



Datensicherheit richtig überwachen und verwalten – wie Sie Datenschutzverstöße verhindern

*„Die praktische Umsetzung der EU-Datenschutz-Grundverordnung
NextGen Security mit Sophos Synchronized Security“*

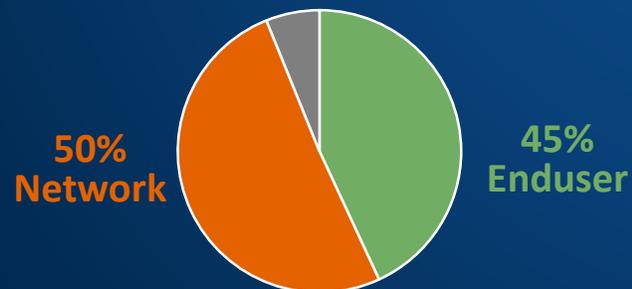
Björn Zackenfels

Sales Engineer

SOPHOS

Sophos im Überblick

- 1985 in Oxford, UK gegründet
- \$632 Millionen Umsatz in FY17
- 3.000 Mitarbeiter, davon 400 in DACH
- 250.000+ Kunden
- 100+ Millionen User
- 26.000+ Channel Partner
- Gartner: Marktführer in den Bereichen Endpoint, Verschlüsselung & UTM



Sophos HQ, Abingdon, UK

Vorgaben der EU-DSGVO

- Klassische Schutzziele der IT berücksichtigen:
 - Vertraulichkeit, Integrität, Verfügbarkeit der Daten
- Stand der Technik
- Verhältnismäßig
- Datenschutzfreundliche Technik:
 - „Data protection by design“
- Datenschutzfreundliche Voreinstellungen
 - „Data protection by default“



Wie kann Sophos Ihnen beim Schutz Ihrer Daten helfen?

1. Durch Verhinderung der Hauptursachen für **Datenabfluss**

- Schutz vor Ransomware und Malware
- Schutz der Daten bei Verlust oder Diebstahl



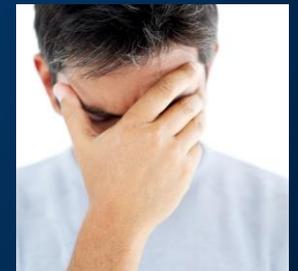
2. Schutz vor **Bedrohungen am Perimeter**

- Schutz vor Hackerangriffen über das Netzwerk
- Sensible Daten in Emails blockieren oder verschlüsseln

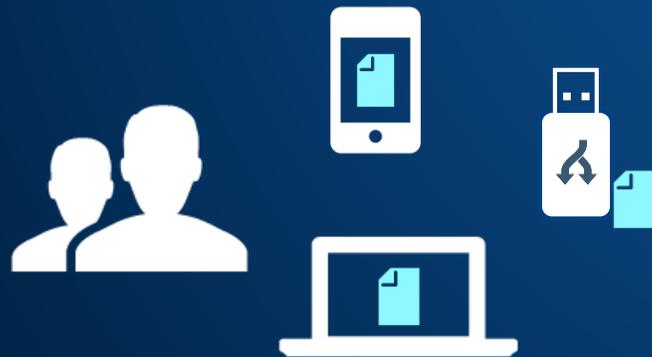


3. Schutz vor **menschlichem Fehlverhalten**

- Dateien verschlüsseln, egal wo sie sind
- Sicherstellen, dass nur berechtigte Personen Zugriff haben



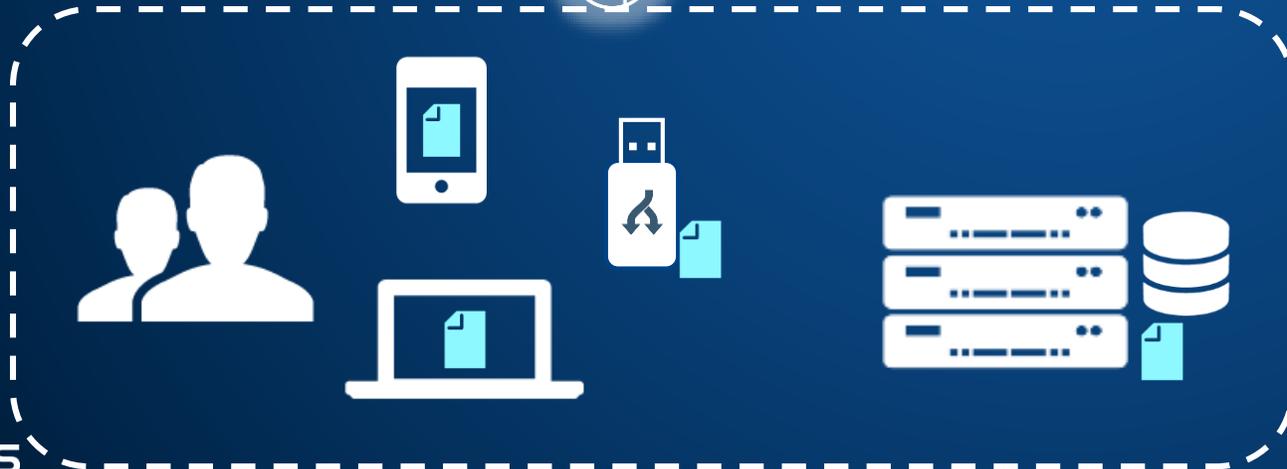
Vertrauliche Daten überall



Schutz gegen Hackerangriffe über das Netzwerk

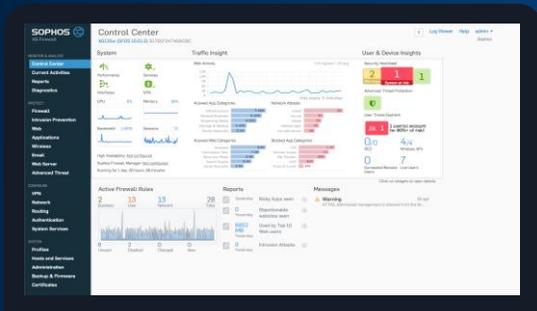


 XG - NextGen Firewall



Sophos XG Firewall Features

Umfassende next-gen Firewall protection



**SYNCHRONIZED
SECURITY**

Security
Heartbeat

Missing
Heartbeat

Destination
Heartbeat

Synchronized
Application
Control



CONTROL

User identity &
awareness

Web Control

Application
Control

Content Control



SECURITY

Advanced Threat
Protection

Next-Gen IPS

Web Protection

Web Application
Firewall

Stateful Firewall

Deep-packet
inspection

Dual anti-virus

Encrypted Traffic
Inspection

Email anti-spam &
phishing Protection

Email
Encryption

Data Loss
Prevention

Sandboxing



NETWORKING

Routing, Bridging
& NAT

Zone
Segmentation

Traffic Shaping

Wireless
Controller

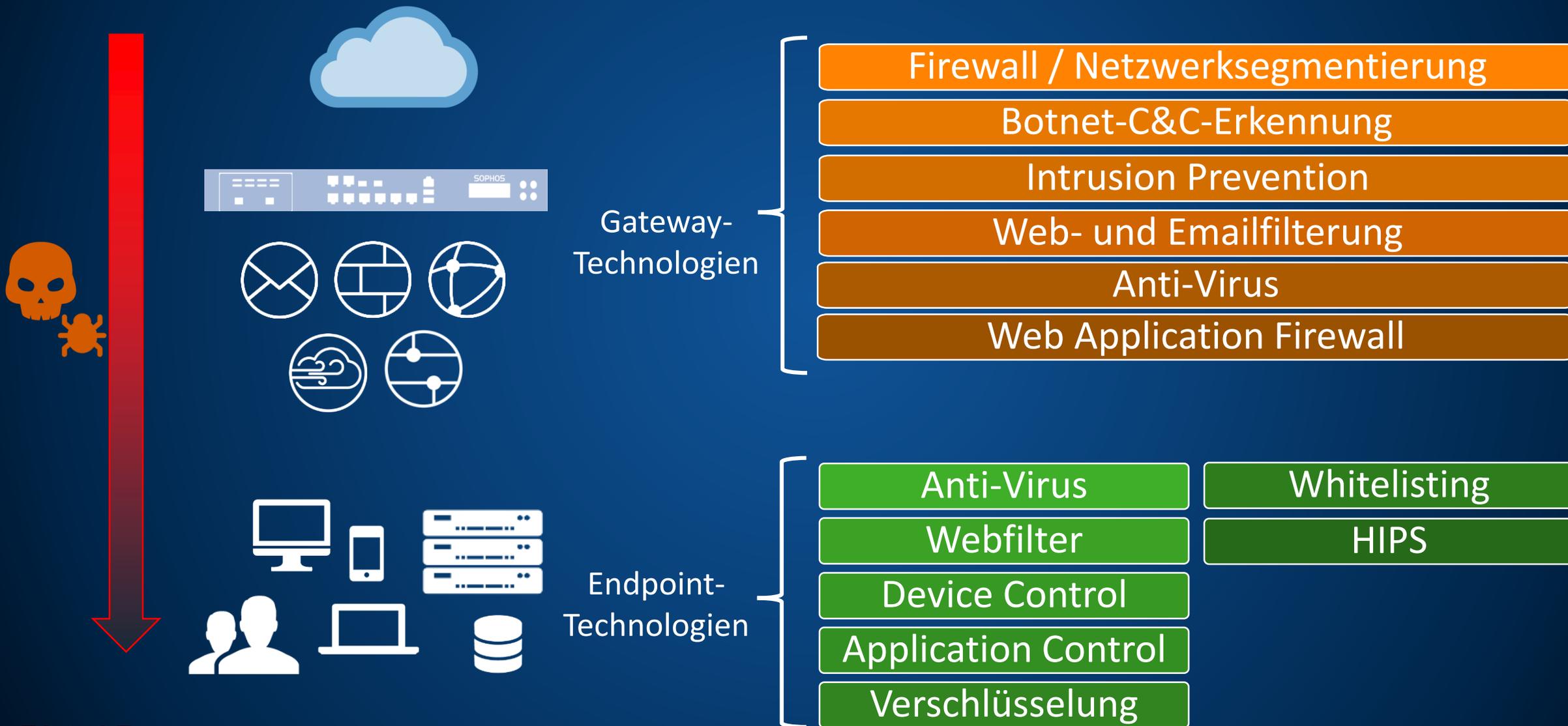
FastPath Packet
Optimization

Full standards-
based VPN

RED VPN

IPv6 Support

Technologien zum Schutz gegen Bedrohungen



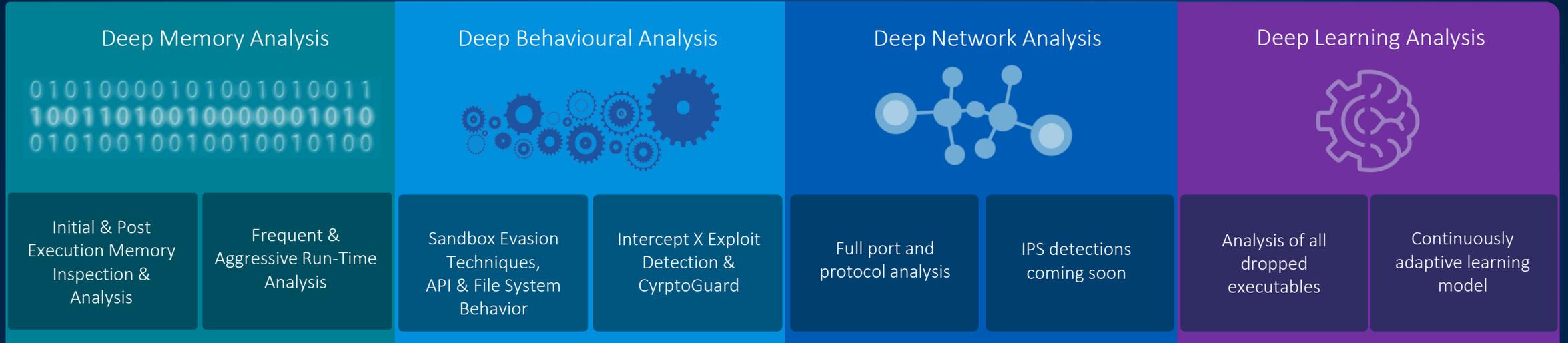
Schutz gegen **unbekannte** Bedrohungen



Sandstorm and Deep Learning

New - Sandstorm Deep Threat Prevention

Your best protection from zero day threats



Sophos Sandstorm



Sandstorm prevention goes beyond endpoint or firewall

Schutz gegen Ransomware und Malware



 XG - NextGen Firewall

  NextGen Endpoint & Server Protection / Intercept X



Endpoint Technologien

Bank

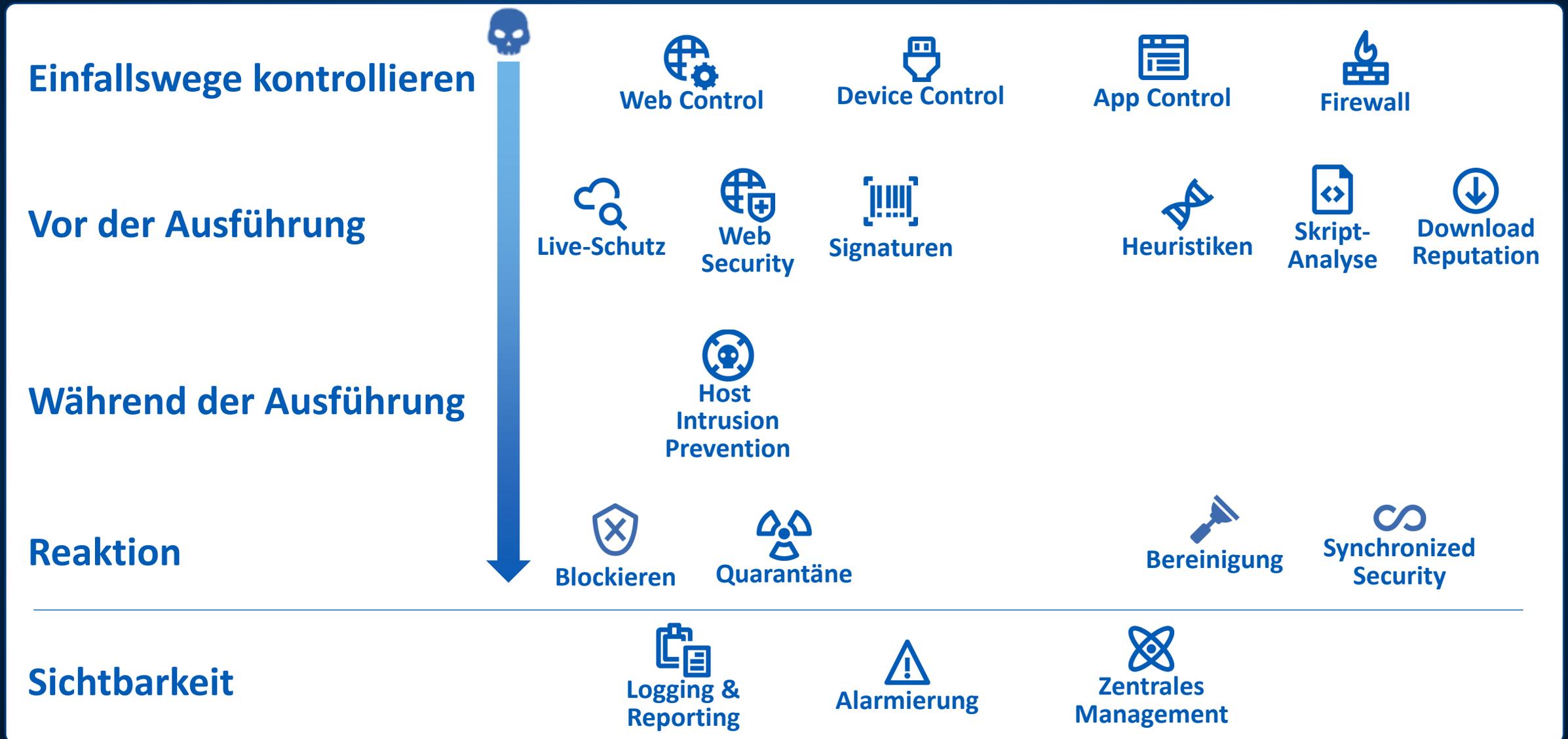
Anti-Virus

WANTED



Vor der Ausführung

Schutzschichten am Endpoint



Endpoint Technologien

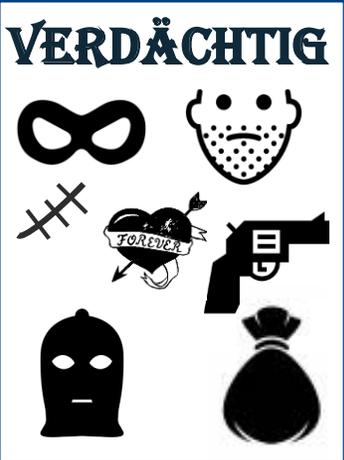
Bank



Anti-Virus

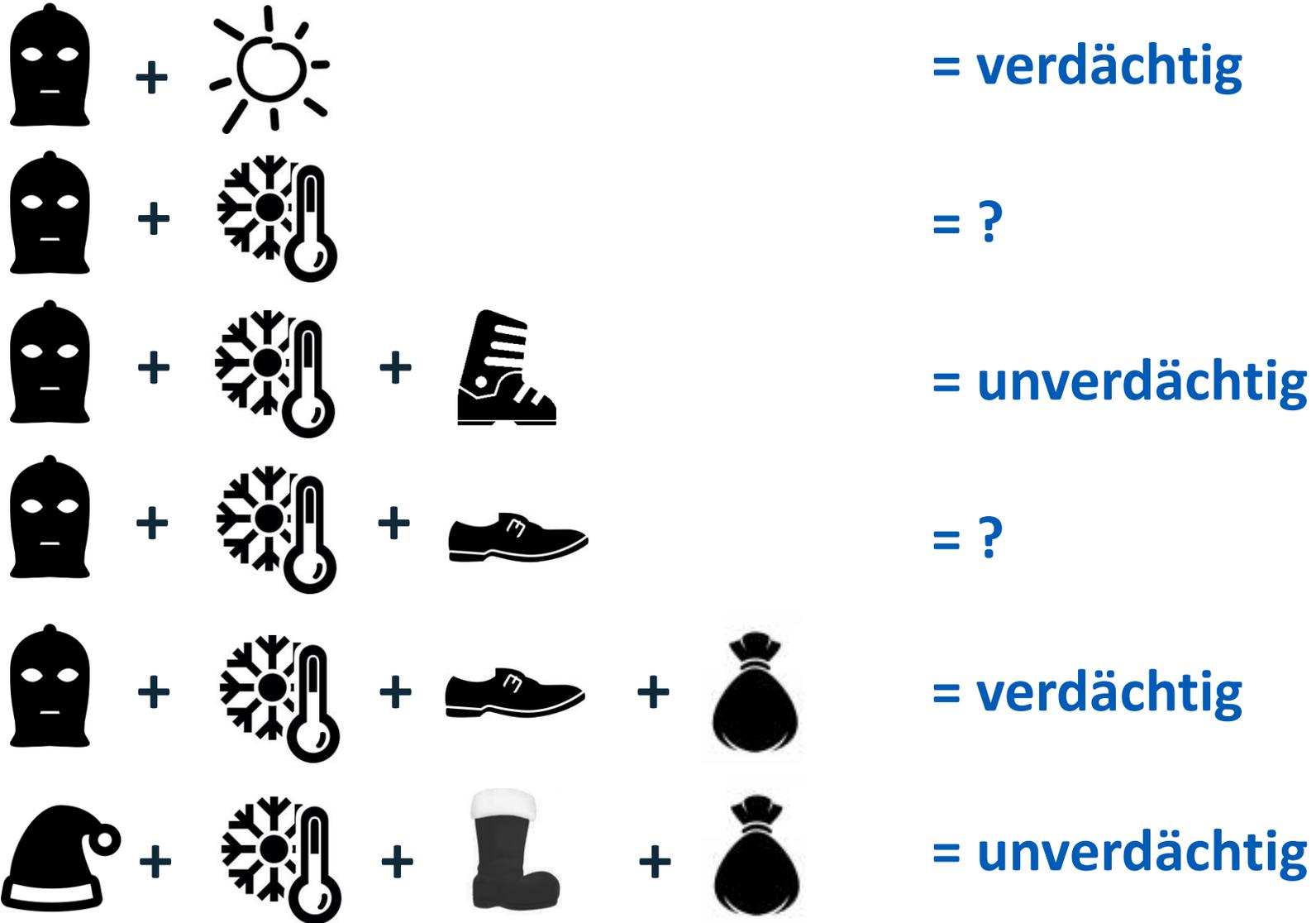


Machine Learning



Vor der Ausführung

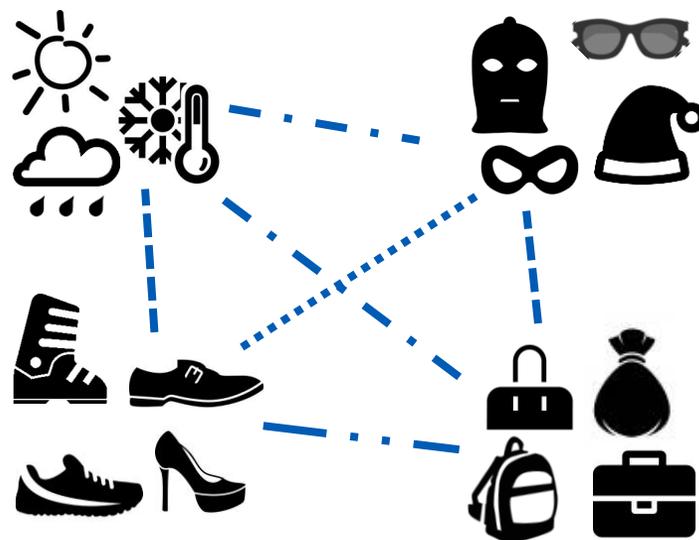
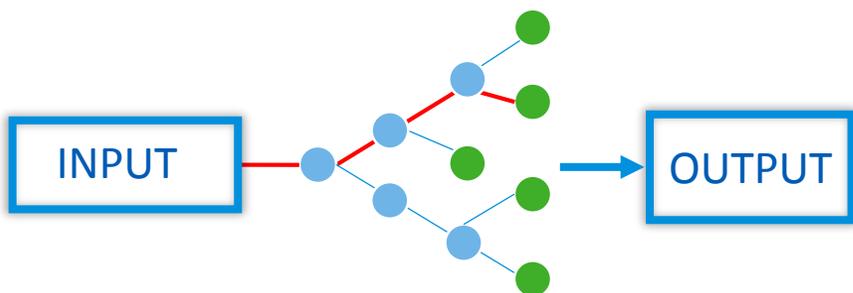
Machine Learning



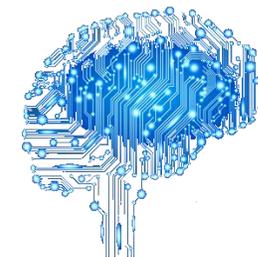
Konventionelles Machine Learning



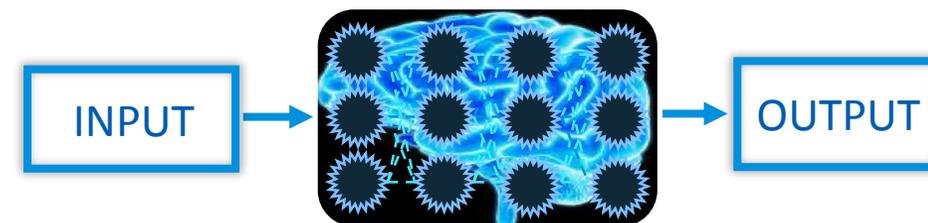
- **Analyst** identifiziert Merkmale und **definiert** deren Beziehungen
- **Manuell** erstelltes **ML-Modell** wird mit Daten trainiert



SOPHOS Deep Learning

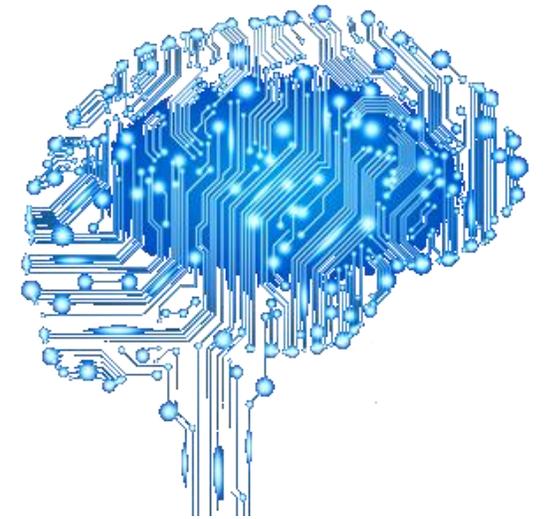


- Neuronales Netz **lernt selbstständig** Merkmale und deren Beziehungen
- DL-Modell **lernt ständig** weiter und **passt sich automatisch an**

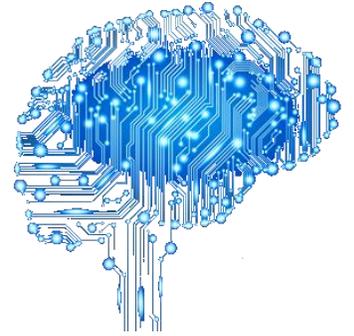


SOPHOS Deep Learning

- **Neuronales Netz** lernt vergleichbar dem **menschlichen Gehirn**
- **Sehr schnelle Einstufung** von Dateien als
 - Malware
 - Legitime Anwendung
 - Potentiell unerwünschte Anwendung
- **Sehr zuverlässig**
 - **Hohe Erkennungsrate** von unbekannter Malware
 - **Geringe False Positive Rate**
- **Lernt selbstständig dazu**
- **Profitiert stark von großer Menge neuer Daten**



Grenzen von Machine Learning



Sehr **effektiv** bei **Programmdateien**

..aber – **nur 56%** aller **Malware** kommt als **Programmdatei**, die von Machine Learning untersucht werden kann



Dateibasierte Malware

| Programmdateien | Dokumente und Mediendateien | Scripts, Java, Webseiten | Sonstige |
|-----------------|-----------------------------|--------------------------|----------|
| 56% | 30% | 11% | 3% |

Endpoint Technologien

Bank



Anti-Virus

WANTED

Machine Learning

VERDÄCHTIG

Exploit Prevention

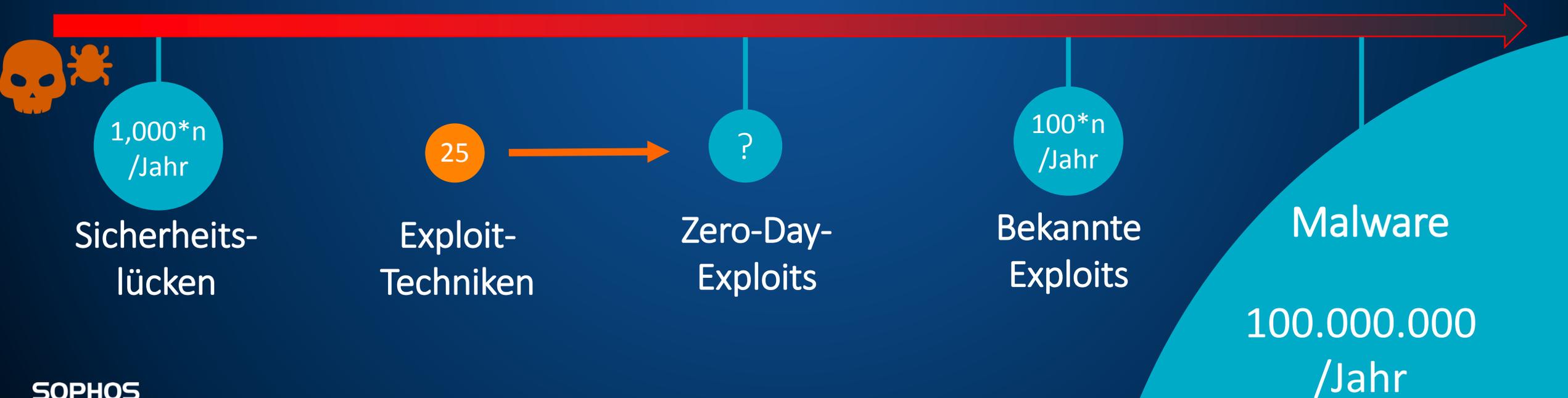
Vor der Ausführung

Während der Ausführung

Exploit Prevention

SOPHOS

Schutz vor unbekannter Malware über Exploit-Prevention



Endpoint Technologien

Bank



Anti-Virus

WANTED

Machine Learning

VERDÄCHTIG

Exploit Prevention

Verhaltens-erkennung

Vor der Ausführung

Während der Ausführung

Verhaltenserkennung

am Beispiel CryptoGuard

SOPHOS

Demo



Synchronized Security

SOPHOS



Papierkorb



Geheim



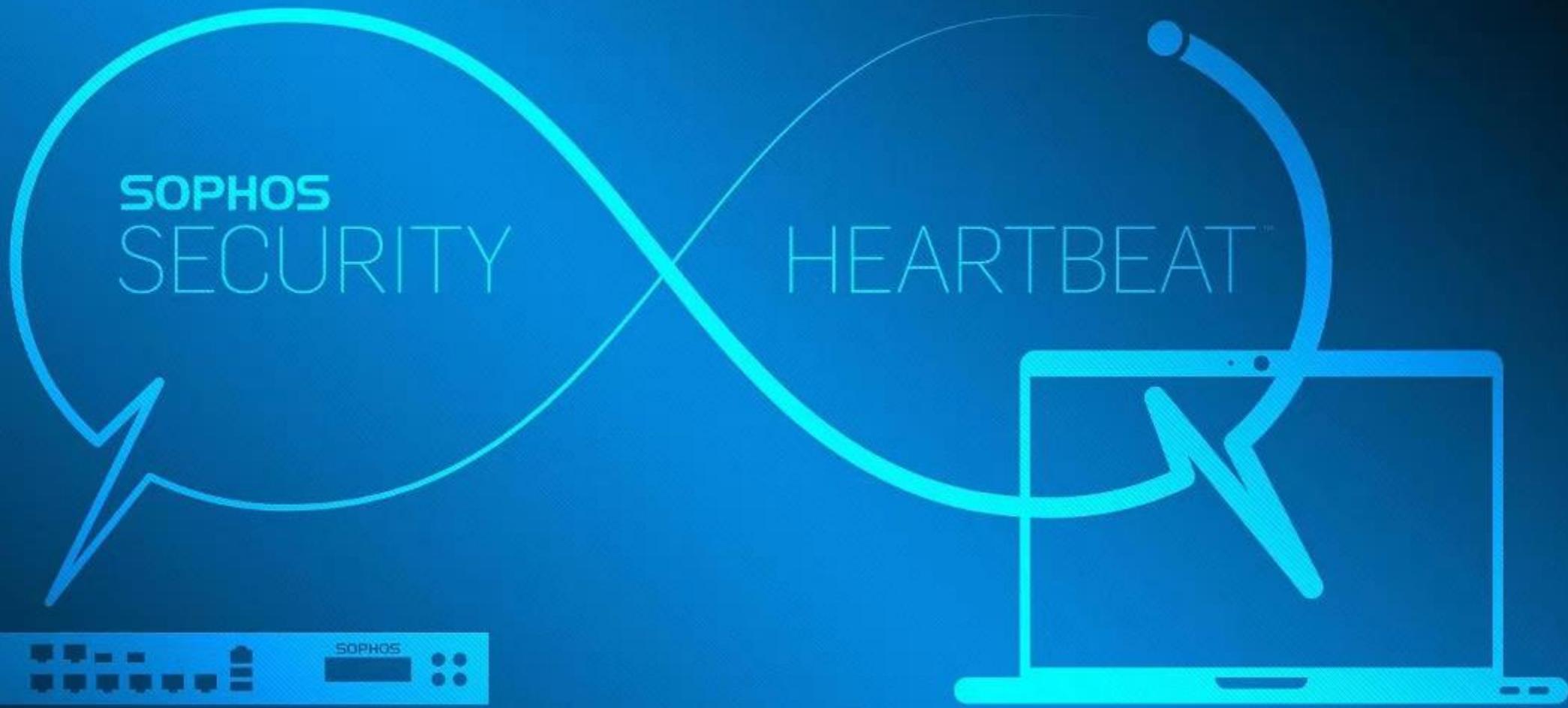
vertrauliche
Daten.docx



SophosTester



Dokumente



Vertraulich



prog



SOPHOS

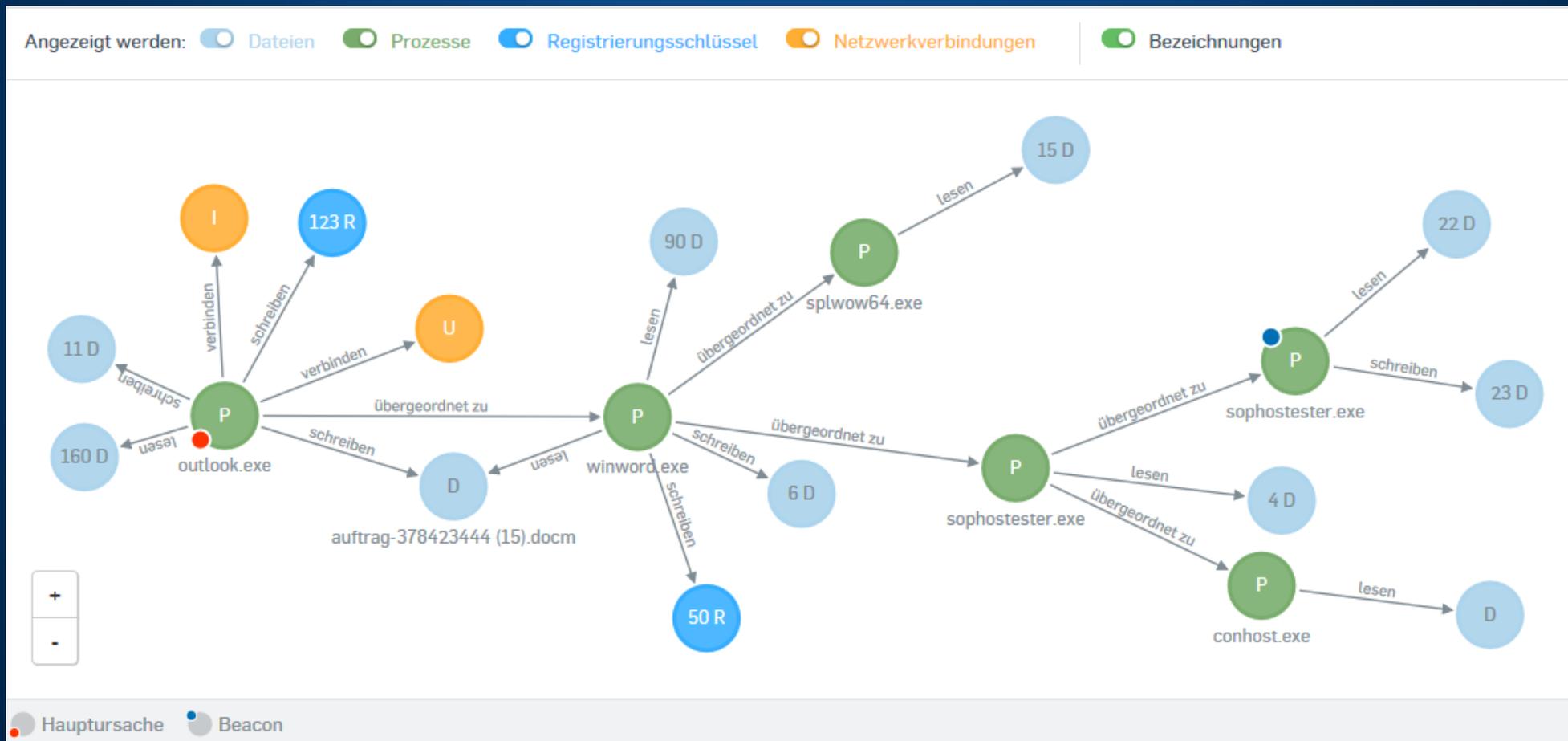


13:49
05.10.2017



Beispiel für Ursachenanalyse

Word-Dokument mit Makro (.docm) per Outlook empfangen (roter Punkt) und mit MS-Word geöffnet. CryptoGuard erkennt die böartige Verschlüsselung (blauer Punkt).



SOPHOS

INTERCEPT

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

INTERCEPT



Einfallswege kontrollieren

Web Control

Device Control

App Control

Firewall

Vor der Ausführung

Live-Schutz

Web Security

Signaturen

Deep Learning

Heuristiken

Skript-Analyse

Download Reputation

Während der Ausführung

Exploit Prevention

Host Intrusion Prevention

Anti-Hacker

Schutz vor Ransomware

Speicher-Scan

Schutz von Passwörtern

Botnet-Traffic-Erkennung

Reaktion

Blockieren

Quarantäne

Wiederherstellung

Erweiterte Bereinigung

Synchronized Security

Sichtbarkeit

Logging & Reporting

Alarmierung

Zentrales Management

Ursachen-Analyse

Schutz von Smartphones und Tablets



 XG - NextGen Firewall

 NextGen Endpoint & Server Protection / Intercept X

 Sophos Mobile



Sophos Mobile

- Sophos Mobile ist eine **umfassende** UEM Lösung
- Manage Mobile, Desktops und IoT
 - iOS, Android, Win 10 Mobile
 - Windows 10, MacOS
 - Android Things, Win 10 IoT
- Sophos Container
- Fully MDM managed oder Container only management
- Sophos Central oder als on-premise

Unified Endpoint Management



Schutz bei Verlust & Diebstahl

- Erzwingen von PIN oder Passwort
- Partielles Löschen von E-Mails, Kalender- und Kontaktdaten
- Remote sperren und/oder löschen
- Geo-Lokalisierung von verlorenen Geräten
- Nachricht im Sperrbildschirm

Vertraulichkeit und Schutz vor Datenabfluss per Email



 XG - NextGen Firewall

 NextGen Endpoint & Server Protection / Intercept X

 Sophos Mobile

 Email Appliance / (E-Mail Protection in der XG)



Email = Postkarte

Dear Alec and Magnus,

It's Izzy. Got your card.
Glad you're having fun.
Nothing's happening here-
Clary's mom is marrying
some werewolf. I think
you guys should get married
too. I'm thinking about
planning it. I love planning
parties.

-Isabelle

THE MORTAL INSTRUMENTS

BOOK 4: CITY OF FALLEN ANGELS • By Cassandra Clare

MortalInstruments.com • Margaret K. McElderry Books



Alec Lightwood

C/O The Great Pyramid

12411

Giza, Egypt

Automatische Email Verschlüsselung

- Jede Station auf dem Weg der Mail kann die Mail lesen.
- Unabsichtlicher oder absichtlicher Datenabfluss via Mail ist die **zweithäufigste** Ursache für Datenverlust
- Email ist in der Geschäftswelt die wichtigste schriftliche Kommunikation
- Sicherheit muss transparent für die Anwender sein – sonst droht der Hillary-Effekt (Nutzung von nicht integren Accounts)



Möglichkeiten der Email Verschlüsselung (mit Sophos Produkten)

- **TLS** (Wegeverschlüsselung)
 - Hier wird lediglich der Weg einer Mail verschlüsselt, die Mail bzw. der Inhalt der Mail ist nicht verschlüsselt.
 - **SG, XG, Mail Appliance**
- **S/Mime oder PGP**
 - Hier wird die ganze Mail verschlüsselt, in der Regel zwischen zwei Gateways, aber auch zwischen Endpunkten möglich.
 - Mail incl. Anhang ist verschlüsselt.
 - **SG**
- **SPX** (secure PDF exchange)
 - Hier wird die Mail in einen PDF Container umgewandelt und mit einem Kennwort versehen.
 - Mail incl. Anhang ist verschlüsselt.
 - **SG, XG, Mail Appliance**
- **HTML5** (Safe Guard Enterprise Outlook Plugin)
 - Hier wird der Anhang einer Mail in einen HTML5 Container umgewandelt und mit einem Kennwort versehen
 - Lediglich der Anhang wird verschlüsselt.
 - **Safe Guard Enterprise**

Schutz gegen Diebstahl + Verlust von PCs und Macs



 XG - NextGen Firewall

  NextGen Endpoint & Server Protection / Intercept X

 Sophos Mobile

 Email Appliance

 Device Encryption



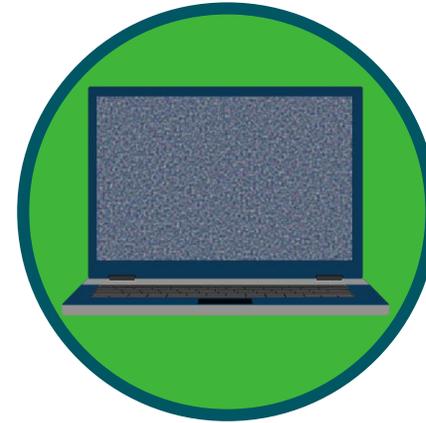
Festplattenverschlüsselung



Unverschlüsselt



Verschlüsselt

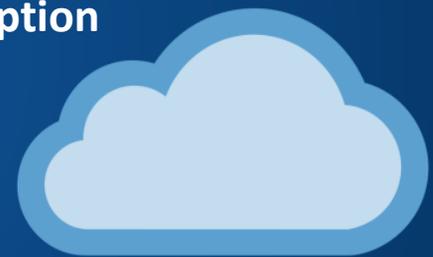


- Schutz der Daten bei versehentlichen Verlust oder Diebstahl von Computern
- Authentisierung erfolgt vor dem Laden des Betriebssystems
- Nur autorisierte Benutzer erhalten Zugriff auf die Daten
- Unterstützung von Windows und Mac Geräten

Schutz gegen menschliche Fehler und Datendiebstahl



-  XG - NextGen Firewall
-   NextGen Endpoint & Server Protection / Intercept X
-  Sophos Mobile
-  Email Appliance
-  Device Encryption
-   SafeGuard Enterprise File Encryption



Verschlüsselung von Wechselmedien



- Schutz von Daten auf Wechselmedien
- Verschlüsselt Dateien auf USB-Sticks, CD/DVD, Memory Card, externen Festplatten etc.
- Sicherer Austausch und sichere Mitnahme von Daten
- Keine Änderung der Arbeitsweise notwendig

Verschlüsselung von Netzlaufwerken



- Schützt den Dateiinhalt am Speicherort und beim Transfer
- Garantiert, dass nur berechtigte Anwender den Dateiinhalt einsehen können
- Gewaltentrennung zwischen Netzwerk- und Sicherheits-Administration
- Transparente für den Benutzer, gewohnte Arbeitsweise

Verschlüsselung von Cloud Speichern



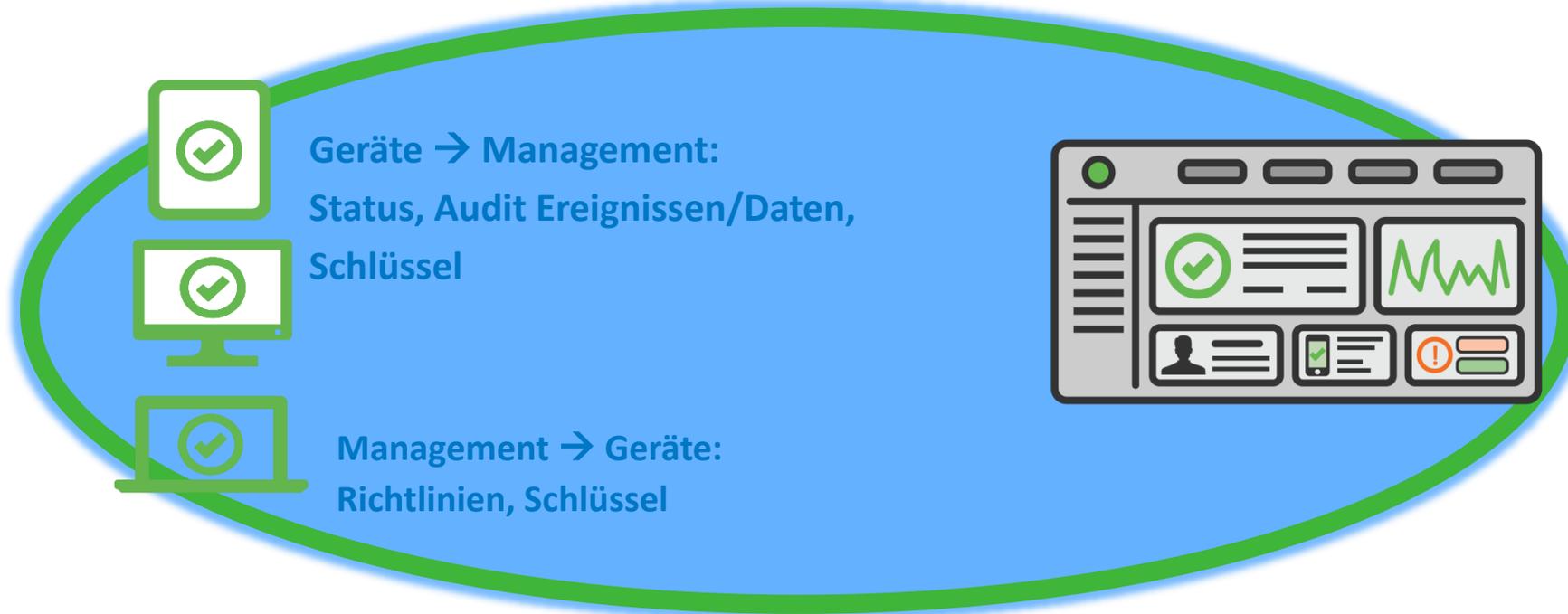
- Verschlüsselt Cloud-Daten transparent auf dem Arbeitsplatz
- Kontrolle über Verschlüsselung / Schlüssel bleibt im Unternehmen
- Unterstützt u.a. Dropbox, Google Drive, Egnyte, OneDrive
- Unterstützung von öffentlichen, privaten und hybriden Clouds

Zugriff mit Smartphones & Tablets



- Auf mobilen Endgeräten können sich genauso viele Daten wie auf Notebooks
- Mitarbeiter sollen auch unterwegs produktiv bleiben
- Schützen Sie die Daten auf Ihren Mobilegeräten

Management & Compliance



- Management, Reporting & Nachweisbarkeit sind wichtige Bestandteile der Lösung
- Management muss einfach aber auch komplett sein
- Die Nachweisbarkeit ist genauso wichtig wie der eigentliche Schutz der Daten

Welche Verschlüsselung also wofür?

Festplattenverschlüsselung

Dateiverschlüsselung



Schutz gegen Diebstahl und Verlust



Schutz der Daten auf gehackten/kompromittierten Systemen



Schutz vor Datenabfluss durch Insider



Schutz von per Email versendeten Daten



Schutz von Daten in der Cloud



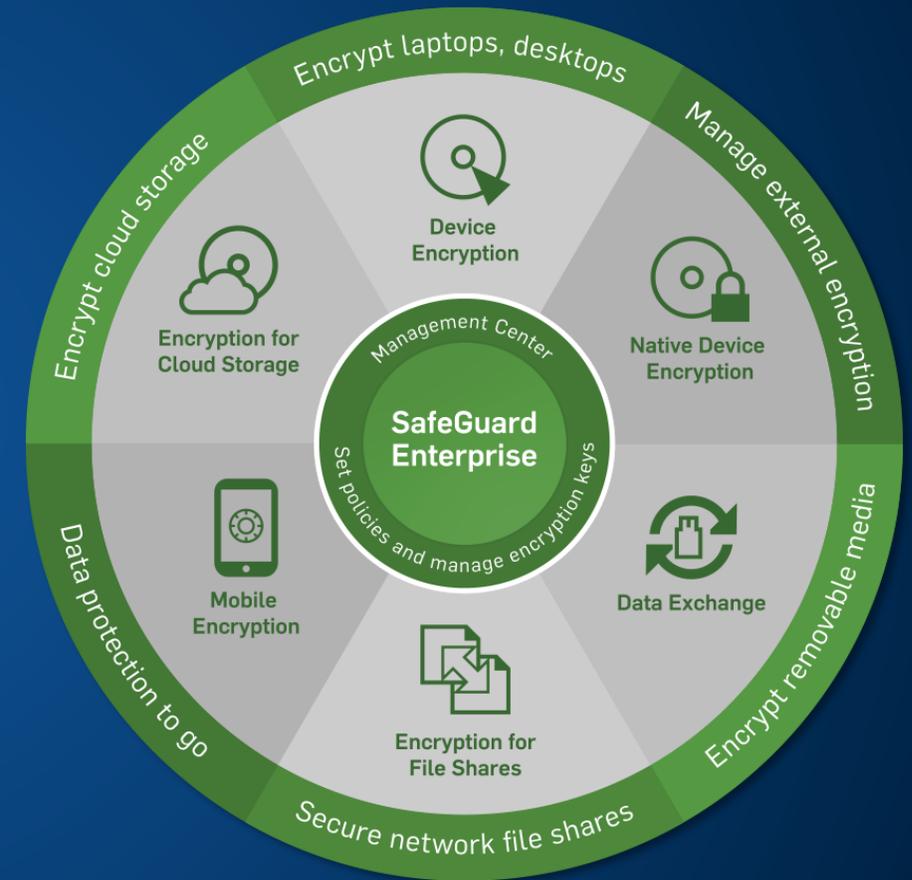
Schutz von Daten auf USB-Sticks



Schutz von Daten auf Smartphones/Tablets



SafeGuard Enterprise – Verschlüsselung überall



Wie kann man nun alle diese Security Features vereinen?



-  XG - NextGen Firewall
-   NextGen Endpoint & Server Protection / Intercept X
-  Sophos Mobile
-  Email Appliance
-  Device Encryption
-   SafeGuard Enterprise File Encryption



Finale Verteidigungslinie

Sicherheit als System



Synchronized Security

SOPHOS

Endpoint Technologien

Bank

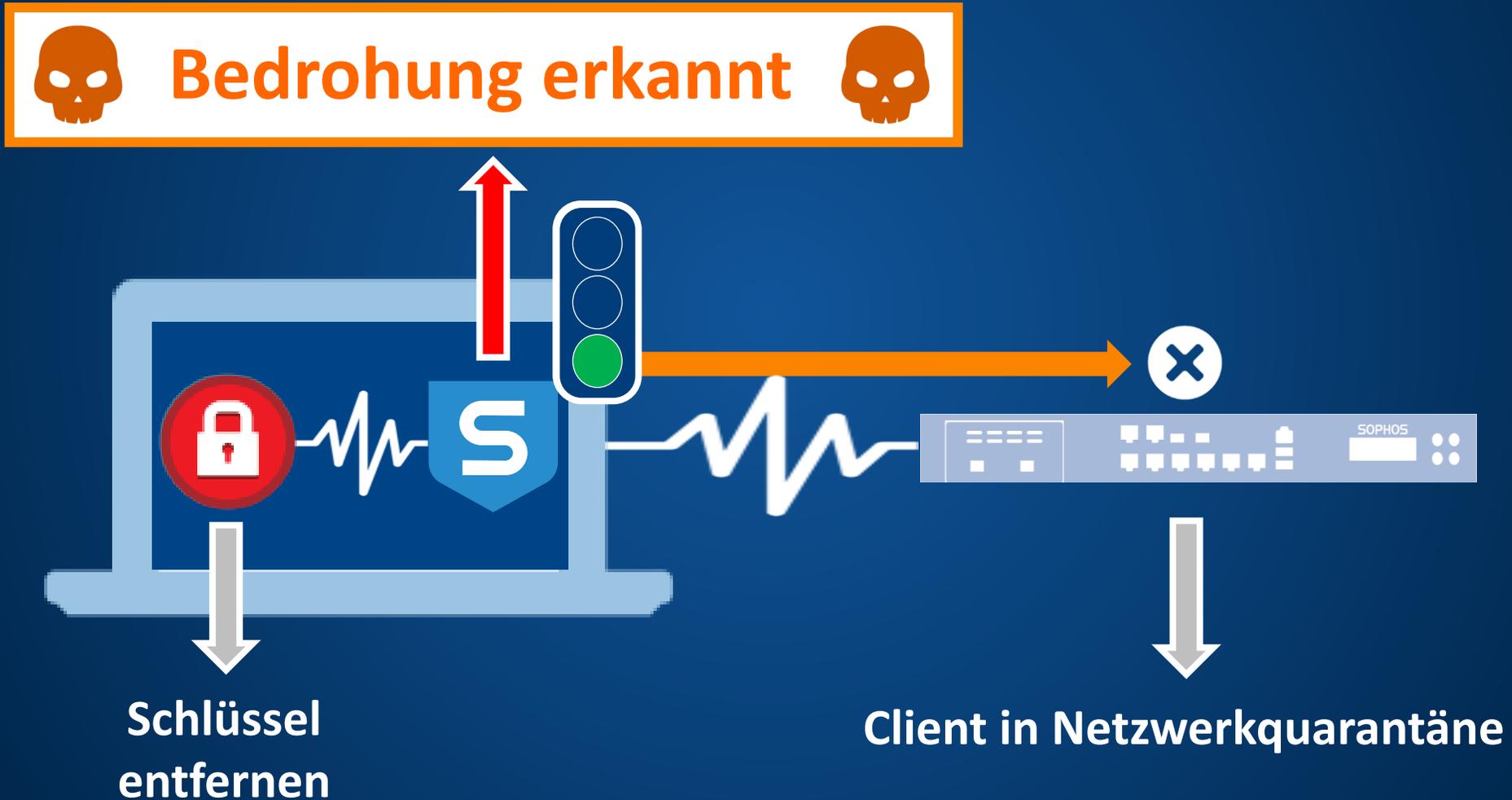
Synchronized Security



Synchronized Security – Teamplay statt Best-of-Breed



Security Heartbeat – Zusammenspiel von Endpoint und Gateway



Synchronized AppControl

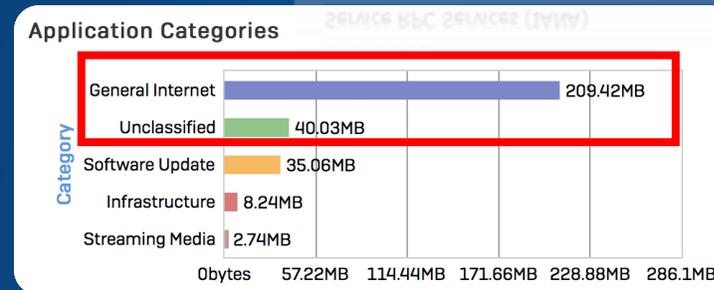


Synchronized Security

SOPHOS

Das Problem der Applikationskontrolle

- In einer Firewall basiert die Applikationskontrolle auf Signaturen
- Einige Apps haben keine Signaturen
- Einige Apps verhindern die Erkennung
- Mancher App Verkehr ist zu unspezifisch (HTTP/HTTPS)



| Application | Category | Risk | Sessions | Bytes (Sent/Received) |
|-------------|-----------------|------|----------|-----------------------|
| BitTorrent | P2P | 4 | 78 | 410.37 K |
| DNS | Network.Service | 1 | 66 | 16.94 K |
| SSL | Network.Service | 1 | 21 | 16.04 M |
| Skype | P2P | 3 | 13 | 273.90 K |
| Unknown | | | 6 | 442 I |
| Twitter | Social.Media | 1 | 3 | 29.61 K |
| LastPass | Storage.Backup | 1 | 1 | 23.05 K |
| Google.Plus | Social.Media | 1 | 1 | 17.78 K |
| Dropbox | Storage.Backup | 1 | 1 | 340.18 K |
| | | | 1 | 19.87 K |
| | | | 1 | 33.38 M |
| | | | 1 | 7.47 K |

| Risk | Application Name | Sessions | Bytes | Threats |
|------|-------------------|----------|---------|---------|
| 1 | dns | 16.2 K | 4.3 M | 0 |
| 4 | bittorrent | 11.4 K | 525.9 M | 0 |
| 1 | web-browsing | 9.2 K | 307.4 M | 6 |
| 1 | ssl | 3.3 K | 1.1 G | 0 |
| 1 | Custom Applet v | 1.4 K | 61.8 M | 0 |
| 1 | facebook-base | 800 | 20.5 M | 0 |
| 1 | insufficient-data | 676 | 429.0 K | 0 |
| 2 | skype-proton | 654 | 582.0 K | 0 |
| 2 | ntp | 488 | 95.0 K | 0 |
| 1 | icmp | 476 | 58.4 K | 0 |
| 2 | icloud | 351 | 2.6 M | 0 |
| 1 | ssdp | 307 | 79.4 K | 0 |
| 2 | netbios-ns | 224 | 30.3 K | 12 |
| 2 | salesforce-base | 223 | 8.5 M | 0 |
| 1 | rtmp | 213 | 8.9 M | 0 |
| 1 | rtmp | 196 | 6.9 M | 0 |
| 1 | flash | 181 | 96.0 M | 0 |

Security Heartbeat – Applikationskontext

Informationen und Kontrolle über unbekannte Apps



Security Heartbeat – Synchronized App Control

Firewall erfährt die kommunizierende Applikation vom Client



Demo

SOPHOS

SOPHOS
XG Firewall

MONITOR & ANALYZE

- Control Center
- Current Activities
- Reports
- Diagnostics

PROTECT

- Firewall
- Intrusion Prevention
- Web
- Applications
- Wireless
- Email
- Web Server
- Advanced Threat
- Synchronized Security

CONFIGURE

- VPN
- Network
- Routing
- Authentication
- System Services

SYSTEM

- Profiles
- Hosts and Services
- Administration
- Backup & Firmware
- Certificates

Control Center

SFVUNL (SFOS 17.1.0 Beta-1-OMC) C01001X68VKJC41

System

Performance Services
Interfaces VPN

0/0 RED
0/0 Wireless APs

Connected Remote Users: 0
Live Users: 0

CPU 11% Memory 61%
Bandwidth 6.3KB Sessions 0

High Availability: [Not configured](#)
Sophos Firewall Manager: [Not configured](#)
Running for 0 day(s), 0 hour(s), 29 minute(s)



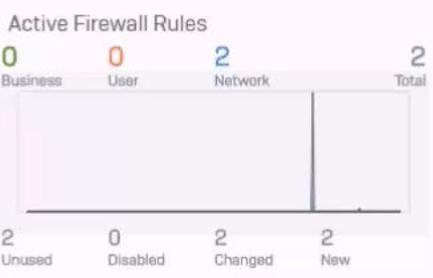
User & Device Insights

Security Heartbeat®: 1 Connected

Synchronized Application Control™: 0 Apps Discovered
No new signatures detected. Do you want your application list to be up-to-date? [Click here](#)

Sandstorm: 0 Suspect, 0 Malicious, 0 Clean

ATP: 0 Source blocked
UTQ: 0 Acc. for 80% of risk



Reports

- 0 Risky Apps seen Yesterday
- 0 Objectionable websites seen Yesterday
- 0 bytes Used by Top 10 Web users Yesterday
- 938 Intrusion Attacks Yesterday

Messages

Warning 10:37
HTTPS, SSH-based management is allowed from the ...

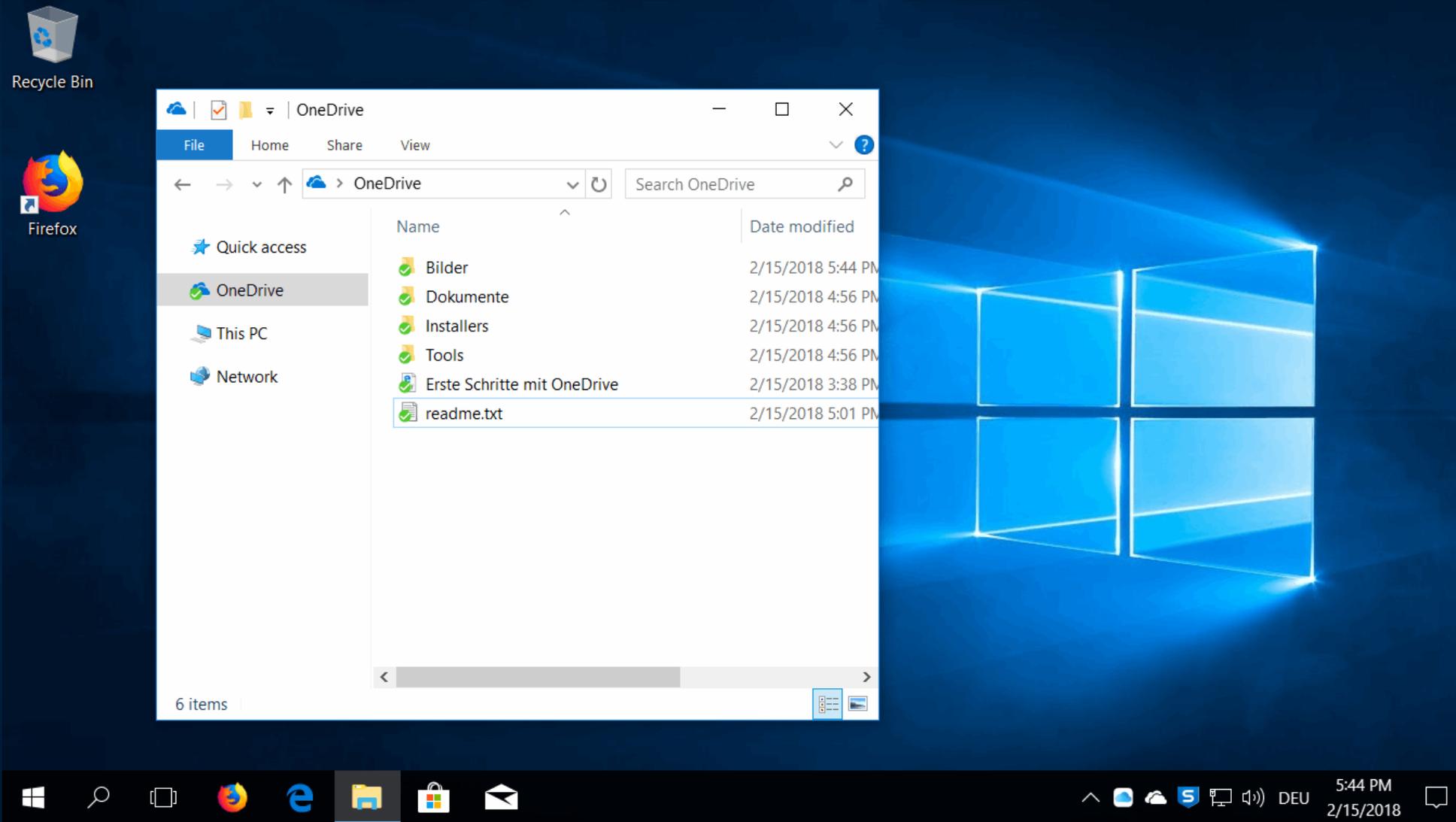
Click on widgets to open details

Cloud Access Security Broker (CASB)

CASB – Funktionsumfang in SFOS v17.1

- Visibilität der Nutzung von Cloud Applikationen im Unternehmen
- “Shadow IT” Erkennung durch Klassifikation von Cloud Applikationen
- Bandbreitenmanagement erlaubter Cloud Applikationen
- Unterbinden unerwünschter Cloud Applikationen im Unternehmen

CASB - Bessere Kontrolle von Cloud Applikationen



- Office365
- Google Apps
- Onedrive
- iCloud
- Dropbox
- Salesforce
- SAP Concur
- Atlassian Jira
- Adobe Creative Cloud
- Cisco WebEx
- GoToMeeting
- Zoom
- Teamviewer
- Facebook
- Xing
- Linkedin
- GoogleAnalytics

Neues Cloud Applications Widget im Dashboard

The screenshot displays the Sophos Control Center dashboard for a device labeled SF01V (SFOS 17.1.0 Beta-1-OMC). The interface is divided into several sections:

- System:** Performance, Services, Interfaces, and VPN. Metrics include 0/0 RED, 0/0 Wireless APs, 0 Connected Remote Users, and 2 Live Users. System resources show CPU at 15%, Memory at 81%, and Bandwidth at 5.5KB. Sessions are at 1.
- Traffic Insight:** A line graph for Web Activity shows 426 highest and 80 average. A bar chart for Allowed Web Categories lists: Information T... (5.02K), None (1.63K), Software Upd... (456), News (208), and Personal Net... (89). Network Attacks are at 0.
- User & Device Insights:** Security Heartbeat with a question mark icon. Synchronized Application Control™ shows 0 Apps Discovered. Sandstorm shows 2 Suspect, 0 Malicious, and 2 Clean. ATP shows 0 Source blocked, and UTQ shows 0 Acc. for 80% of risk.
- Cloud Applications (highlighted in red):** A widget showing 2 Apps Discovered. It includes a bar chart with categories: New (blue), Sanctioned (green), Unsanctioned (red), and Tolerated (orange). Metrics include 414 KB In and 639 KB Out.
- Active Firewall Rules:** A table with columns for Business (1), User (1), Network (0), and Total (2).
- Reports:** 0 Risky Apps seen Yesterday, 0 Objectionable websites seen Yesterday, and 0 bytes Used by Top 10 Web Yesterday.
- Messages:** A section for messages with a download icon.

Navigation links include 'How-To Guides' and 'Log View'. A footer note says 'Click on widgets to open details'.

Nutzungsübersicht Cloud Applikationen

The screenshot displays the Sophos XG Firewall 'Applications' page. The left sidebar shows navigation options under 'MONITOR & ANALYZE' and 'PROTECT'. The main content area shows a list of cloud applications with their respective risk levels and status. Two applications, 'iCloud' and 'SkyDrive Base', are highlighted with red boxes. A table on the right provides transfer statistics for these applications, also highlighted with a red box.

| Application | Traffic | Users | Uploads | Downloads | File Types |
|---------------|---------|-------|---------|-----------|------------|
| iCloud | 870 KB | 3 | 0 | 0 | 0 |
| SkyDrive Base | 183 KB | 2 | 0 | 0 | 0 |

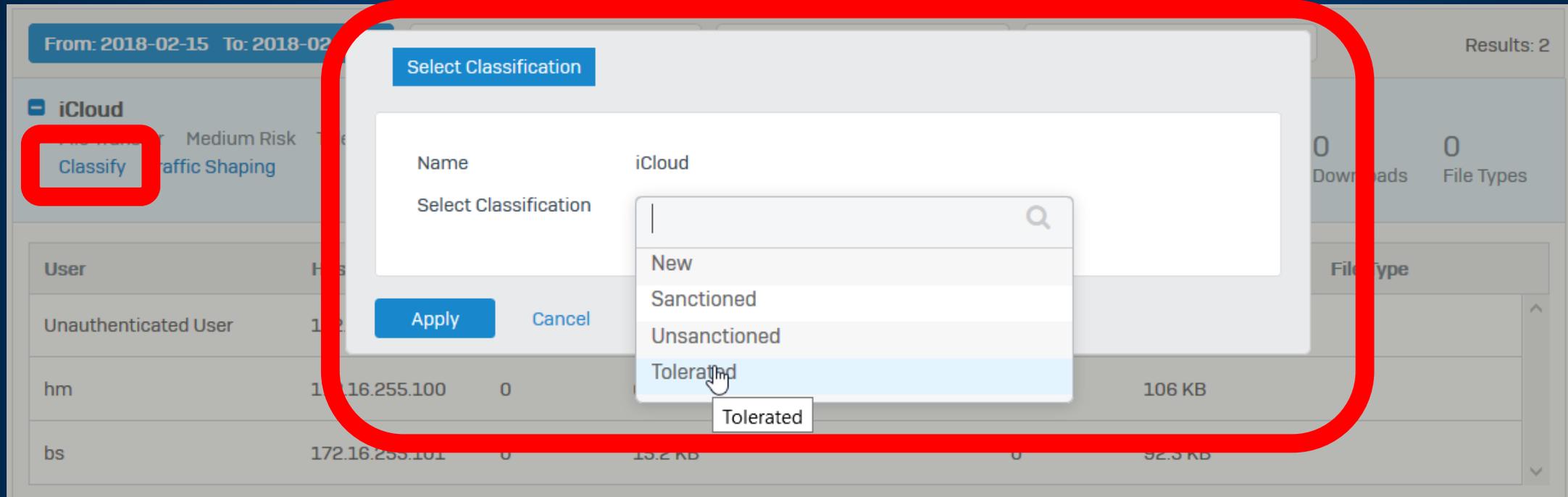
- Erkannte Cloud Applikation
- Transfer Statistik

Per User Einsicht

| User | Host | Uploads | Upload Data | File Type | Downloads | Download Data | File Type |
|----------------------|----------------|---------|-------------|-----------|-----------|---------------|-----------|
| Unauthenticated User | 172.16.255.100 | 0 | 301 KB | | 0 | 289 KB | |
| hm | 172.16.255.100 | 0 | 66.2 KB | | 0 | 106 KB | |
| bs | 172.16.255.101 | 0 | 15.2 KB | | 0 | 92.3 KB | |

- Identifizierte Nutzer und Source IP Adressen
- Per User Transferstatistik und wenn verfügbar Anzahl Up-, und Downloads
- Wenn verfügbar identifizierte Dateitypen

Custom Klassifikation von Cloud Applikationen



- Cloud Applikationen können nach geschäftlichen Vorgaben klassifiziert werden

Traffic Shaping Policy per Cloud Applikation

The screenshot shows a web interface for configuring traffic shaping policies. A modal dialog titled "Traffic Shaping Policy" is open, showing the configuration for the "iCloud" application. The dialog has a "Name" field set to "iCloud" and a "Traffic Shaping Policy" dropdown menu set to "THROTTLE_CLOUD_STORAGE". There are "Save" and "Cancel" buttons at the bottom of the dialog. In the background, a table lists traffic for various users, with a "Traffic Shaping" button highlighted in the left sidebar.

| User | Host | Port | Bytes | Packets | KB |
|----------------------|----------------|------|---------|---------|---------|
| Unauthenticated User | 172.16.255.100 | 0 | 66.2 KB | 0 | 106 KB |
| hm | 172.16.255.101 | 0 | 15.2 KB | 0 | 92.3 KB |

- Für jede Cloud Applikation lassen sich Traffic Shaping Policies definieren

Traffic Shaping Policy per Cloud Applikation

Name *

Policy Association Users Rules Web Categories Applications

Rule Type Limit Guarantee

Limit Upload/Download Separately Disable Enable

Priority *

Guarantee - Limit * - KBps [2 - 2560000]

Bandwidth Usage Type Individual Shared

Description

- Die Traffic Shaping Policy kann pro Cloud Applikation entweder per Benutzer (Individual) oder als gescharter Pool über alle Nutzer (Shared) definiert werden

Filter für die Informationssuche

The screenshot shows the Sophos XG Firewall 'Applications' page. The left sidebar contains navigation menus for 'MONITOR & ANALYZE' (Control Center, Current Activities, Reports, Diagnostics), 'PROTECT' (Firewall, Intrusion Prevention, Web, Applications, Wireless, Email, Web Server, Advanced Threat, Synchronized Security), and 'CONFIGURE' (VPN). The main content area is titled 'Applications' and has tabs for 'Cloud Applications', 'Synchronized Application Control', 'Application List', 'Application Filter', and 'Traffic Shaping Default'. The 'Application Filter' tab is active, showing a date range filter set to 'From: 2018-02-15 To: 2018-02-15'. Below this is a calendar for February 2018 with the 15th selected. A classification dropdown menu is open, showing options: 'All Classifications', 'New', 'Sanctioned', 'Unsanctioned', and 'Tolerated'. A category dropdown menu is also open, showing options: 'E-commerce', 'File Transfer', 'Gaming', 'General Business', 'General Internet', and 'Infrastructure'. A sorting dropdown menu is open, showing options: 'Sort by Bytes Transferred', 'Sort by Users', 'Sort by Uploads', 'Sort by Downloads', and 'Sort by File Types'. The results section shows 'Results: 2' and a summary table with columns: Traffic (183 KB), Users (2), Uploads (0), Downloads (0), and File Types (0).

- Die Cloud Applikationen lassen sich nach Bedarf durchsuchen und sortieren nach:

- Datumsrange
- Klassifikation
- Kategorie
- Transferdetails

CASB Applikationen in der App Control

SOPHOS
XG Firewall

MONITOR & ANALYZE
Control Center
Current Activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion Prevention
Web
Applications
Wireless
Email
Web Server
Advanced Threat
Synchronized Security

CONFIGURE
VPN
Network
Routing
Authentication
System Services

SYSTEM
Profiles
Hosts and Services
Administration

Applications

How-To Guides Log Viewer Help admin

Cloud Applications Synchronized Application Control Application List Application Filter Traffic Shaping Default

Name * Cloud Storage

Description

Add Delete

| Application | Application Filter Criteria | Schedule | Action | Manage |
|--|---|----------|--------|--------|
| <input type="checkbox"/> SkyDrive Base, iCloud | <input type="checkbox"/> Category = File Transfer, General Internet Risk = 3-Medium Characteristics = Cloud Application, Excessive Bandwidth, Loss of productivity, Transfer files, Widely Used Technology = Browser Based Classification = Unsanctioned, Tolerated | | | |

- Die CASB Cloud Applikationen können wie jegliche anderen identifizierten Anwendungen auch in der App Control der Sophos Firewall verwendet werden um Cloud Apps zu blocken oder Bandbreitenmanagement zu betreiben

Cloud Application Reporting

Reports How-To Guides Log Viewer Help admin

[Show Reports Settings](#)

Dashboards **Applications & Web** Network & Threats VPN Email Compliance Custom

Show: Cloud Application Usage View All FROM: 2018-02-15 TO: 2018-02-15 [Generate](#)

- User App Risks & Usage
- Cloud Application Usage**
- Blocked User Apps
- Synchronized Applications
- Web Risks & Usage
- Blocked Web Attempts
- Search Engine
- Web Content
- Web Server Usage
- Web Server Protection
- User Data Transfer Report
- FTP Usage
- FTP Protection

| Application | Bytes |
|--------------------|-----------------------------------|
| iCloud | 558.11KB |
| Other Applications | 28.36KB, 42.54KB, 56.72KB, 70.9KB |

| Host | Sent Bytes | Received Bytes | Bytes |
|----------------|------------|----------------|-----------|
| 172.16.255.101 | 374.06 KB | 460.43 KB | 834.5 KB |
| 172.16.255.101 | 30.38 KB | 164.13 KB | 194.51 KB |

Classification: Sanctioned

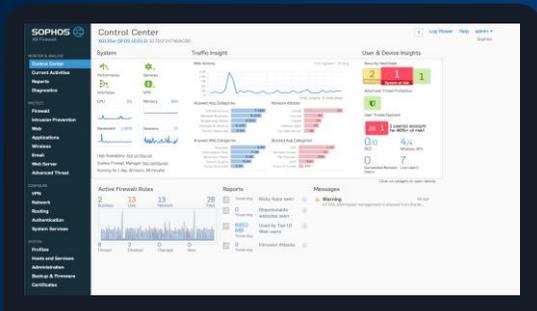
| Application | User Count | Hits | Bytes |
|-----------------|------------|------|-------|
| No Record Found | | | |

| Application | User Count | Hits | Bytes |
|---------------|------------|------|-----------|
| iCloud | 1 | 14 | 558.11 KB |
| SkyDrive Base | 1 | 2 | 89.31 KB |

- Erweiterung der Reportingsektion um «Cloud Application Usage»

Sophos XG Firewall Features

Umfassende next-gen Firewall protection



**SYNCHRONIZED
SECURITY**

Security
Heartbeat

Missing
Heartbeat

Destination
Heartbeat

Synchronized
Application
Control



CONTROL

User identity &
awareness

Web Control

Application
Control

Content Control



SECURITY

Advanced Threat
Protection

Next-Gen IPS

Web Protection

Web Application
Firewall

Stateful Firewall

Deep-packet
inspection

Dual anti-virus

Encrypted Traffic
Inspection

Email anti-spam &
phishing Protection

Email
Encryption

Data Loss
Prevention

Sandboxing



NETWORKING

Routing, Bridging
& NAT

Zone
Segmentation

Traffic Shaping

Wireless
Controller

FastPath Packet
Optimization

Full standards-
based VPN

RED VPN

IPv6 Support

Synchronized Security von Sophos



- Best-of-Breed wird ersetzt durch **Security als System**
- **Kommunikation** von Netzwerk-, Endpoint-, Server- und Verschlüsselungslösungen
- **Erkennung** und **Eindämmung** von Hacker-Aktivitäten
- **Automatische Reaktion** auf Vorfälle
- **Analyse** der Infektions- und Verbreitungswege

Sophos Compliance Check

Sophos Compliance Check

SOPHOS **SOPHOS** **SOPHOS** **SOPHOS** **SOPHOS** **SOPHOS**

SOPHOS PRODUKTE ▾ SOPHOSLABS PARTNER SUPPORT UNTERNEHMEN ANMELDEN ▾

Ihre Auswertung ... [Neu beginnen](#) Auswertung ausdrucken

| Fragen? | Ihre Antwort & unser Hinweis | Was bietet Ihnen Sophos? |
|--|--|---|
| 1 Sehen Ihre Kerngeschäftsprozesse eine regelmäßige und systematische Überwachung von Datensubjekten im großen Stil vor? <i>Datensubjekte sind Einzelpersonen, die anhand von Daten identifiziert werden bzw. identifiziert werden können. Im Rahmen dieses Checks sind unter Daten Informationen zu verstehen, mit denen eine Einzelperson direkt oder indirekt identifiziert werden kann. Hierzu zählen u. a. Zahlungs-, Kunden-, Patientendaten.</i> | Ja. Hinweis: Sie müssen alle Vorschriften der Verordnung einhalten, also u. a. auch einen Datenschutzbeauftragten benennen. | In unserem Whitepaper zur EU-Datenschutz-Grundverordnung erfahren Sie alles Wichtige über die neuen Vorschriften und die Konsequenzen für Unternehmen. Whitepaper lesen |
| 2 Verfügen Sie über eine Datenschutzrichtlinie, die Ihren Mitarbeitern Hilfestellung gibt, was den Schutz personenbezogener Daten anbelangt? | Ja. Hinweis: Stellen Sie sicher, dass die Richtlinie Ihren Mitarbeitern gegenüber klar kommuniziert wird. | Unsere Sophos-Beispiel-Datenschutzrichtlinie können Sie als Vorlage nutzen, wenn Sie Ihre eigene Richtlinie in Zukunft aktualisieren möchten. Passen Sie diese an die Erfordernisse Ihres Unternehmens an. Zur Richtlinie |
| 3 Sind Ihre Unternehmens- | Ja. Hinweis: Die auf den Laptops | Wenn Sie BitLocker zur |

Frage 1 von 6 Frage 2 von 6 Frage 3 von 6 Frage 4 von 6 Frage 5 von 6 Frage 6 von 6

PhishThreat

(User Awareness)



SOPHOS

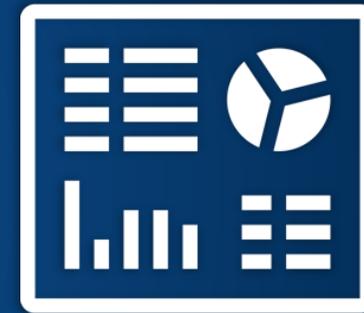
Was ist Sophos Phish Threat?



Benutzer-
Training



Überprüfung



Reporting

1

Neue Kampagne

- Test-Vorlage auswählen
- Test-Vorlage anpassen

The screenshot shows the Sophos Phish Threat interface. At the top, it says 'SOPHOS CENTRAL Admin' and 'Phish Threat'. The main heading is 'Phish Threat - Neue Kampagne' with sub-navigation: 'Überblick / Phish Threat Dashboard / Kampagnen / Neue Kampagne'. A progress bar shows four steps: 'Erste Schritte' (active), 'Angriff auswählen', 'Angriff benutzerspezifisch anpassen', and 'Training auswählen'. Below this, three email templates are visible: 'DHL fehlgeschlagene Lieferung' (Einfach), 'Hintergrundprüfbenachrichtigung' (Einfach), and 'Telearbeit-Möglichkeiten' (Mittel). A detailed preview of the 'DHL' template is shown, including a yellow DHL logo, a recipient name 'Lieber (FirstName),', and text about a failed delivery. A 'Diesen Angriff auswählen' button is at the bottom. Another preview for 'Autolichter an' (Schwer) is also visible, with text about a car's lights being on. A rich text editor is shown with a toolbar and the text: 'An alle Mitarbeiter! Jemand hat an seinem Fahrzeug auf dem Parkplatz das Licht angelassen. Ein Mitarbeiter hat [ein Foto von dem Fahrzeug gemacht, das ich hier hochgeladen habe](#). Schauen Sie bitte, ob es vielleicht Ihr Fahrzeug ist, damit nachher nicht die Batterie leer ist. Vielen Dank für Ihre Mithilfe! Amena Adnan Hausverwaltung'. A red 'ACME SUPPLIES COMPANY' logo is at the bottom.

Benutzer- Training

- Training-Videos
- Abschlusstest

Phishing Attacks Overview (German



Zurück zu: [Überblick Phishing-A](#)

Phishing Attacks Overview (German – Deutsche) Quiz

1 Wie können Sie überprüfen, ob ein Link legitim ist?

- Auf den Link klicken und nachschauen
- Mit der Maus über den Link fahren und unten im Browserfenster nachschauen
- Rechtsklicken und „In neuem Fenster öffnen“ auswählen
- Einfach das lesen, was in der E-Mail steht, das stimmt immer

2 Sie bekommen eines Tages eine interne E-Mail von einem Kollegen. Sie kennen den Namen nicht, aber die E-Mail-Adresse @ihrunternehmen.com, scheint richtig zu sein. Der Kollege arbeitet in der Personalabteilung und möchte einige Daten für Ihren Rentensparplan überprüfen. Er hat ein Excel-Dokument mit den Daten angehängt. Was sollten Sie tun?

- Versuchen, den Mitarbeiter aus der Personalabteilung ausfindig zu machen, und ihn persönlich zu dem Dokument befragen
- Nachschauen, ob das Dokument echt ist, in Excel-Tabellen kann es ja keine Viren geben
- Ihren Computer auf den Boden werfen und ihn in Einzelteilen zur IT bringen
- Auf die E-Mail antworten und fragen, was ein Rentensparplan ist

3 Richtig oder Falsch: Ein Angriff kann sich über eine E-Mail Zugang zu Ihrem Computer verschaffen.

- Richtig
- Falsch

Best Practices

1. Verwenden Sie die vollständige Festplattenverschlüsselung für alle Computer und die Dateiverschlüsselung für alle vertraulichen Daten
2. Stellen Sie sicher, dass ein effektiver Endbenutzer-, Netzwerk- und E-Mail-Schutz vorhanden ist
3. Erstellen Sie eine Datenschutzrichtlinie, um Mitarbeitern beizubringen, wie Daten sicher aufbewahrt werden
4. Wenden Sie URL-Filter an, um den Zugriff auf nicht autorisierte Cloud-Speicher-Websites zu steuern
5. Erzwingen Sie Data Loss Prevention (DLP) - Steuerelemente für E-Mail



SOPHOS
Security made simple.

Deciphering the Code: A Simple Guide to Encryption

By **Anthony Merry**, Director of Product Management - Data Protection

A business's success is increasingly dependent on its ability to leverage its data. Whether it's achieving top-line growth or improving the bottom line, businesses rely on data to boost sales, drive product innovation, target market customers, and gain competitive advantage. Your data is valuable, but in the wrong hands it could hurt you.

Fragen?



SOPHOS

Security made simple.