Orange
Cyberdefense

Case Study

Aalborg Municipality protects its e-mail and collaboration environments with a powerful, cost-effective Check Point Harmony solution delivered by Orange Cyberdefense

Business challenge

Seeking consistent, outstanding e-mail protection
The Aalborg Municipality IT team supports users and systems across mor than 800 locations. Approximately 17,000 users work from a wide range of devices. In all, the IT team manages 19,000 individual and shared mailboxes—as well as the municipality's Microsoft 365 solution. Users access Outlook e-mail and Teams collaboration applications either directly from their devices or through a browser on tablets, mobile devices, and thin clients. Regardless of device, everyone is targeted by high volumes of phishing and Business Email Compromise (BEC) cyberattacks. Users required continuous assistance in determining whether to open e-mail messages, creating a burden on the support team.

The municipality had been using Microsoft Defender for e-mail security, but when it was time to renew the license, coverage terms had changed. Tablet, thin-client, and mobile users no longer had the same level of protection as users who accessed e-mail directly from desktop systems. The subscription cost also increased significantly.

"First, we needed to ensure consistent e-mail security for all users while remaining cost effective," says René Ellergaard, Systems Engineer at Aalborg Municipality. "At the same time, we wanted to relieve the burden on our support team by making it easier for users to manage quarantined e-mail. We began considering new e-mail security solutions."

"We evaluated several solutions, including Microsoft, and Orange Cyberdefense, our Managed Security Service provider, told us about Check Point Harmony Email & Collaboration. After talking with other partners and doing further research, we decided to implement a Proof of Concept", says René Ellersgaard.

Solution

Easy setup and use
Working with Check Point Professional Services, Aalborg Municipality initially tested Harmony Email with 80 users and mailboxes. One week later, they expanded the test to 2,000 users and then to 4,000 users. After four weeks everyone across the municipality was enrolled.

Harmony Email & Collaboration provides complete protection for Microsoft 365, as well as Google Workspace and other collaboration or file-sharing apps. It blocks advanced phishing, malware, BEC, account takeover, and

Organization

Aalborg Municipality is located in the North Jutland Region of Denmark and is the country's fourth-largest city.

Challenge

- Ensure outstanding, consistent e-mail protection across all users and devices
- Simplify e-mail security for users
- Integrate with Microsoft 365 and ITSM solution

Solution

- Check Point Harmony Email & Collaboration
- Check Point Professional Services

Benefits

- Deployed advanced e-mail and collaboration protection across municipality in just four weeks
- Integrated seamlessly with ITSM system and reduced daily support tickets from 25 to 2
- Increased security visibility and awareness for users and support teams

"I would definitely recommend Check Point Harmony Email & Collaboration. It's easy to deploy and use and we're looking forward to continuing implementing new features."

René Ellersgaard
Systems Engineer

Aalborg Municipality

ransomware attacks before they reach users' inboxes, and it protects sensitive business data from leaving the organization. Organizations typically experience a 99% reduction in phishing attacks that reach mailboxes.

"Implementation went great - we were up and running within a day. Over the next few weeks as we expanded coverage, we also integrated Harmony Email with our ITSM solution. With a few tweaks, Harmony Email worked seamlessly in our organization", says René Ellersgaard.

Seamless integration
Harmony Email & Collaboration integrates with Aalborg Municipality's ITSM product to automate review of suspicious e-mails. When users are notified that they have a quarantined e-mail, they can decide to release it or not. If they decide to release the e-mail, just a click automatically creates a ticket in the ITSM. A support team member looks at the questionable e-mail and decides whether it is safe to release.

"ITSM integration is the key to our success. "It gives users the power to decide whether to accept an e-mail or not which greatly reduces the number of calls for support and enables quick response. The integration also gives us the opportunity to have a dialog with our end users and provide additional education on threats", says René Ellersgaard.

Benefits

Protection for everyone
Harmony Email now protects all Aalborg Municipality's users, whether they use Outlook e-mail, web access without an Outlook client, or Microsoft Teams. Built-in AI capabilities continuously scan inbound emails using contextual analysis, anomaly detection, and anti-phishing algorithms to detect BEC and employee impersonation. Harmony Email then creates custom threat profiles by learning communication patterns, relationships, and historical e-mails within users' inboxes.

Reduced support time
Before Harmony Email, the support team had little visibility into threats while having to make decisions about which e-mails to release. Now the team now can see the types of e-mails coming in and is highly aware of current spam campaigns and the current threat landscape.

Increased awareness
As the AI capabilities of Harmony Email learned the Aalborg Municipality's e-mail patterns, users and the support team gained valuable awareness of e-mail safetyand current cyberthreats. As a result,users are more aware of sensitive data that citizens send in e-mails to the municipality. They have begun helping citizens understand the risks of sending sensitive data in e-mails and suggesting better ways of sharing that data.

Business relevance

What types of organizations/ companies would benefit from a similar solution?
According to René Ellersgaard Checkpoint Harmony Email and Collaboration is particularly relevant for companies and organizations that have a high degree of confidential and sensitive data, such as personal information about customers, citizens or patients. It can be companies of different sizes within different industries, e.g. the financial and healthcare sectors, retail trade, manufacturing companies, public institutions and many others.

"I would like to highlight three important factors that have made the cooperation with Orange Cyberdefense successful:

Firstly, we have experienced a close collaboration with a committed partner who has a good understanding of our organization and our needs. This means that the solution has been adapted precisely to our requirements and wishes.

I also want to mention the quick response. Orange Cyberdefense has always been available when we had questions or problems – and they have solved all challenges with great expertise and efficiency.

Finally, I would like to emphasize that everything has always been followed through with no loose ends. Orange Cyberdefense has been dedicated to ensuring that our implementation has been carried out to our full satisfaction and theyhave always been willing to go the extra mile to ensure that our requirements were met.