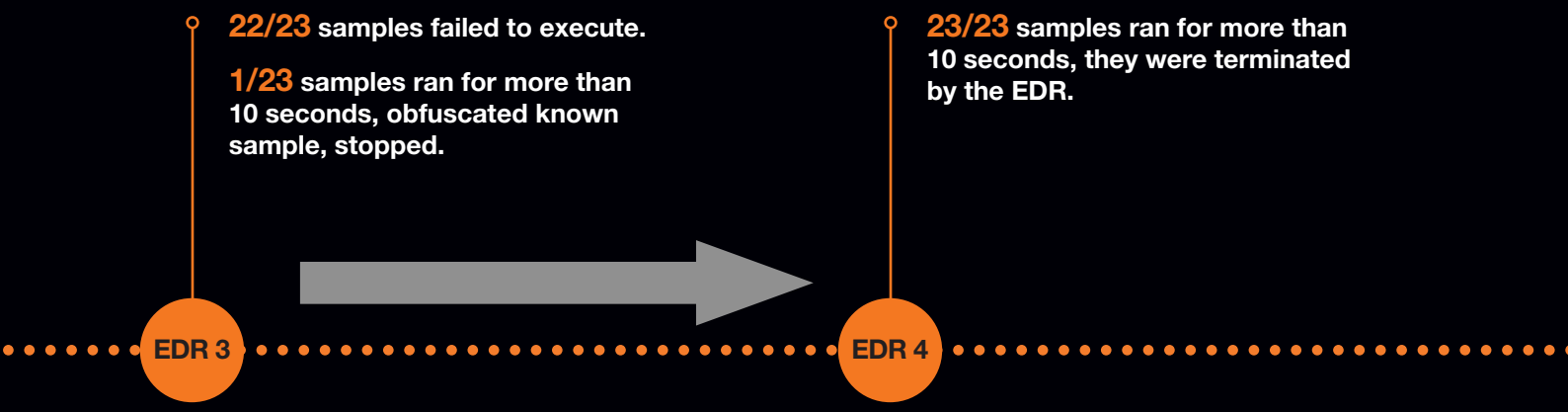
Once the investigation phase is complete, any critical incident will most likely also require rapid response actions. If the time from compromise, to detection, to remediation takes too long, it greatly increases costs and damage that could have been avoided.

Choose the right EDR

The choice of Endpoint Detection & Response (EDR) solution therefore plays a significant role in protecting your endpoint clients and servers from attack. There is a whole myriad of EDR solutions available, making it difficult to select the right one.

Ideally a solution will use multiple detection techniques, including signature-based, static IOCs, and behavioural analysis capabilities. The solution should be cloud-based, allowing for continuous monitoring and centralised collection of activity data, along with the ability to perform remote remediation actions, whether the endpoint is on the corporate network or outside of the office. In addition, the endpoint agent does not have to maintain a local database of all known IOC's but can query the cloud system for analysis of objects that it is unable to classify.

Our results for the 23 samples demonstrated the different approaches EDR solutions have, as they did not act in the same way and do not have the same signature databases, which did not come as a surprise. Of course, it is difficult to compare EDR solutions as there are so many factors in play and so many configuration options.



From this we can see that 22 samples were picked up by static analysis and the one that got away was detected by behavioral analysis.

From this we can see that this EDR configuration allowed for the execution of all the samples, but they were all promptly stopped. This solution seems to rely mostly on behavioral analysis.

EDR success lies in the details of the implementation

You also need to factor in the complexity of EDR solution deployment. It is comforting to believe they are fire and forget solutions, but this is often not the case. **You need to determine whether you have the in-house capabilities and workload availability to effectively deploy, manage and tune the solution**. If not, you should consider using a service provider to ensure optimum protection.

Whichever solution is chosen it needs to have coverage for all the major operating systems in use in your environment. We would recommend going with **a single solution that provides the benefits of standardized reporting, easier data correlation, and one place to manage alerts.**

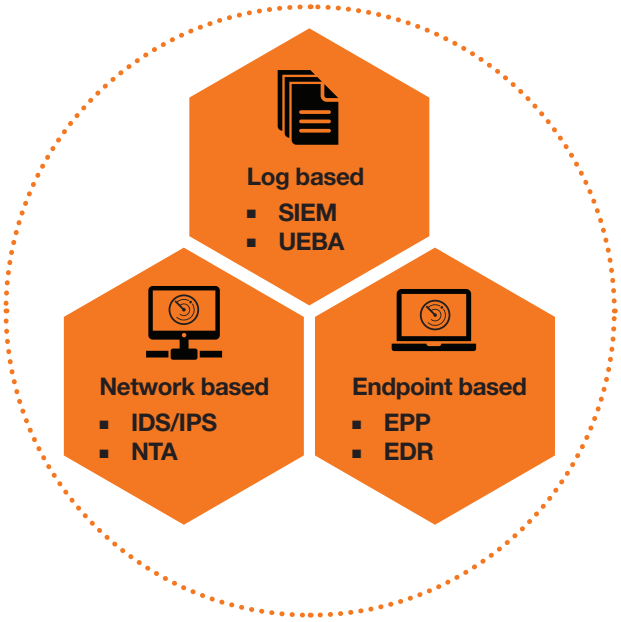
The emphasis is on detection and response

The lesson we learn from our penetration testing teams is that **all alerts must be investigated** even if the solution reports that it cleaned or blocked the activity. Malware and malicious activity should not be present in your environment, so identifying the source or cause of anything detected, even if it is cleaned or blocked, is critical as it could be a precursor to something more sinister.

Complement EDR with other forms of detection

Complementary to EDR we would also suggest deploying a network threat detection solution. **By analyzing the network traffic at certain choke points in your network, these solutions can identify threats that otherwise may fly under the radar**. Using behavioral analysis and AI capabilities can alert organizations to suspicious, malicious, or anomalous traffic flows and patterns. This extra layer of protection can identify threats originating from devices where it has not been possible to deploy an EDR agent or where an attacker has managed to bypass the EDR solution.

Some solutions also can perform automated remediation actions such as terminating connections, quarantining a device or cutting off a subnet to prevent lateral movement. An ideal solution should be deployed in on-premises, virtual and cloud network environments to provide total coverage and protection.



Log based
+ Good hub for collection of logs and alerts
- Not everything is logged

Endpoint based
+ Best detection where you can install an agent
- Threats present on devices without an agent

Network based
+ Detection across all network connected devices
- Activities that happen within an endpoint

Enterprise-grade operating systems, such as Windows, provide many event monitoring and log sources. A tool called Sysmon offers a means to tap into the Windows operating system and inspect certain events and behaviors[37]. These behaviors combined with some analytics can then be used to identify anomalous activity on an endpoint. **The Logging Made Easy (LME) project by the UK NCSC provides enough information for anyone to get going with their own logging and monitoring platform using freely available tools[38] .**

There is one big limitation with this type of approach where remote workers are concerned. The LME approach requires an active VPN connection to facilitate the log and event forwarding to the central collector. Without the VPN connection, no events can be passed onto the collector and no analysis or alerting can be performed.

Extended detection and response

A new product category has emerged over the past couple of years that is a culmination of existing products and ideas such as threat detection, investigation, and threat hunting. This is combined with telemetry of security and network tools, email security, identity and access management, cloud security, etc into a new product category called extended detection and response (XDR)[39].

These capabilities are very similar to what is currently associated with SIEM and security automation orchestration and response (SOAR) solutions. The distinction is that **XDR values the endpoint and events generated on it more than the large-scale data analytics approach associated with SIEM[40].**

There are two types of XDR solutions, according to Forrester. One being hybrid XDR that relies on integration with products from other vendors. Another approach is what Forrester defines as native XDR. This is a one-stop shop approach where the XDR solution integrates with the telemetry of all the security tools of a specific vendor. This approach will mean that one vendor is used for all aspects of the security deployment.

Dominic White is the Ethical Hacking Director at Orange Cyberdefense.

There's a weird fetish in infosec to "do the basics first". They tend to focus on prevention, with detection saved for when you have an expensive blue team and SOC. But what offensive work will teach you is that many of the things people think of as preventative controls are often only detective controls. Take AV, it's cheap to bypass in the short term, but sometimes a mid-day update could unmask part of your toolkit and trigger an alert.[36]

Detect checklist

Check	Control	Impact
	Do I have an endpoint security technology that does not just depend on signatures, but can also detect and respond to anomalous behaviors, even those that have perhaps not been recorded before?	High
	Do I have an appropriate endpoint security technology deployed across all the technologies in my environment that may be targeted, including server, workstations, and remote workers?	High
	Is my endpoint solution cloud-based (if appropriate), and does it allow for continuous monitoring and centralized collection of activity data, along with the ability to perform remote remediation actions, whether the endpoint is on the corporate network or outside of the office?	High
	Am I receiving relevant alerts from all my endpoints, regardless of where they are, and do I have the platforms and processes in place to assess those alerts within a reasonable time and initiate an appropriate response?	High
	Do I have the skills and resources to manage and monitor my endpoint security technology properly and respond appropriately to suspicious events and incidents when they are flagged?	High
	Given that not all EDR and AV are equal, have I invested enough in an endpoint security technology that weighs up sufficiently against contemporary threat vectors?	Medium
	Do I have visibility of attacks launched against my internet exposed services, such as VPN appliances?	Medium
	Do I have complementary technologies to detect and disrupt attacks at diverse points across the cyber kill chain? For example, am I able to detect anomalous login events on my VPN and remote access systems?	Medium
	Can we detect attacks launched from the remote local network directed at devices used by remote staff?	Medium
	Are my platforms and processes configured for a state of “continuous engagement”? Am I responding with enough suspicion and aggression to “suspicious” or “anomalous” events, rather than just waiting for the obviously catastrophic ones?	Medium
	Does my endpoint solution provide me with a single set of tools to gain visibility and protect all the technologies in my portfolio from one central interface?	Low
	Have I segmented my network, and isolated remote access traffic, enough to monitor remote user traffic where it hits my network?	Low
	Have I considered the strategic use of deception technologies, for example, on remote worker endpoints, or on the network where my VPN terminates?	Low

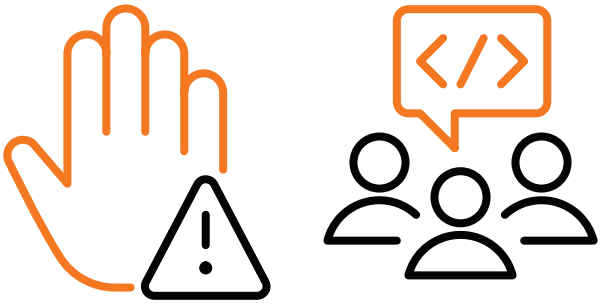
Respond

Respond to an incident knowing you have prepared and are ready to restore business operations.

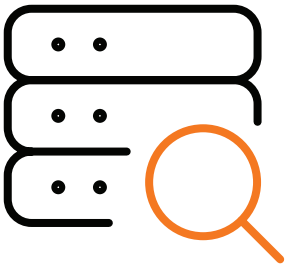
Stay calm and keep to the plan

If the worst should happen and you do fall foul of an attack, the first key thing is to remain calm and not panic or make rash decisions. Now is the time to **initiate your incident response plan and get control of the situation**. Ideally, you should have a retainer in place with a CSIRT who can help coordinate and provide much-needed additional manpower on a 24x7 basis. If so, they should be engaged at the earliest opportunity.

Your incident response plan needs to take remote workers into account. **Ensure you and your CSIRT partners have a plan for dealing with incidents on one or more remote endpoints**, where you may not be able to get physical or even remote access to the endpoint.



1



2

Stop the spread

Being physically removed from a device that has possibly been compromised can be challenging. **The standard playbook to investigate a compromised device is quite different for a remote device**. Some tools allow for remote investigation and analysis. A remote device that is under investigation must be quarantined like any other. The process for this may be very different than normal since you will need remote access to the device while investigating the incident.

Some vendors include remote response and investigation capabilities in their endpoint detection and protection solutions. Alternatively, you can use free tools such as Google's Rapid Response (GRR) to perform initial assessment on a remote host[41]. These tools are not full-on forensic tools, but merely tools that allow you to get a sense of the state of the remote host for you to decide on the next course of action.

Part of the remote quarantine can involve isolating the host using a specific VPN profile. This VPN profile can enforce a full VPN tunnel that forces all network traffic to a dedicated and special purpose network segment. It allows responders to analyze and observe network traffic.

Another approach is to disconnect the host from the wired and wireless networks physically. However, this makes little sense for a remote device as there is no way for someone to remotely access it. In this case it may make sense to power off the device and ship it to the incident response team for investigation, but this action may destroy some evidence.

3

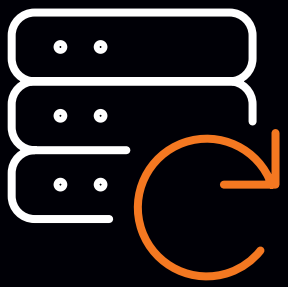
Keep people informed

Clear, open, and honest communication is vital, both internally and externally. Internally, staff need to be made aware of what has happened, what is being done about it and how they can help. If staff understand what's happening, they will be less likely to work around measures you put in place to recover and improve security, which may otherwise appear obstructive to their work.

Ensure you have a channel open to your legal team to clearly understand what you may and may not say regarding a potential breach.

Externally, it is important to take control of the narrative from the outset. A clear, strong public statement should be issued explaining what happened, how much you currently know and what you are doing about it. The appropriate regulatory bodies and law enforcement agencies should also be notified. Trying to keep the incident secret will only serve to make you look dishonest and inept. The reality of the situation will probably come out in the end. Depending on the type of incident, the attackers could release details of the incident, such as an incident involving ransomware.

4



Establish a trustworthy beachhead

While it's feasible to detect and remove specific malware or hacking tools from a computer, it's almost impossible to assert that a network is "clean" after it's been infected or compromised. To fully recover from the attack, and completely evict the attackers from your environment, you should seriously consider scrapping everything and rebuild the affected networks from scratch.

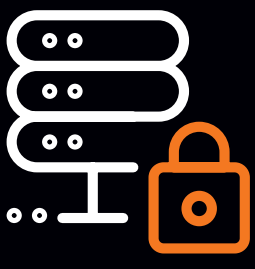
You should even go as far as recreating your Active Directory domain if domain controllers were compromised. While this can clearly be a daunting undertaking, it is the only way to 100% know that the attacker has been removed from your networks, as often it is not possible to fully know where an attacker has been and what they have done.

Rather than spending the time trying to work that out it will likely be quicker, easier and cheaper to rebuild everything, you also have the opportunity to implement better security controls during the build process. This is where your secured backups become a critical component as they should allow you to get mission-critical systems up and running quickly, providing they have not been compromised.

5

Recovery is a marathon, not a sprint

Full recovery from a serious incident can take a long time, and the response effort will claim a huge toll on your team. The well-being of any staff involved in the recovery process should be considered. They will likely be working long hours and care should be taken to ensure they get adequate rest and time off to avoid burnout. This is again where a CSIRT can be crucial as it can provide the additional manpower needed to allow the rotation of key staff required in the recovery process.



Hope for the best, plan for the worst

Despite your best efforts, **you need to plan for an attacker slipping your defenses**. In the worst case, you will only be aware of this after it has already happened, and you may have to respond to the crisis using IT platforms that are crippled or destroyed. Given the possibility of such a nightmare scenario, however remote it may be, here are nine steps to plan for in advance.

1. Secure your backups

Store them offsite and segmented where they will be shielded from destruction in the case of a compromise.

2. Have a response team

Ensure that your response team is well defined, authorized and equipped with what they may need in a disaster.

3. Have a plan

Your response team should be working from a clear playbook that covers as many eventualities as you can anticipate.

4. Plan for reinforcements

It is highly unlikely that you will be able to respond and recover from an extortion incident without the help of expert incident responders and other professionals. It therefore makes sense to have security and IT support vendors selected ahead of time, and perhaps even to have commercial and contractual frameworks in place, in case you need to call on them in a crisis.

5. Keep your contact book updated

You may need to reach out to any number of people internally and externally, including business leaders, incident responders, insurance, law enforcement, suppliers and providers, your legal and communications teams and more. Ensure that you have their latest contact details readily available, even if you can't access your workstation or mobile phone.

6. Have a communications plan

An extortion attack very quickly becomes public, and there is very little you can do to prevent employees, the press and other outsiders from speculating that you may be a victim. Rather than hide the incident, consider a pre-planned communications strategy designed to reach all your stakeholders, both internal and external.

Think about the level of transparency you are comfortable with and the kind of wording you will use. Assign clear responsibilities and an authorization process that includes stakeholders from IT, security, legal and communications. You also need to think about the channels you will use, as traditional communications platforms like your website, email or social media might not be available to you.

And don't forget your internal stakeholders. Communicating clearly, frequently and transparently with staff is the best way to make them part of the solution during a crisis, rather than part of the problem.

Please see our **Beating Ransomware** paper for guidance on preparing for ransomware incidents.

Respond checklist

Check	Control	Impact
	Do I have a clearly documented, reviewed, and communicated incident response plan in place that anticipates the worst-case of a successful attack?	High
	Do I have clear plan for isolating or disconnecting computers from the network in the event of a compromise? Does that plan extend to my home workers also?	High
	Do I have a clear communications plan for keeping IT staff, leadership and employees informed about the incident and my response? Do I have a backup plan in case “traditional” channels like email are impacted?	High
	Do I know the quality of my backups, and whether they are reliable and complete? Have I tested recovery from backups to develop familiarity with that process and gauge how long it may take?	High
	Have I gathered intelligence about the experiences of other companies that have fallen victim to cyberattacks, and have I incorporated those lessons into my plan?	Medium
	Have I engaged with my legal, communications and marketing teams regarding a strategy for informing customers and the public about an incident?	Medium
	Do I have a retainer in place with a 24x7 CSIRT who can help me assess the impact, coordinate a response needed additional manpower during the recovery efforts? Does that agreement take remote worker endpoints into account?	Medium
	Has my team had the opportunity to “practice” the plan as a tabletop exercise or under real-life exercise?	Medium
	Do I have a plan that will enable me to isolate and triage remote devices before launching a fully-fledged forensic investigation?	Medium
	Do I have a plan to replace devices associated with remote staff to ensure as little impact as possible to the business?	Medium
	Do I have a strategy for how I will source, manage, and remunerate the human resources that may be required for an intensive, multi-week compromise recovery effort?	Low
	Do I have an agreement with my legal team, financial team, risk team, and leadership about the eventuality of having to pay a ransom, and the basis on which a decision to pay might be made?	Low
	Have I engaged with my financial team, legal, risk and leadership about the possible short-term costs of a breach, and funds and cryptocurrency might be obtained in the worst-case scenario?	Low

Conclusion

Building a business with resilience means a lot of different things today. It means having a good sales pipeline, effective marketing, a healthy revenue stream and motivated staff who are trustworthy even when times are tough. These business elements depend on a steady flow of information and the ability to extract, transform, correlate, amend, and distribute new information to stakeholders in a trustworthy, timely and accurate manner. Doing business without computer systems is near inconceivable and business relies heavily on information systems to support it in achieving its goals.

The ability to minimize the impact on business operations in response to a change in work policy due to external factors, such as a pandemic, is an excellent demonstration of resilience. It's sometimes impossible to foresee events, and that can catch us all off guard. COVID-19 was one such event, and we've all been pressed to execute an unreasonably fast transition that has sometimes required compromises and uncomfortable shortcuts. The costs of assuring the security of our new remote workforce were deferred into the future, and that's totally "ok". But the future resilience of our businesses requires that we assess our security posture in light of emergent new threats, tally up our debts, and pay those down… before someone comes to collect.

Protecting the confidentiality, integrity, and availability (CIA) of any information system is key to business success. While some aspects of the CIA triad may be more important to one business than to others, it is unlikely that any can forego a single aspect and with no business impact.

There's a lot to be done to fully protect our newborn remote workforce. **An intelligence-led approach will help guide teams tasked with protecting business systems to prioritize actions**. The threat landscape is constantly changing and that means that businesses must keep abreast of significant changes to ensure that their risk exposure remains within an acceptable threshold. To do so they must have the latest information about tactics and techniques used by attackers and what the most effective means are to detect attacks and to limit risks associated with a successful attack.

An increase in remote work has exposed businesses to several new dynamics that bring new challenges to the table, from a support point of view as well from a cybersecurity point of view.

The good news is that no magic is required. In this paper, we recommend a simple plan that is inspired by the CIS Top 20 controls and the NIST cybersecurity framework. We're in a war against threats, not a battle, and **every additional control you implement will raise the cost for an attacker and improve your resilience.**

Do the basics right by running a proactive vulnerability management program, reduce the exposure of accounts with administrative privileges, and monitor remote systems. Supplement these with **endpoint detection and protection** solutions, **review and harden configuration** of software such as VPN clients to ensure that remote staff receive all the protection offered by mature enterprise products, use i**ndustry-recognized identity providers backed by multi-factor authentication**.

Finally, ensure that your people are properly trained and keep them well informed regarding the tactics and techniques of current active threats. Prepare for the worst by having an incident response plan that can help remote staff and make sure you regularly practice this to ensure staff is familiar with the drill.

Orange
Cyberdefense

orange™

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe.

As Europe's go-to security provider, we strive to build a safer digital society. We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security. Distributed across the world we have:

- **250+ researchers and analysts**
- **18 SOCs**
- **11 CyberSOCs**
- **4 CERTs**
- **Sales and services support in 160 countries**

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors. We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community, Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences including, Infosec, Manchester DTX, RSA, 44Con, BlackHat and DefCon.

If you would speak to us about securing your remote workforce, feel free to contact us at **info@orangecyberdefense.com** or visit our Managed Detection and Response page: **https://orangecyberdefense.com/global/all-services/detect-respond/**

We hope you found this whitepaper insightful. Stay safe!

Visit us at: www.orangecyberdefense.com

Twitter: @OrangeCyberDef

Sources:

1. https://www.ipsos.com/en-us/world-work-global-study-online-employees-shows-one-five-17-work-elsewhere
2. http://allthingsd.com/20130222/physically-together-heres-the-internal-yahoo-no-work-from-home-memo which-extends-beyond-remote-workers/
3. https://www.huffpost.com/entry/the-future-is-happening-now-ok_n_6887998
4. https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/why-are-some-companies-moving away-from-telework.aspx
5. https://hbswk.hbs.edu/item/18-tips-managers-can-use-to-navigate-covid-s-rising-waters
6. https://hbr.org/2020/12/the-pandemic-is-widening-a-corporate-productivity-gap
7. https://hbswk.hbs.edu/item/18-tips-managers-can-use-to-navigate-covid-s-rising-waters
8. https://hbr.org/2020/12/the-pandemic-is-widening-a-corporate-productivity-gap
9. https://www.rackspace.com/solve/cloud-beyond-covid-19-cloud-adoption-will-see-businesses-emerge-stronger
10. https://www.channelnewsasia.com/news/business/microsoft-earnings-rise-as-pandemic-boosts-cloud-computing-xbox-14049072
11. https://www.republicworld.com/business-news/international-business/alphabet-sets-record-profits-revenue-surges-34-percent-in-q1-as-users-stayed-online-amid-covid.html
12. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
13. https://www.theverge.com/2020/6/4/21279633/laptop-pc-shortages-supply-chain-coronavirus-covid-19-pandemic
14. https://corpgov.law.harvard.edu/2020/09/07/cyber-risk-and-the-corporate-response-to-covid-19/
15. https://www.cisa.gov/telework-reference-materials-home-worker
16. https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets
17. https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework
18. https://www.opensignal.com/2020/03/30/analyzing-mobile-experience-during-the-coronavirus-pandemic-time-on-wifi
19. https://media.defcon.org/DEF%20CON%20China%201/DEF%20CON%20China%201%20presentations /DEF%20CON%20China%201.0%20-%20Workshops/DEF%20CON%20China%201.0%20-%20 Philippe-Delteil-WiFi-Hacking.pdf
20. https://papers.mathyvanhoef.com/dragonblood.pdf
21. https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf
22. https://www.sans.org/blog/insights-6th-annual-sans-security-awareness-report-managing-human/
23. https://cybersecurity.att.com/blogs/security-essentials/incident-response-methodology-the-ooda-loop
24. https://www.theregister.com/2021/02/18/cve_exploitation_2_6pc_kenna_security/
25. https://en.wikipedia.org/wiki/Box_plot
26. https://www.knowbe4.com/press/q4-2020-knowbe4-finds-work-from-home-related-phishing-email-attacks-on-the-rise
27. https://metabase.dip.secdata.net/question/575
28. https://en.wikipedia.org/wiki/Microsoft_System_Center_Configuration_Manager
29. https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview
30. https://twitter.com/singe/status/1382368147869679620?s=20
31. https://gdpr-info.eu/art-15-gdpr/
32. https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide
33. https://www.veracode.com/security/man-middle-attack
34. https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/
35. Ponemon 2018 Endpoint Security Statistics Trends
36. https://twitter.com/singe/status/1382368147869679620?s=20
37. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
38. https://www.ncsc.gov.uk/blog-post/logging-made-easy
39. https://go.forrester.com/blogs/xdr-defined-giving-meaning-to-extended-detection-and-response/
40. https://www.zdnet.com/article/xdr-defined-giving-meaning-to-extended-detection-and-response/
41. https://github.com/google/grr

Orange Cyberdefense

orange™