Extensive Security DATA BACKUP & PROTECTION

In the digital age, there is no 100% protection, but it is vital for organisations to consider all the possible measurements for data protection including solid processes around cybersecurity, cloud security, identity access management, and risk management.

A solid backup setup not only protects against cyberattacks, but also ensures data loos prevention and recovery, in case the information is accidentally deleted, the work device gets stolen, or the hard drive gets corrupted of fails.

Besides our regular data backup and security procedures (data storage, access and Firewall), our experts recommend companies to also consider:

1. EXTERNAL BACKUP
A local replication device that can assure a higher protection of your data in the event of catastrophic failure and outrage.

2. SOPHOS CYBERSECURITY (MDR)
A 24/7 Threat Detection and Response service.

1. EXTERNAL BACKUP DEVICE

01 HOW IT WORKS

During night time, we run a backup of all our database servers (HANA and SQL). This backup is stored on a dedicated backup server in another network.

To provide even more protection, we offer the optional possibility to store this backup also at the customers' location (at their choice).

The backup is transferred through a push pull system between the data center and a storage.

The storage is based on a sinology and equipped with a special connection tool that establishes a secured and encrypted tunnel between the storage and the backup server.

No firewall rules or any other configuration are needed. It is plug and play. The device can be placed anywhere. You only need an internet connection. Any home used router or ISP connection with DHCP may be used.

02 REQUIREMENTS

– Internet Connection with minimum bandwidth of 25 Mbit, 50 Mbit are recommended, 100 Mbit is optimal
– 1 GB Port on the router or switch. Wifi is NOT an option.
– 110/220V power outlet with 2 Amps. Different plug types Nema, EU et care available.

03 TECHNICAL INFORMATION

– storage system with RAID 1
– 2x 1 GB Port
– different sizes are available from 4 TB to 10 TB
– retention policy starting at 10 day up to customers choice (depends on the device space size) – system based on Synology NAS devices

From July 1st 2023 our policy changes. Only for customers with the "extensive security" package, we guaranty a valid backup for ransomware attacks. All other customers are excluded from our cybersecurity insurance and may suffer from data loss, if one of our data centers is attacked. Furthermore, if the root source of the attack is the customer network, the customer becomes liable for the damages if the MDR package is not booked.

2. SOPHOS CYBERSECURITY MANAGED & RESPONSE (MDR)

INTRODUCTION

Sophos Managed Detection and Response (MDR) is a 24/7 managed threat protection, detection, and response service.
The MDR service tier provides analyst–led threat hunting, investigation, and threat containment so attacks are interrupted to prevent spreading.

Sophos Firewall is already included in our datacenter, also Intercept X and Server protection for all our data center services.
The customer may book Intercept X and Server Protection for their local network, managed by our experts as well.

Threat Hunting

Proactive 24/7 hunting by our elite team of threat analvsts. Determine the potential impact and context of threats to your business.

Incident Response

Initiates actions to remotely disrupt, contain, and neutralize threats on your behalf to stop even the most sophisticated threats.

Continuous Improvement

Get actionable advice for addressing the root cause of recurring incidents to stop them for occurring again.

XDR–Enabled

Sophos XDR is included so Sophos analvsts can detect and neutralize security threats from all available data sources while you can identify and remediate IT issues across estate.

LICENSING

The MDR service for SAP cloud hosting is included in our contracts. For local devices it starts at:

1 **Central Intercept X Advanced**

with XDR as well as 3rd party endpoint compatibility

2 **Central Intercept X Endpoint Advanced**

with XDR, 'Built for both cybersecurity analysts and IT administrators.
Includes all features in Central Intercept X Advanced, as well as additional, powerful features for detection and remediation.

Ask and answer business critical IT operations and threat hunting questions with Live Discover and respond remotely with Live Response.
Includes 30 days of storage in the Sophos Data Lake and enables queries across the data collected from any Sophos XDR–ready product.