Orange
Cyberdefense
Ahead of the Storm

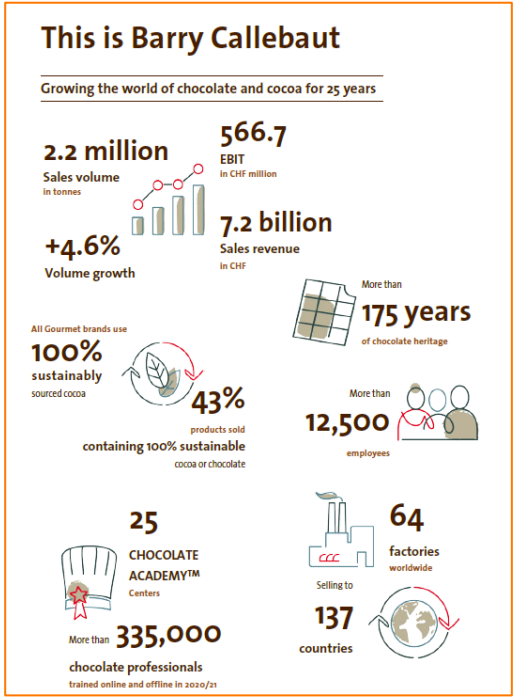
Cyber threat resilient backups

Amol Gangras,
Global Hybrid Datacenter Services Manager
Barry Callebaut

About Barry Callebaut

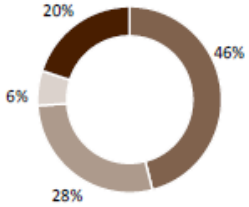
Headquartered in Zurich, Switzerland, the Barry Callebaut Group is the world's leading manufacturer of high-quality chocolate and cocoa. We are the heart and engine of the chocolate industry and our mission is to be number one in all attractive customer segments. We are a business-to-business company, fully integrated with a strong position in cocoa-origin countries.

Barry Callebaut:
Employs more than 12,000 people operating out of more than 30 countries
Operates more than 50 production facilities
As per 2020/21 Annual results, generating Sales revenue of CHF 7.2 billion, up +8.7% in local currencies (+4.6% in CHF)
Has comprehensive competencies in the art of making chocolate and cocoa products — from sourcing and processing cocoa beans to producing the finest chocolates, including chocolate fillings, decorations and compounds



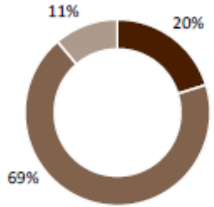
Sales volume by Region

In tonnes	
EMEA	997,324
Americas	610,133
Asia Pacific	138,396
Global Cocoa	445,719

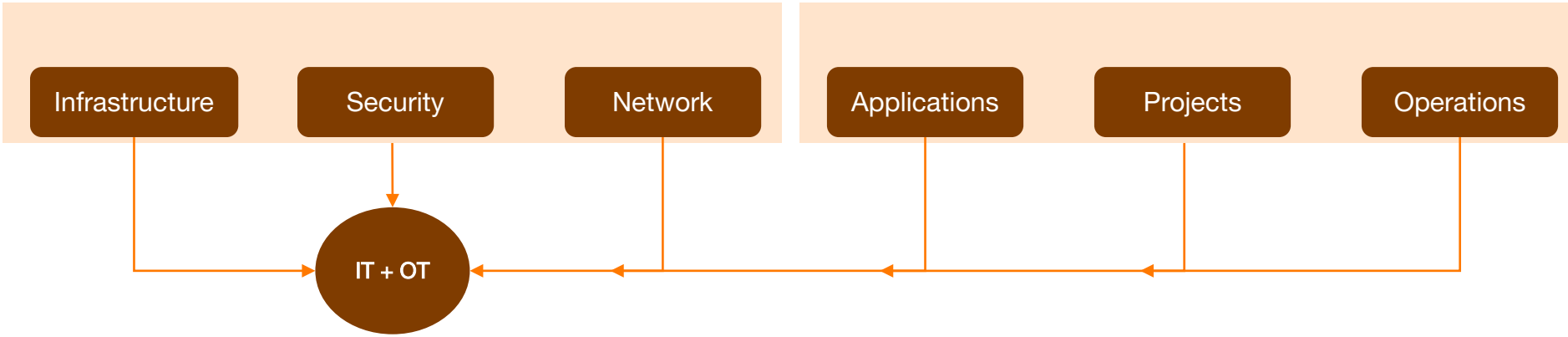


Sales volume by Product Group

In tonnes	
Food Manufacturers	1,498,496
Cocoa Products	445,719
Gourmet & Specialties	247,357



Barry Callebaut IT landscape at a glance



Strong architecture footprint

- Global twin datacenter (fully mirrored) PaaS model, hosting 80% of SAP backbone
  - Today limited analytical applications in public cloud (example SAP)
- Harmonized local data center hosting MES on hyper-converged highly resilient clusters, standardized operations
- 130+ sites fully connected with global SD-WAN

The only missing part was ‘data protection’

The challenge

Scale
- Too many sites/data
- Insufficient performance
- SLAs were getting breached

Manageability
- Global overview: difficult
- Complex lifecycle management

Future proof
- Not catered toward modern requirements
- Limited cloud protection capabilities

Security
- Backup environments were a large attack vector
- Final bastion

Rethinking remote back-up

Technical requirements

- Efficiency
- Performance
- Global
- Future-proof

Partner requirements

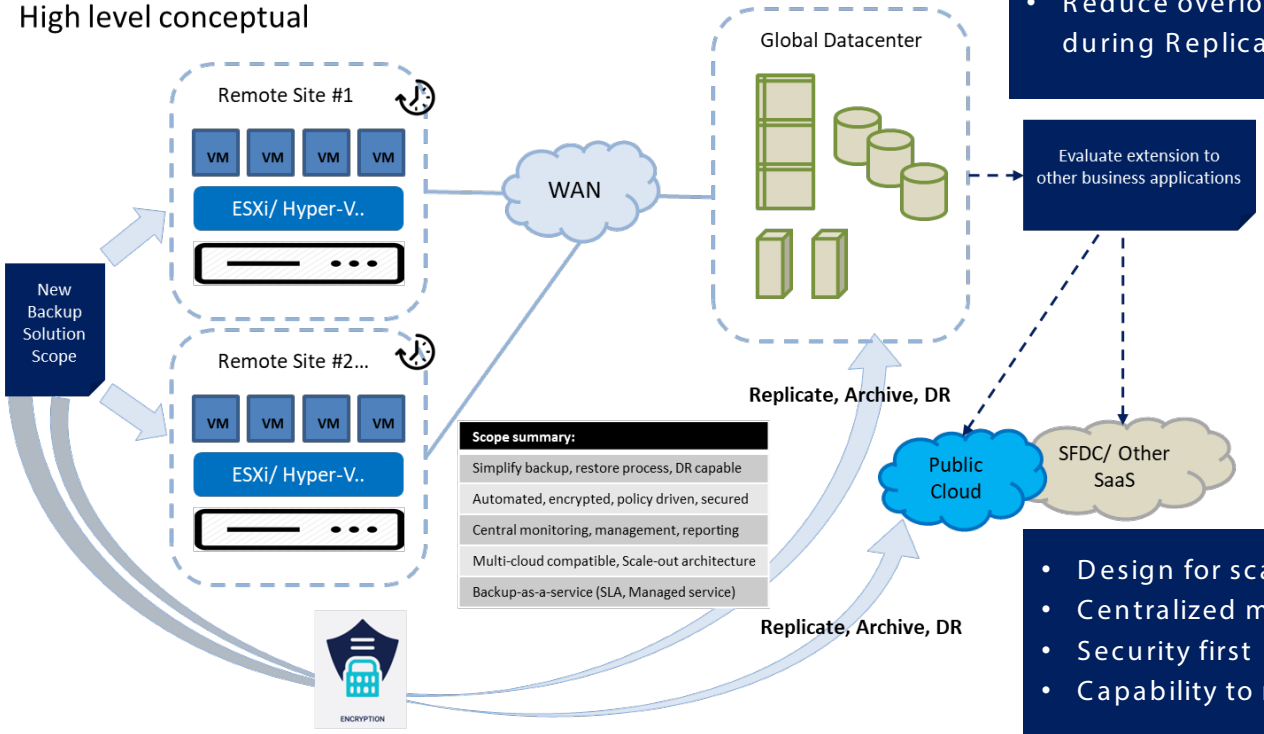
- Focus on security
- Operational expertise
- Global capabilities
- Managed services
- Technology experts

Vision

Architecture principles:

- End-to-end data encryption (at source, in transit & REST)
- Extend solution to other business apps where possible (public cloud, SaaS,..)
- Reduce overload on WAN, optimize bandwidth during Replication

High level conceptual



- Design for scale
- Centralized management
- Security first
- Capability to restore complete sites

Common factors in recent ransomwares attacks

1

Exploited vulnerabilities

Have a patch management and vulnerability management strategy

2

Keys to the kingdom stolen

Have a Privileged Access Management (PAM) strategy

3

Compromised backup

Have a business continuity and disaster recovery strategy

4

Long business impact

Have an incident response strategy

Challenges	Co-managed backup and restore service
Scalability (number of sites and amount of data)	Designed for limitless scalability from the ground-up.
Disaster recovery requirements not met / off-site backups not for every site	Provide off-site backups in combination with live-mount capabilities
Platform management is time consuming	Orange Cyberdefense services combined with vision on data recoverability
Only basic reporting	Rich and automated reporting functionality
Future proof	Gartner 2020 MQ for data center backup and recovery solutions.
Ransomware recovery!	Detect anomalies, analyze threat impact and accelerate recovery in combination with CSIRT services

SWOT analysis of the implemented service

Strengths:

- Innovation-driven | Gartner recognized Leader & Visionary
- SaaS platform for global insight and management with Global automated reporting capabilities
- Scale-out solution with API first strategy
- SLA & policy-driven backups
- CSIRT retainer, ransomware remediation

Opportunities:

- Free up FTE for business-oriented projects
- Enables customer to venture further into public cloud
- Gain alerting, insight on impact, and easy remediation after cyberattack

Weaknesses:

- Limited support for older (\"legacy\") operating systems for workloads
- Challenging to predict cloud spend

Threats:

- Network topology/failover should be carefully planned to enable DR-scenarios!

The situation today

- 100+ sites protected worldwide
- 4749 backups per day
- Diverse workloads being protected
- Globally defined SLAs
- Automated backup scheduling

Tasks

All clusters

	48 In Progress	4,749 Completed
6 Failed	4,908 Scheduled	12 Canceled

Events

in the last 24 hours

	364 Replication events completed out of 364 0%	1,898 Backup events completed out of 1905 -0%
354 Critical system events	427 Archive events completed out of 447 -3%	1 Anomaly event detected Powered by Ransomware Investigation

Compliance Overview

Past 24 hours

- 1.3k In compliance
- 7 Out of compliance

Protection Overview

- 1.3k Protected
- 71 No SLA
- 1.1k Do Not Protect

Data Centers

93 Connected 2 Disconnected

The situation today

- 100+ sites protected worldwide
- 4749 backups per day
- Diverse workloads being protected
- Globally defined SLAs
- Automated backup scheduling
- Integrated anomaly detection

DATA PROTECTION ›

Protected Objects

1.4k
Objects

Data Centers

93 Connected 2 Disconnected

Past 24 hours

Cloud

You don't have any cloud accounts added to Rubrik

SETUP

SaaS

Use Rubrik to protect your Microsoft 365 apps

READ MORE

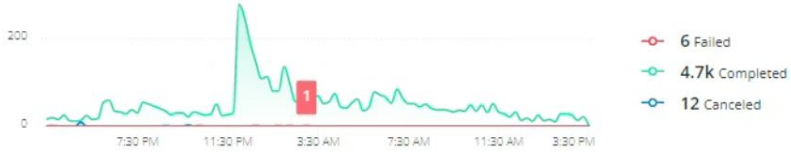
Data Center

1.4k -7 Objects

14.1 PB -217.5 TB

Tasks

All clusters



6 Failed
4.7k Completed
12 Canceled

RANSOMWARE INVESTIGATION ›

Pipeline health 100%

1.2k
Objects

1
Anomaly event

INVESTIGATE

DATA DISCOVERY

Data Discovery is an application to discover, classify, and protect sensitive data, such as credit card numbers, social security numbers, or ITIN, across data sources and locations.

READ MORE

APPLICATION RECOVERY ›

The situation today

- 100+ sites protected worldwide
- 4749 backups per day
- Diverse workloads being protected
- Globally defined SLAs
- Automated backup scheduling
- Integrated anomaly detection
- CSIRT

Dashboard

Status

in the last 24 hours

1.2k
Objects

1
Anomaly event

INVESTIGATE

Pipeline

in the last 24 hours

100%
Healthy

1741
Backups Completed
4 Failed

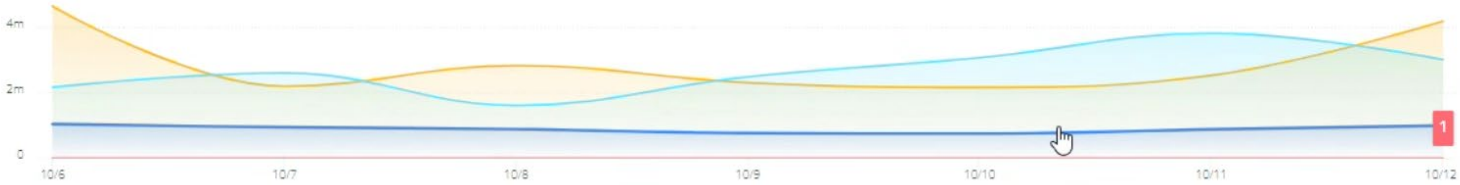
2966
Indexed
6 Failed

1263
Analyzed

File Analysis

All SLA Domains | All Clusters | All Object Types | Past 7 Days

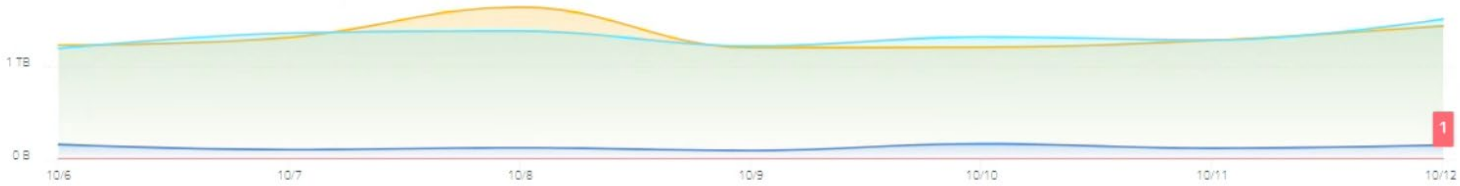
Oct 6 - Oct 12



0 Suspicious Files
20.8m Deleted Files
18.8m Added Files
6.3m Modified Files

Data Analysis

Oct 6 - Oct 12



0 B Suspicious Data
9.32 TB Deleted Data
9.28 TB Added Data
902.84 GB Modified Data

The benefits

Collab between global experts

- Capability to combine agility with global services
- References & know-how on different levels: design/deploy/managed

Proven managed services

- Opportunity to align with specific BC objectives
- Flexibility to balance level of managed services
- Extension of our own team

Recover Capabilities

- Regular fire drills
- Capable to restore full sites
- Ransomware & anomaly detection + CSIRT

Focus on cybersecurity

- Choice for innovative and specialized solution
- Industry recognition e.g. Gartner MSS / Forester Wave / IDC

KPI's

- Reporting on missed Rubrik SLA's: 99,88% successful per quarter
- Successful rate, restores to same source: 99% per quarter Details incorporated in presentation
- Customer ticketing portal uptime : Uptime 99.88% / quarter
- Telephone call pickup time: Within 60 seconds: 1 failure/quarter
- CSIRT service : An Incident Manager will be assigned within a max. of 4 hours of initial triage. Initial triage will be initiated via Cybersoc, available 24x7.
- Anomaly detection : Within 24h reported
- Monthly health check reporting by Design Authority (capacity runway + software versioning)
- Percent of lost or corrupted backup data : 0%
- Replication Success Rate from onsite to cloud storage: 100% success rate

Backup service KPI’s

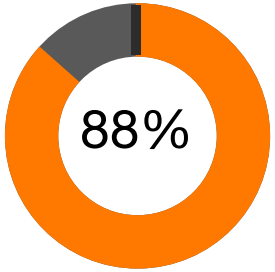
Reporting on Rubrik SLA’s

Successful rate, restores to same source

Customer ticketing portal uptime

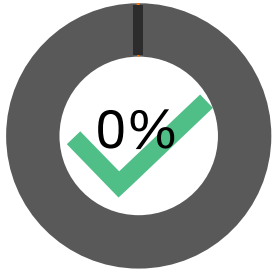
Telephone call pickup time

CSIRT service



Anomaly reporting

Monthly health checks



lost or corrupted backup data

Replication Success Rate from onsite to cloud storage

Upcoming initiatives

- Migrate more applications to public cloud
- Redefine crown jewels
- Revisit BIA
- Enhance incident response process (cyber events)
- PAM
- Azure AD
- Cloud security posture management
- Enhance OT security

Orange
Cyberdefense

Thank you

Amol Gangras, Global Hybrid Datacenter Services Manager
Barry Callebaut

October 21, 2022

orange™