Next Generation Technology at a glance

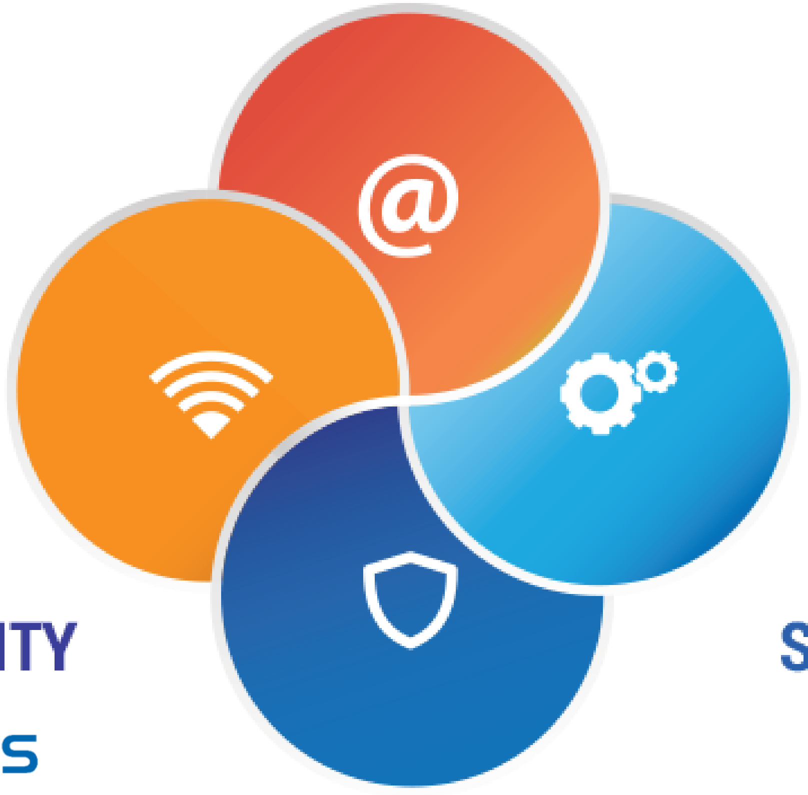
(Synchronized Security vs. Best-of-Breed)

George Kouimintzis
Sales Director NSS (Sophos VAD)

nss
Affordable Cutting Edge

SOPHOS

Product Portfolio



NETWORKING

- Array Networks
- peplink
- mojo Networks

COMMUNICATIONS

- CommuniGate Systems
- PATTON
- GlobalSign GMO Internet Group

SECURITY

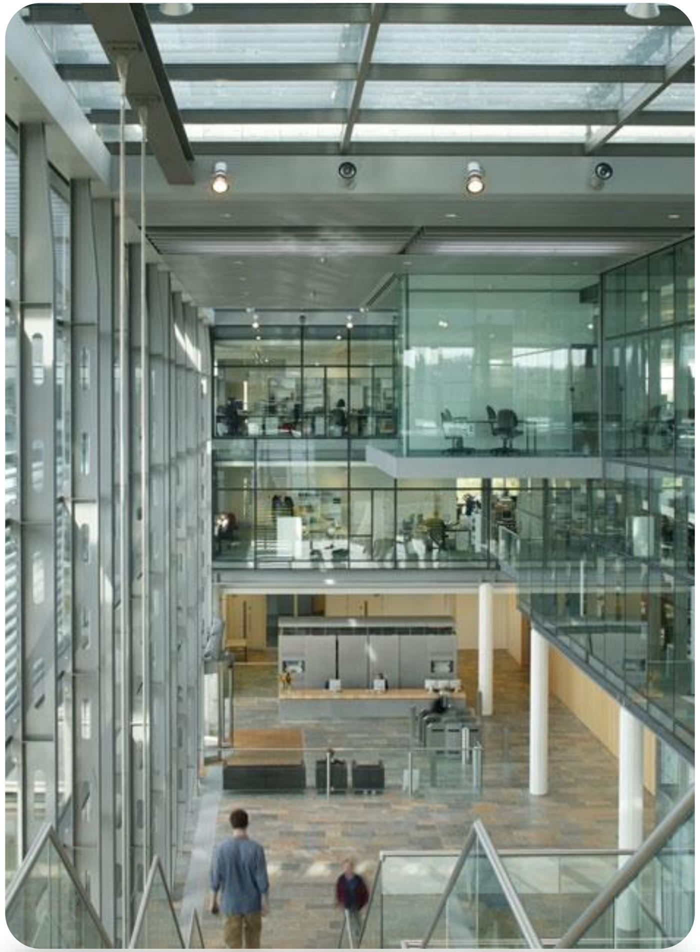
- SOPHOS
- CYBERARK
- iboss
- sealpath

SYSTEMS

- SEP
- logpoint
- PROXMOX
- Jacarta

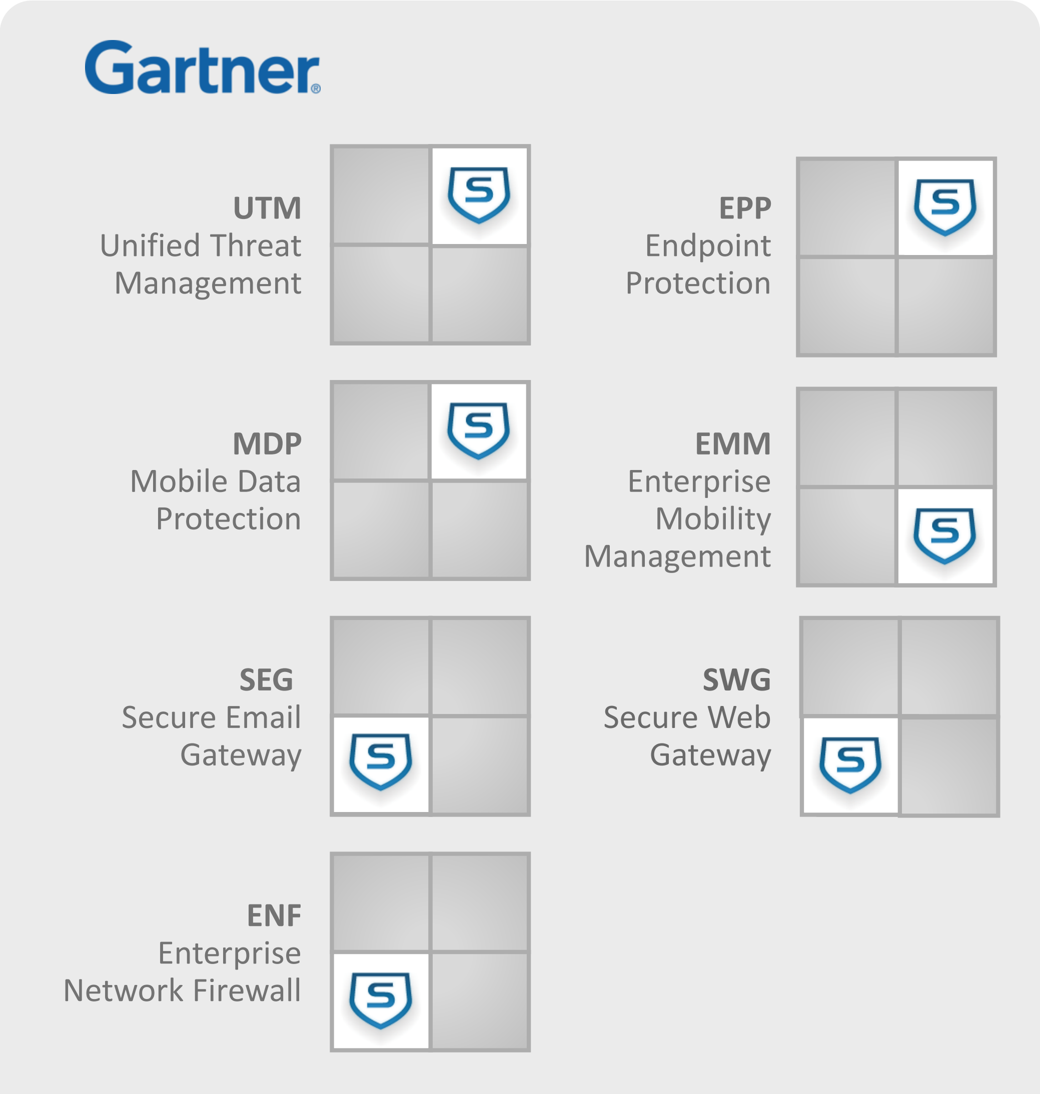
Sophos Snapshot

- Founded 1985 in Oxford, UK
- $534.9+ million in FY16 billings
- Solid cash EBITDA margin (20%+) and strong cash conversion
- 2,700 employees
- Over 200,000 customers
- 100+ million users
- 90%+ best in class renewal rates
- 20,000+ channel partners
- SophosLabs: one of world's leading threat research laboratories
- “Channel first” go to market model
- Key OEM Partners: Cisco, IBM, Juniper, Citrix, Lenovo, Rackspace
- History of organic and acquired growth



Sophos HQ, Abingdon, UK

A Proven Market Leader



Gartner

UTM
Unified Threat
Management

EPP
Endpoint
Protection

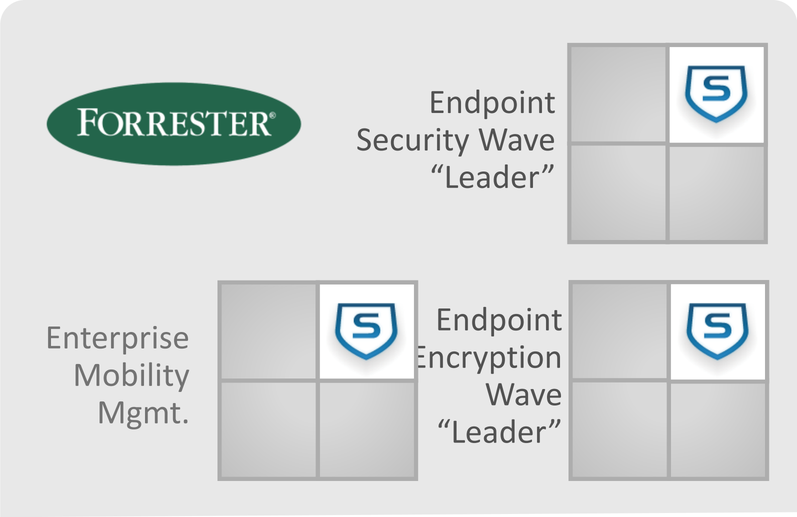
MDP
Mobile Data
Protection

EMM
Enterprise
Mobility
Management

SEG
Secure Email
Gateway

SWG
Secure Web
Gateway

ENF
Enterprise
Network Firewall

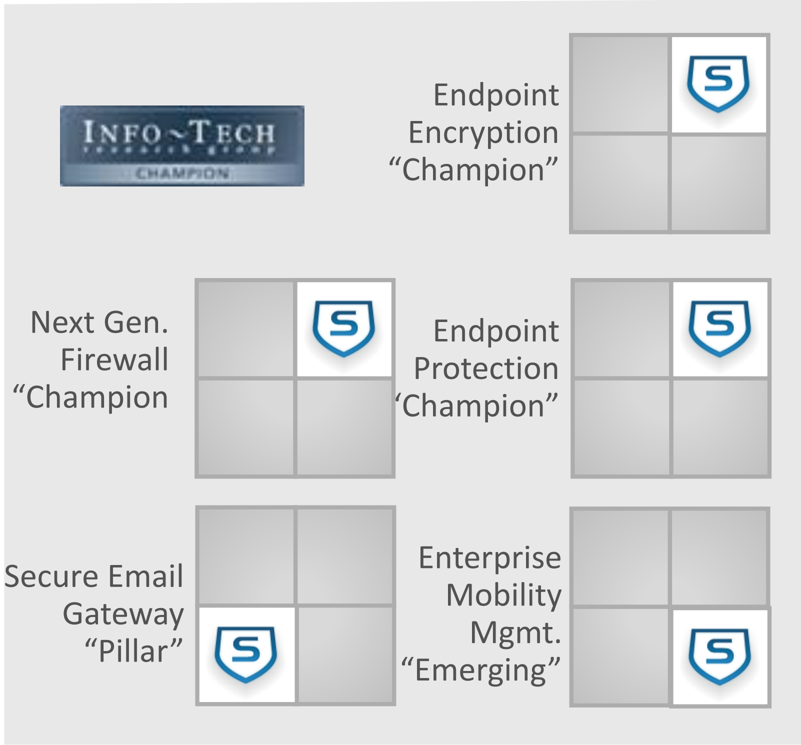


FORRESTER

Endpoint
Security Wave
“Leader”

Enterprise
Mobility
Mgmt.

Endpoint
Encryption
Wave
“Leader”



INFO~TECH research group CHAMPION

Endpoint
Encryption
“Champion”

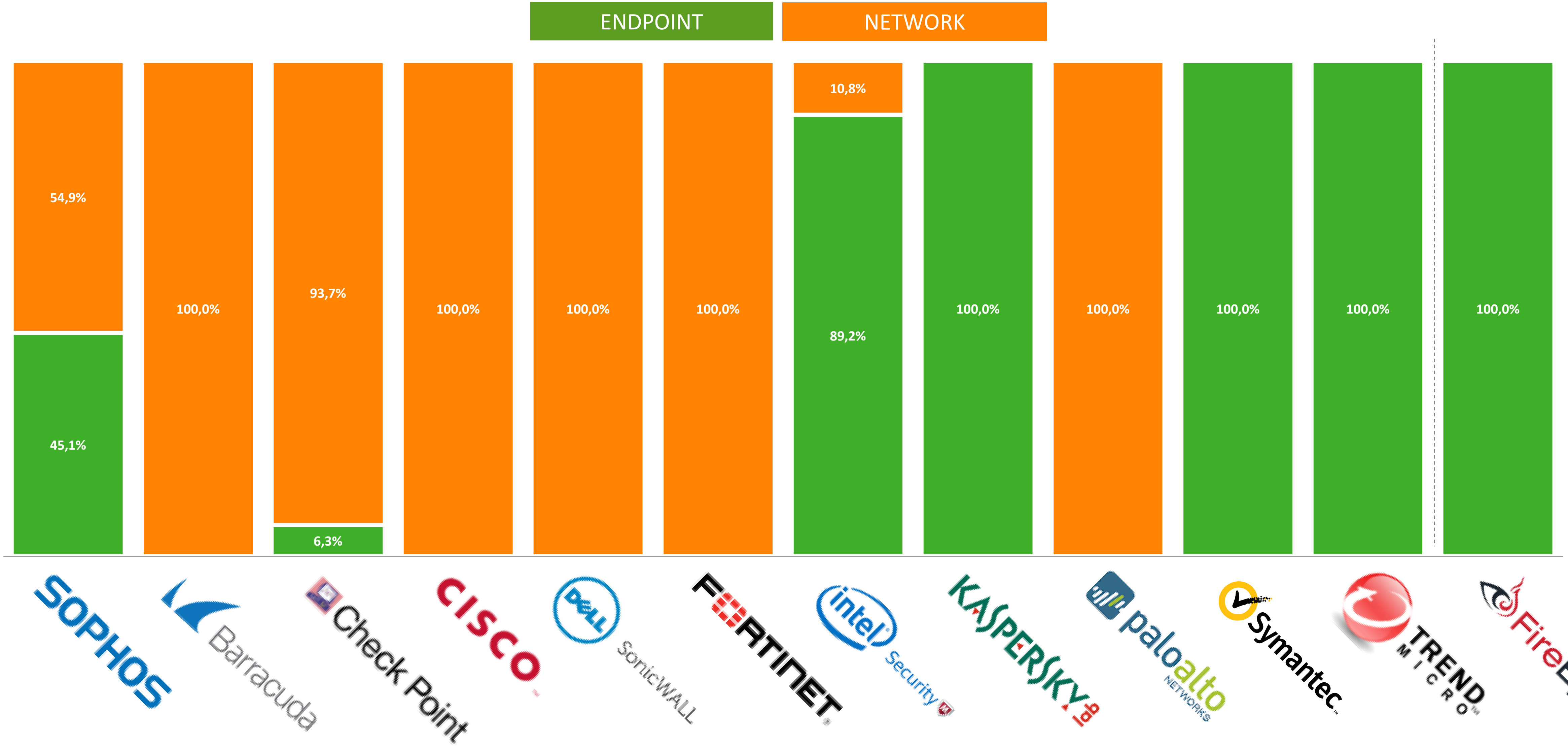
Next Gen.
Firewall
“Champion

Endpoint
Protection
“Champion”

Secure Email
Gateway
“Pillar”

Enterprise
Mobility
Mgmt.
“Emerging”

Unique Balance Between Endpoint and Network



Synchronized Security Platform and Strategy

Admin | Manage All Sophos Products

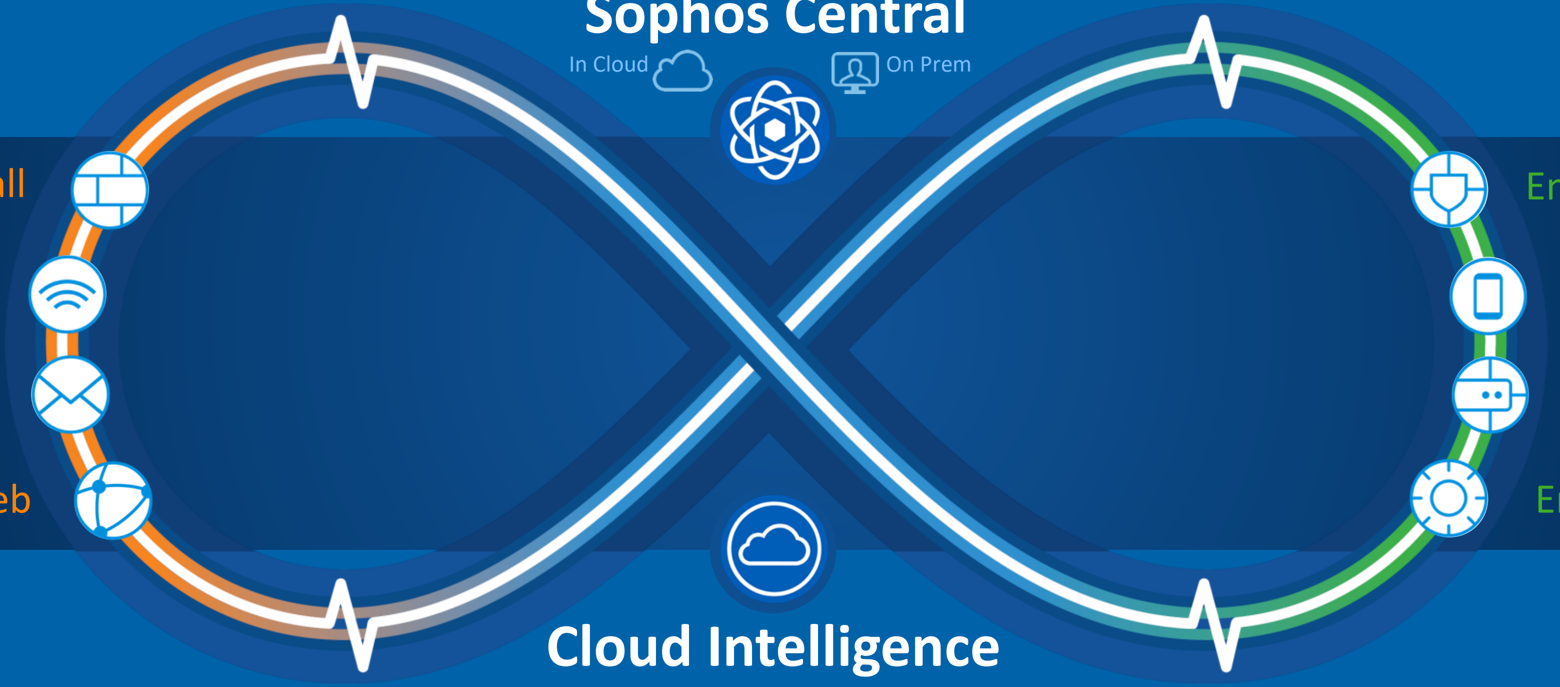
Self Service | User Customizable Alerts

Partner | Management of Customer Installations

Sophos Central

In Cloud

On Prem



UTM/Next-Gen Firewall

Wireless

Email

Web

Endpoint/Next-Gen Endpoint

Mobile

Server

Encryption

Cloud Intelligence

Analytics | Analyze data across all of Sophos' products to create simple, actionable insights and automatic resolutions

Sophos Labs | 24x7x365, multi-continent operation | URL Database | Malware Identities | File Look-up | Genotypes | Reputation | Behavioural Rules | APT Rules
Apps | Anti-Spam | Data Control | SophosID | Patches | Vulnerabilities | Sandboxing | API Everywhere

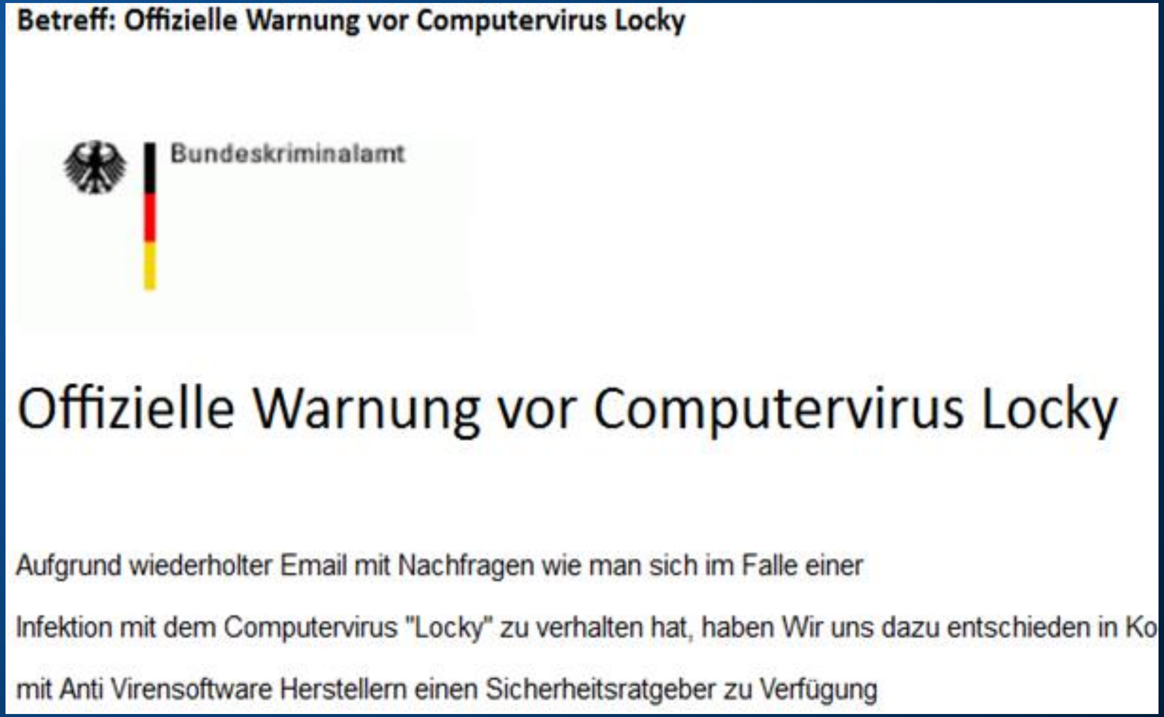
Why is Ransomware so effective?

Affordable Cutting Edge

SOPHOS

Root Cause of Infections despite Best-of-Breed Security

- Office-Documentformats and PDFs are normally allowed in E-Mail based communication
- Security Controls do not work together or act as a system
- Advanced Malware
- Professional Adversaries
- Social Engineering



Betreff: Offizielle Warnung vor Computervirus Locky

Bundeskriminalamt

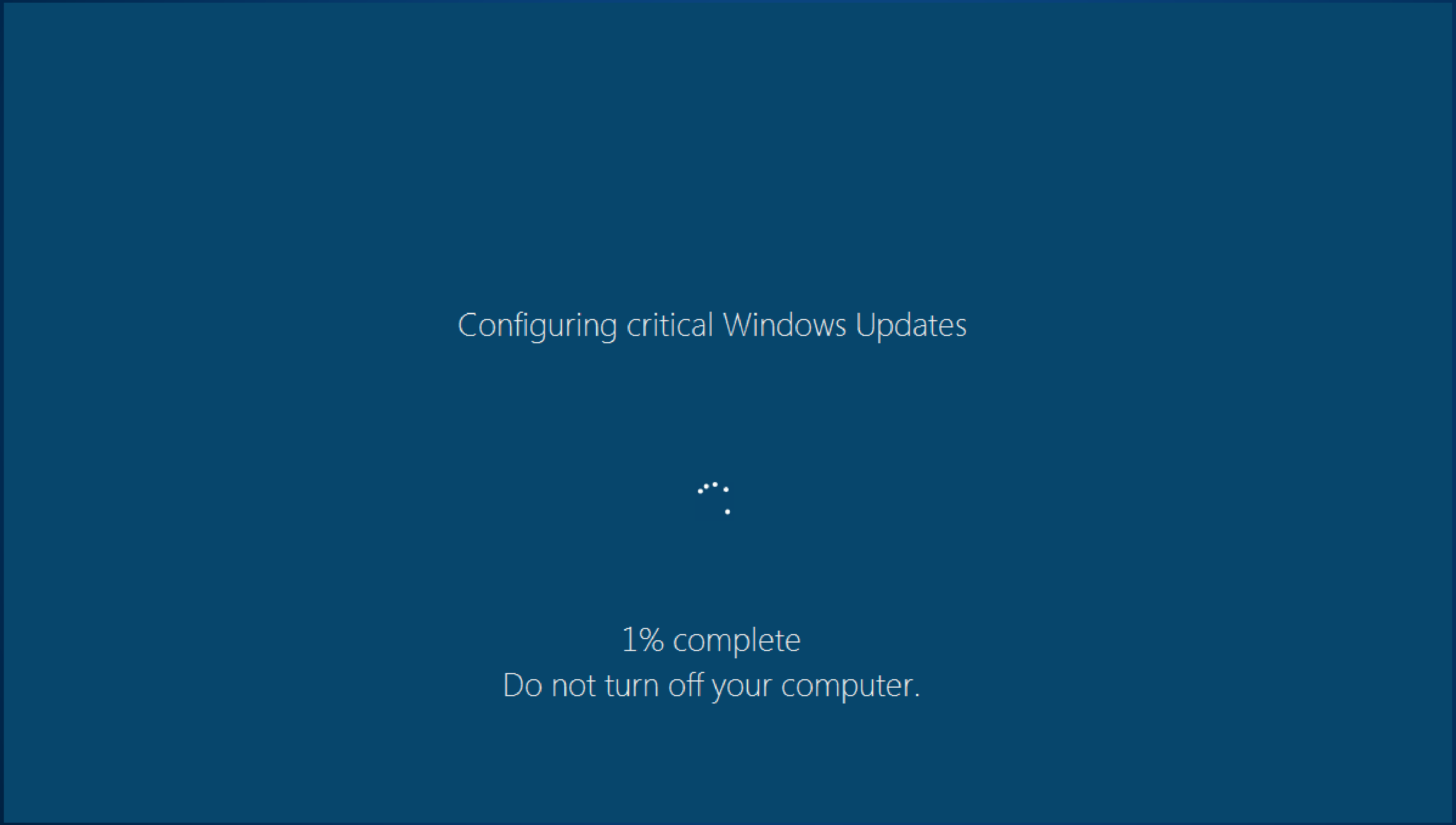
Offizielle Warnung vor Computervirus Locky

Aufgrund wiederholter Email mit Nachfragen wie man sich im Falle einer

Infektion mit dem Computervirus "Locky" zu verhalten hat, haben Wir uns dazu entschieden in Ko

mit Anti Virensoftware Herstellern einen Sicherheitsratgeber zu Verfügung

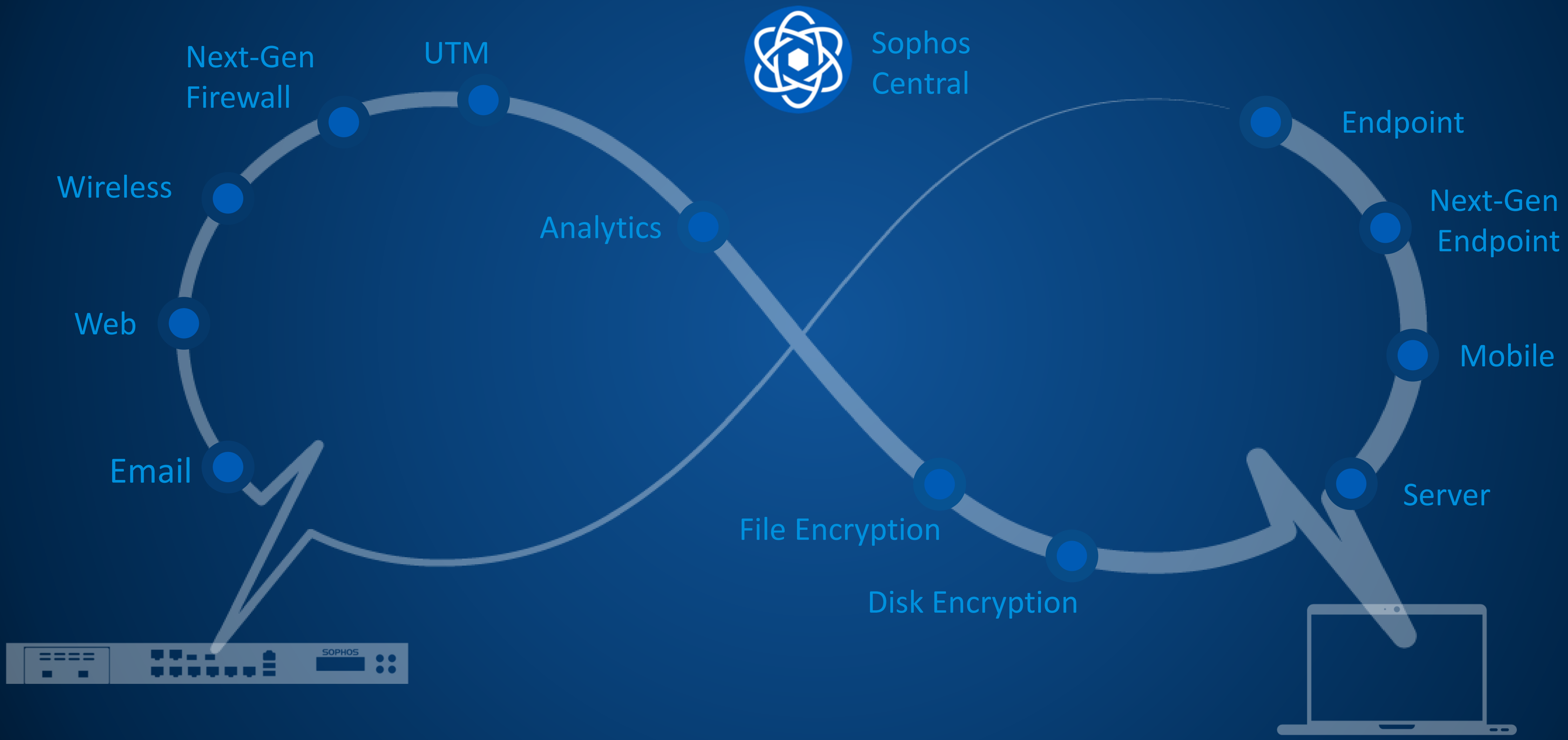
Example Fantom Ransomware



Configuring critical Windows Updates

1% complete
Do not turn off your computer.

Synchronized Security – Teamplay vs. Best-of-Breed

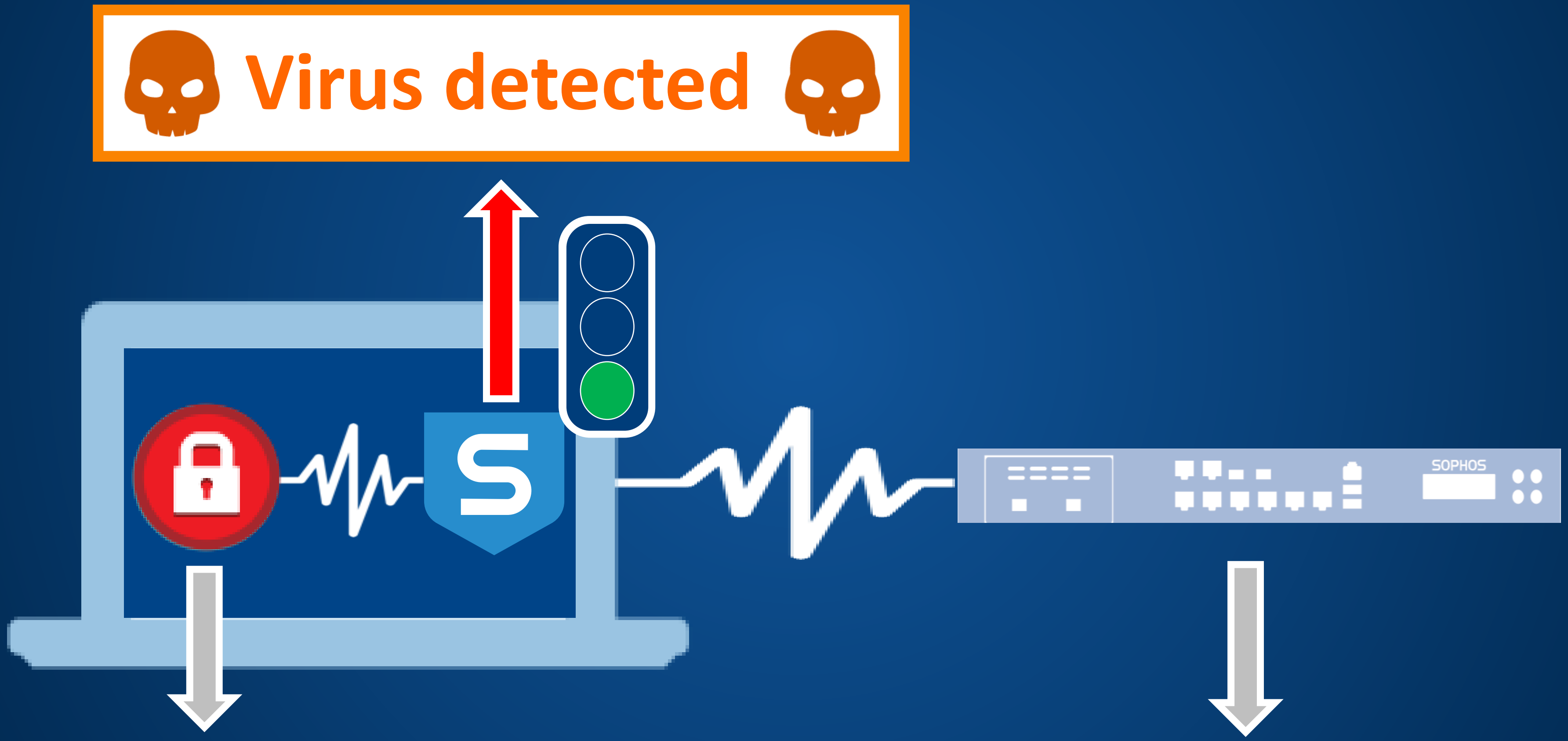


Security Heartbeat

Synchronized Security

Affordable Cutting Edge

Security Heartbeat – Malware Infection

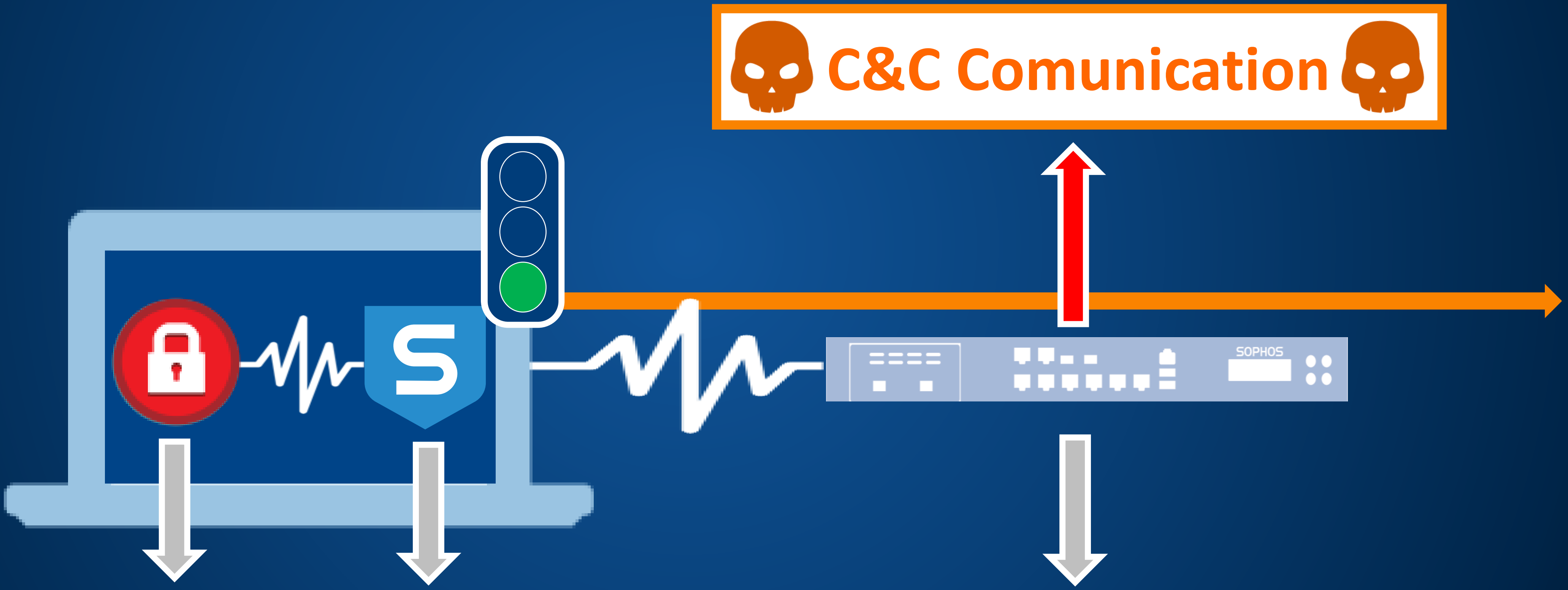


Virus detected

Remove Keys

Network Quarantine of Client

Security Heartbeat – Botnet C&C-Traffic detected



C&C Comunication

Remove Keys

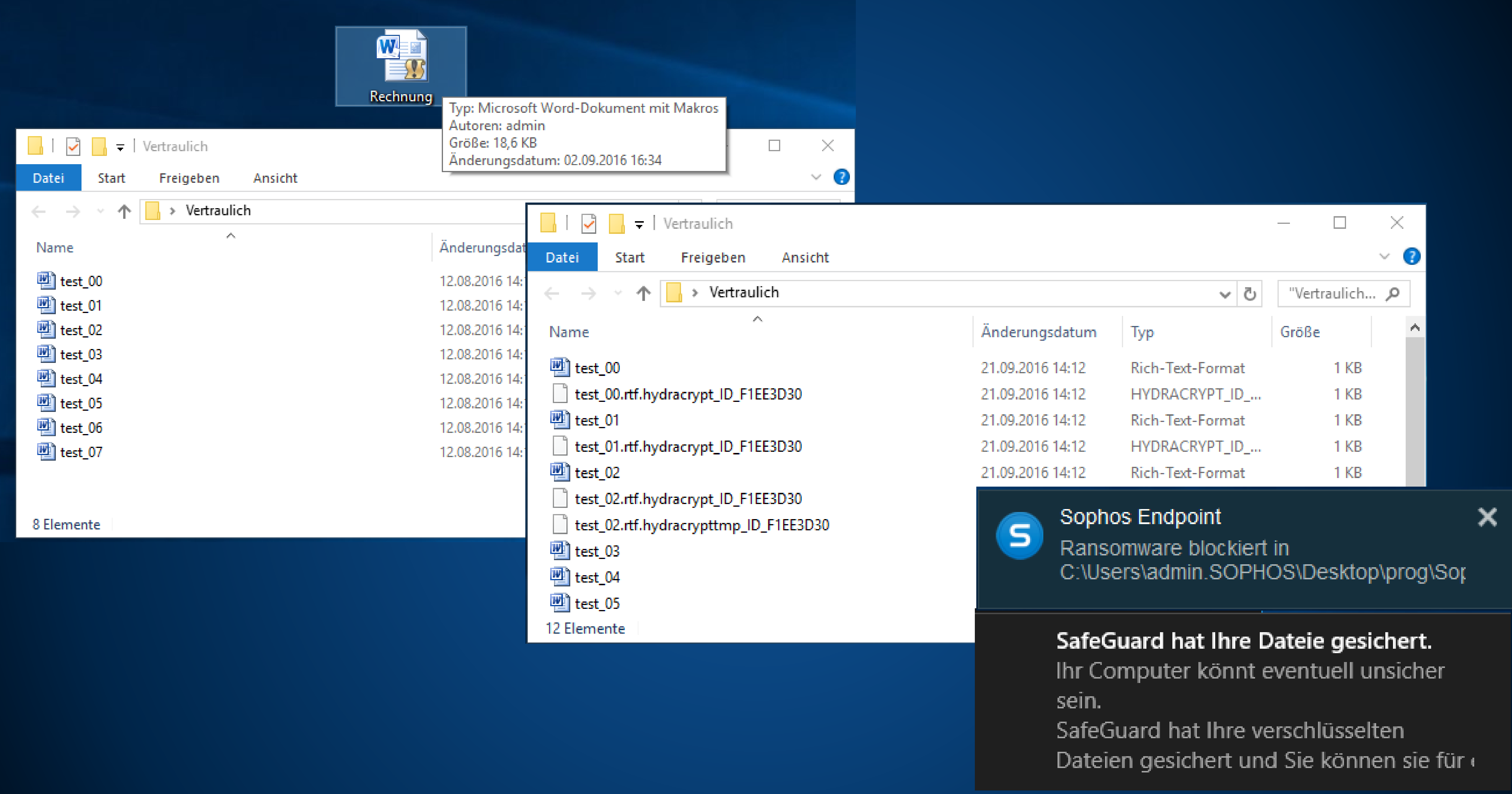
Kill Process

Network Quarantine of Client

Demo

Ransomware

Affordable Cutting Edge



Typ: Microsoft Word-Dokument mit Makros
Autoren: admin
Größe: 18,6 KB
Änderungsdatum: 02.09.2016 16:34

Name	Änderungsdat
test_00	12.08.2016 14:
test_01	12.08.2016 14:
test_02	12.08.2016 14:
test_03	12.08.2016 14:
test_04	12.08.2016 14:
test_05	12.08.2016 14:
test_06	12.08.2016 14:
test_07	12.08.2016 14:

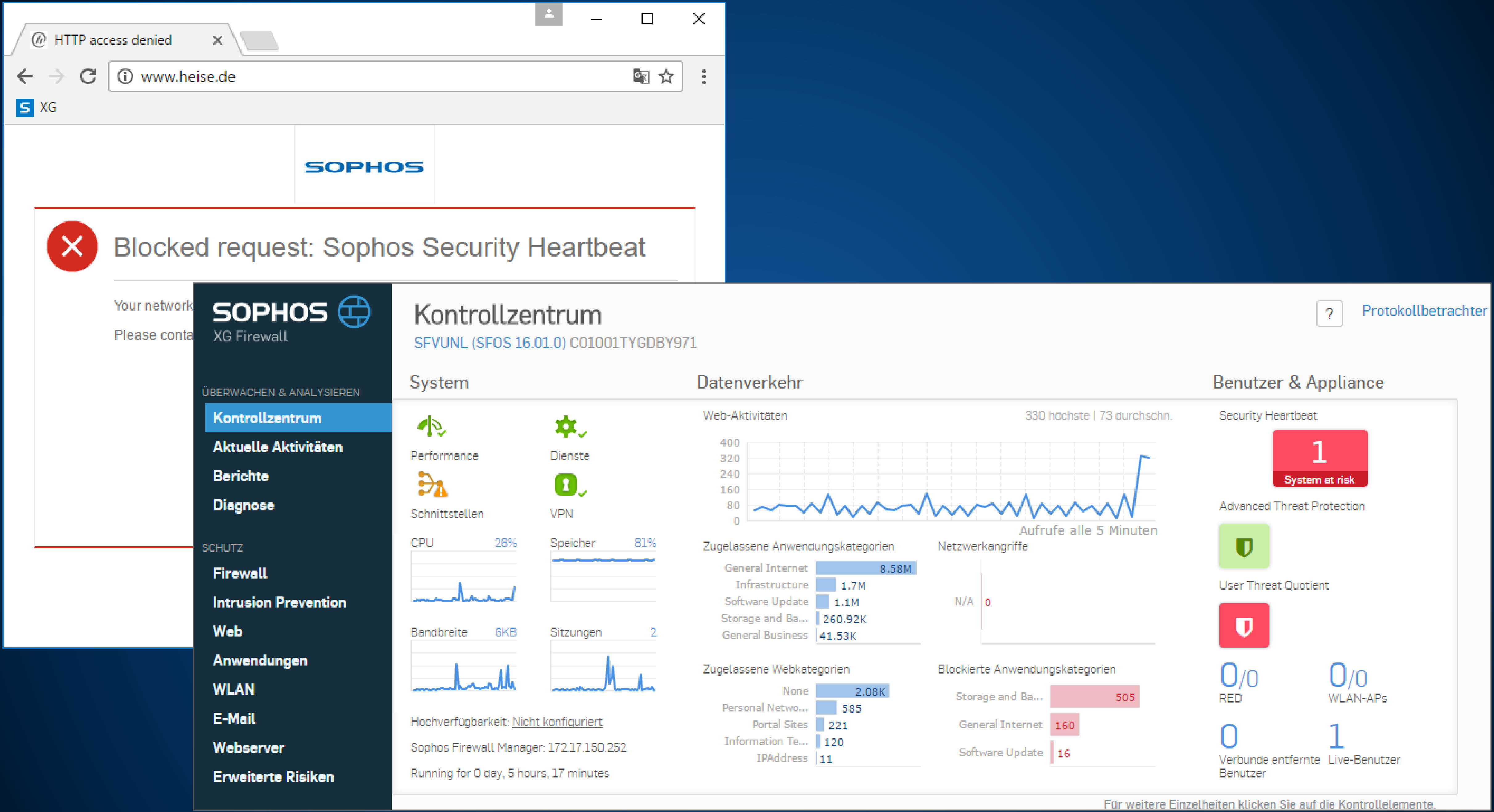
8 Elemente

Name	Änderungsdatum	Typ	Größe
test_00	21.09.2016 14:12	Rich-Text-Format	1 KB
test_00.rtf.hydracrypt_ID_F1EE3D30	21.09.2016 14:12	HYDRACRYPT_ID_...	1 KB
test_01	21.09.2016 14:12	Rich-Text-Format	1 KB
test_01.rtf.hydracrypt_ID_F1EE3D30	21.09.2016 14:12	HYDRACRYPT_ID_...	1 KB
test_02	21.09.2016 14:12	Rich-Text-Format	1 KB
test_02.rtf.hydracrypt_ID_F1EE3D30			
test_02.rtf.hydracrypttmp_ID_F1EE3D30			
test_03			
test_04			
test_05			

12 Elemente

Sophos Endpoint
Ransomware blockiert in
C:\Users\admin.SOPHOS\Desktop\prog\Sop

SafeGuard hat Ihre Dateie gesichert.
Ihr Computer könnt eventuell unsicher sein.
SafeGuard hat Ihre verschlüsselten Dateien gesichert und Sie können sie für



Blocked request: Sophos Security Heartbeat

Your network

Please conta

Kontrollzentrum

SFVUNL (SFOS 16.01.0) C01001TYGDBY971

System

Performance

Dienste

Schnittstellen

VPN

CPU 26%

Speicher 81%

Bandbreite 6KB

Sitzungen 2

Hochverfügbarkeit: Nicht konfiguriert

Sophos Firewall Manager: 172.17.150.252

Running for 0 day, 5 hours, 17 minutes

Datenverkehr

Web-Aktivitäten 330 höchste | 73 durchschn.

Zugelassene Anwendungskategorien

General Internet	8.58M
Infrastructure	1.7M
Software Update	1.1M
Storage and Ba...	260.92K
General Business	41.53K

Netzwerkangriffe

N/A 0

Zugelassene Webkategorien

None	2.08K
Personal Netwo...	585
Portal Sites	221
Information Te...	120
IPAddress	11

Blockierte Anwendungskategorien

Storage and Ba...	505
General Internet	160
Software Update	16

Benutzer & Appliance

Security Heartbeat

1 System at risk

Advanced Threat Protection

User Threat Quotient

0/0 RED

0/0 WLAN-APs

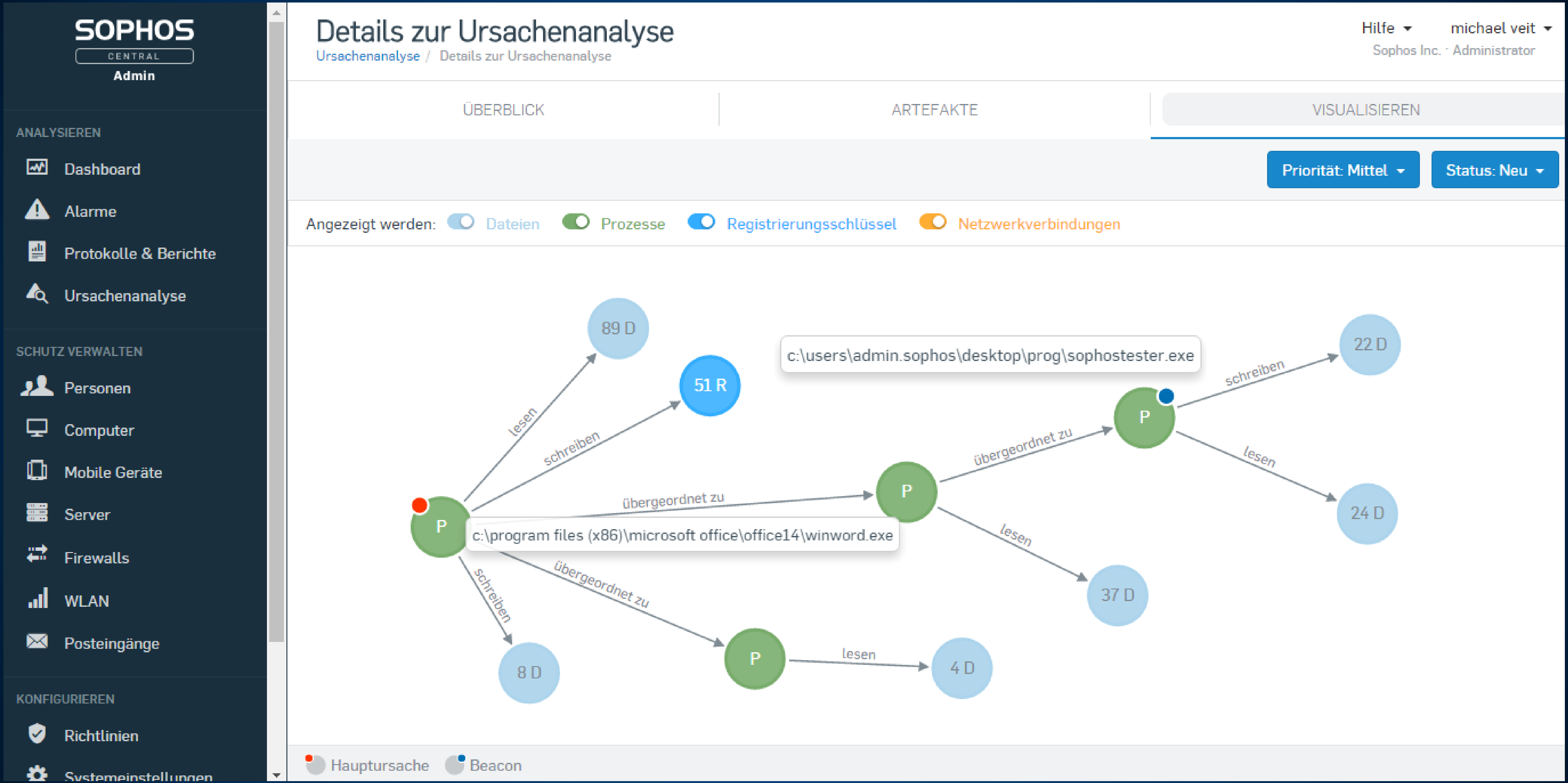
0 Verbunde entfernte Benutzer

1 Live-Benutzer

Für weitere Einzelheiten klicken Sie auf die Kontrollelemente.

SOPHOS

nss Affordable Cutting Edge



Details zur Ursachenanalyse

Ursachenanalyse / Details zur Ursachenanalyse

Priorität: Mittel ▾ Status: Neu ▾

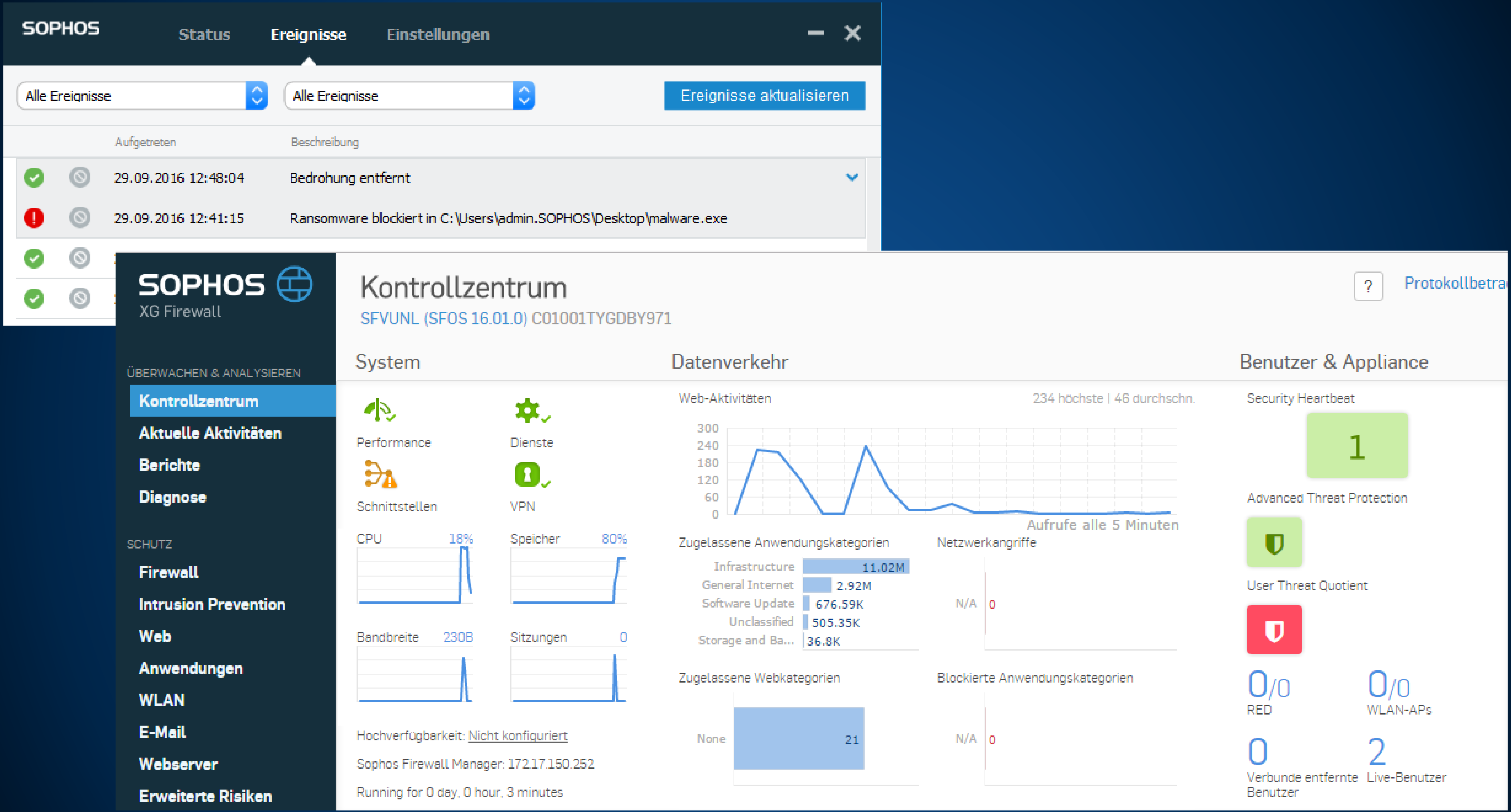
Angezeigt werden: Dateien, Prozesse, Registrierungsschlüssel, Netzwerkverbindungen

c:\users\admin.sophos\desktop\prog\sophostester.exe

c:\program files (x86)\microsoft office\office14\winword.exe

● Hauptursache ● Beacon

SOPHOS



Aufgetreten	Beschreibung
29.09.2016 12:48:04	Bedrohung entfernt
29.09.2016 12:41:15	Ransomware blockiert in C:\Users\admin.SOPHOS\Desktop\malware.exe

Kontrollzentrum

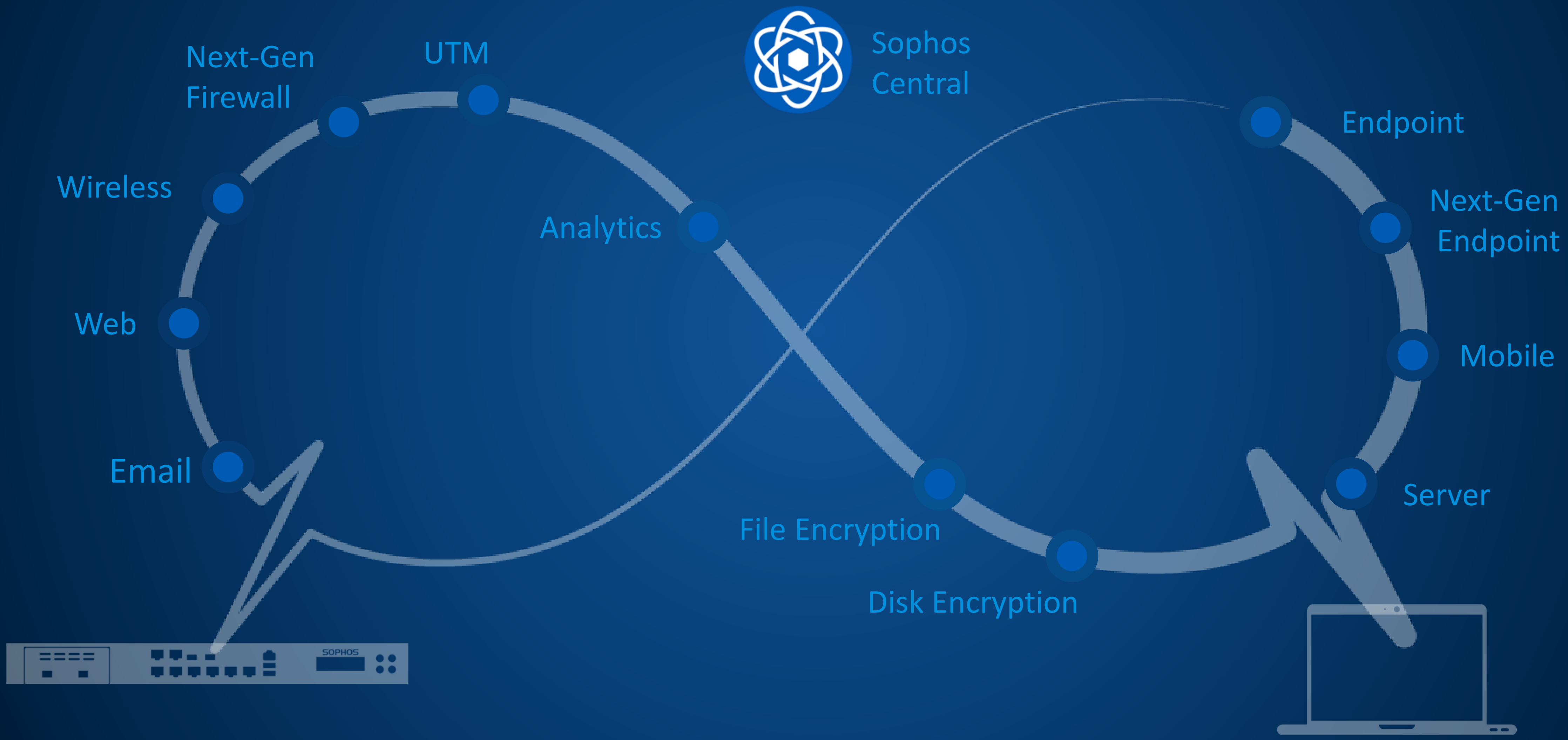
SFVUNL (SFOS 16.01.0) C01001TYGDBY971

Hochverfügbarkeit: Nicht konfiguriert

Sophos Firewall Manager: 172.17.150.252

Running for 0 day, 0 hour, 3 minutes

Synchronized Security – Teamplay vs. Best-of-Breed



Synchronized Security by Sophos

- Best-of-Breed will be replaced by Security as a System
- Intercommunication of Network-, Endpoint- and Encryption Controls are mandatory
- Detection of Advanced Threats (e.g. Exploit techniques)
- Identification of compromised assets in realtime
- Automation of Incident Response and Remediation
- Security Analytics (attack path, trajectories and lateral movement)

SOPHOS

Security made simple.

nss

Affordable Cutting Edge