



**SOPHOS**

**Erleben Sie die Revolution der IT-Sicherheit**

**Sascha Paris**

Snr Sales Engineer

**SOPHOS**

# Synchronized Security - die Zukunft der IT Security

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

# Synchronized Security – Teamplay statt Best-of-Breed



# Heutige Demo der Synchronized Security

Clients und Server

- Windows
- Mac OS X
- Linux

Security Heartbeat

Sophos XG Firewall

Mit Sophos Endpoint



# Sophos INTERCEPT (Sophos Central Managed)



**Anti Ransomware**

## **Stops Crypto Trojans**

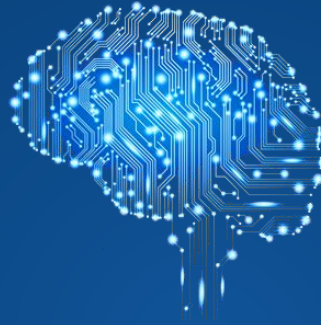
- Detects and Prevents spontaneous file encryption
- «Signatureless»



**Anti Exploit**

## **Mitigates Exploits**

- Protects vulnerable applications against exploits
- Active Adversary Mitigation
- «Signatureless»



**Deep Learning**

## **Deep Learning Recognition**

- Machine Learning based malware recognition
- «Signatureless»



**Cleanup**

## **Malware Cleanup**

- Removal of active malware and malware remnants
- Recovery of compromised system files and settings

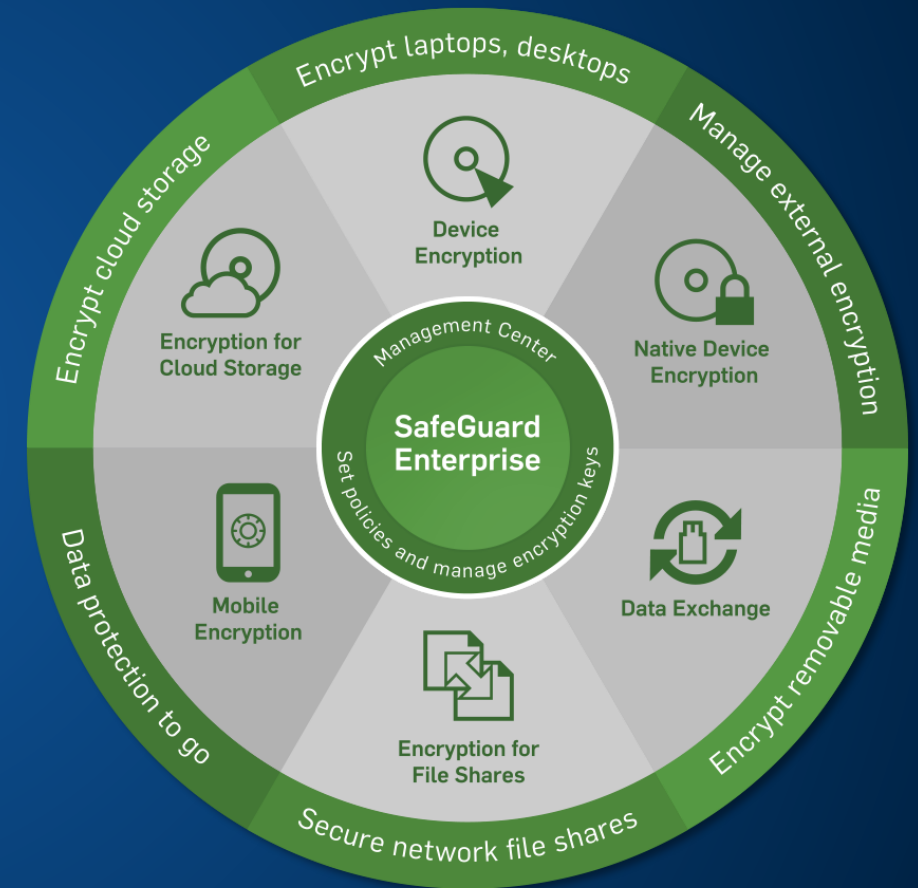


**RCA**

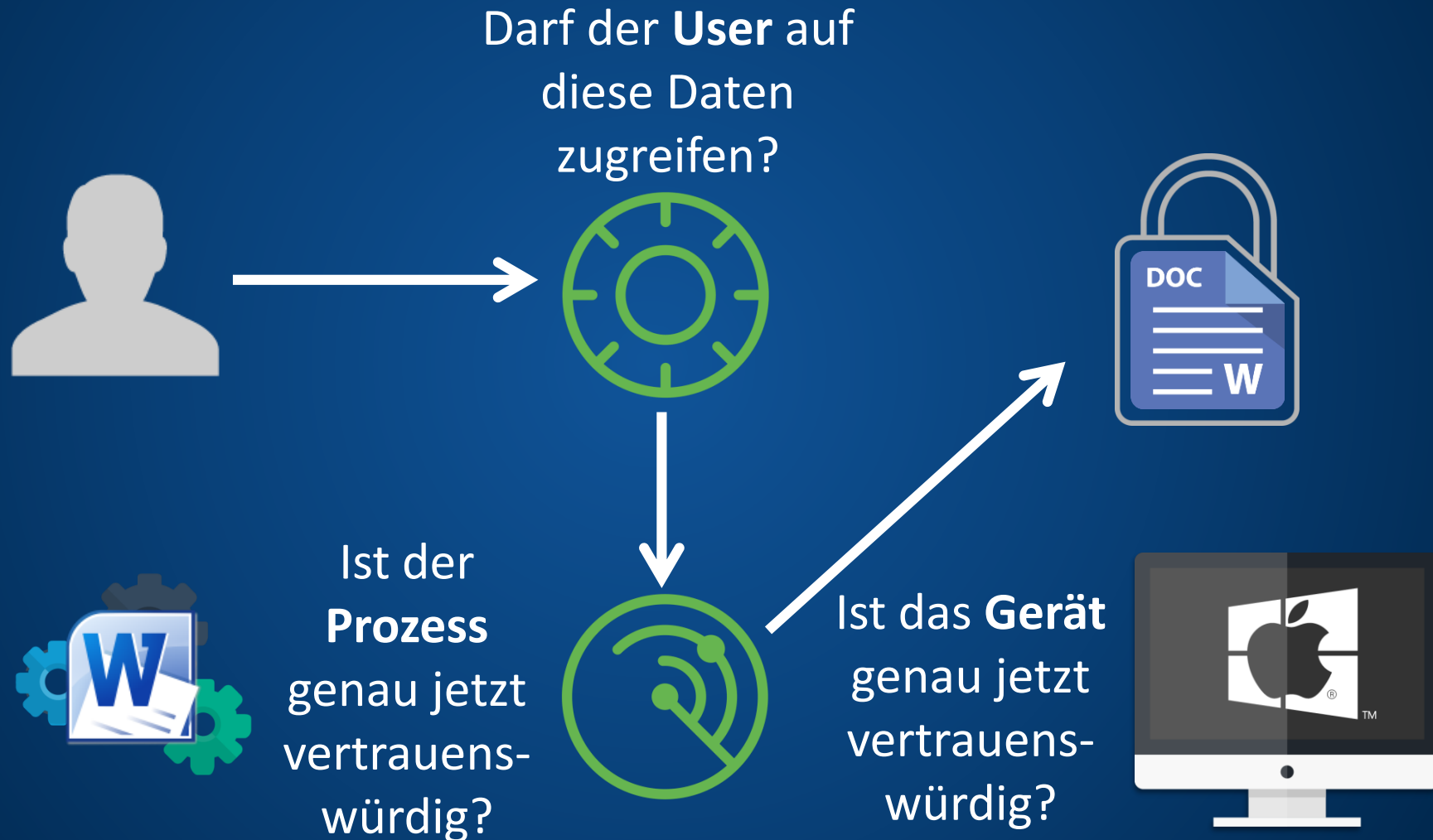
## **Root Cause Analytics**

- Root Cause Analytic
- Visualization of recorded malicious events

# SafeGuard Enterprise – Verschlüsselung überall



# Ablauf beim Zugriff auf verschlüsselte Daten



# Sophos XG Firewall

**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 17.0.0 RC-1) C01001X8JM99W4C

How-To Guides | Log Viewer | Help | admin | Sophos

### System

Performance: Services:   
Interfaces: VPN:

0/0 RED Wireless APs  
0 Live Users

Connected Remote Users: CPU 17% Memory 57%  
Bandwidth 85KB Sessions 0

High Availability: [Not configured](#)  
Sophos Firewall Manager: [Not configured](#)  
Running for 0 day(s), 0 hour(s), 9 minute(s)

### Traffic Insight

Web Activity (5 highest | 5 avg)

Allowed App Categories (Hits every 5 minutes)

Infrastructure	1.92M
Unknown	1.22M
General Internet	709.06K
Unclassified	414.32K
Gaming	894

Network Attacks: N/A 0

Allowed Web Categories

None	735
Portal Sites	35
Software Upda...	29
Information Te...	21
IPAddress	10

Blocked App Categories: N/A 0

### User & Device Insights

Security Heartbeat: Connected

Synchronized Application Control

1 Mapped Apps | 0 New Apps

22 Apps in total detected

Sandstorm: Suspect Malicious Clean

ATP: UTQ:

Click on widgets to open details

### Active Firewall Rules

2 Business	0 User	5 Network	7 Total
------------	--------	-----------	---------

7 Unused | 0 Disabled | 0 Changed | 0 New

### Reports

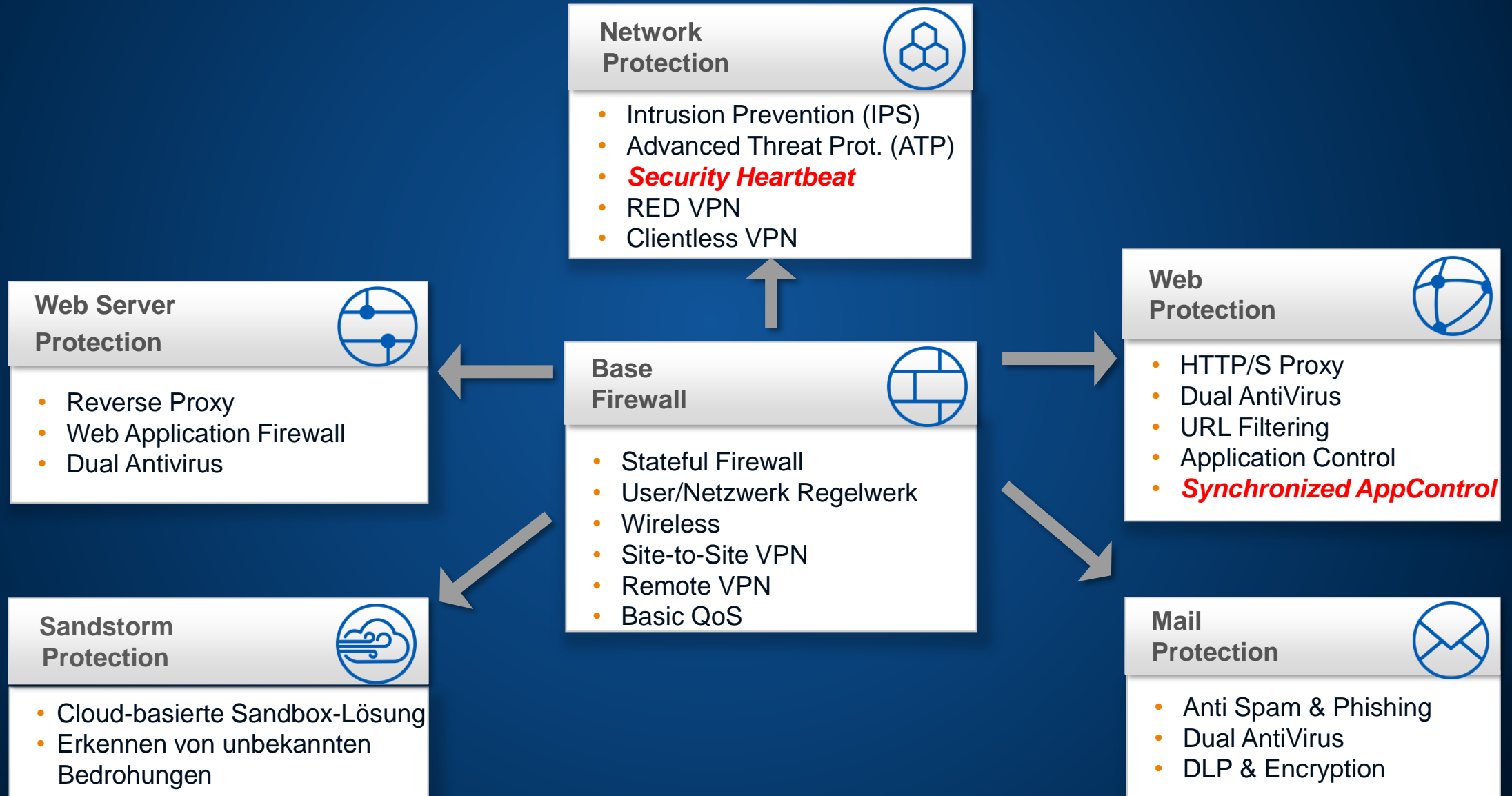
- 5 Risky Apps seen Yesterday
- 5 Objectionable websites seen Yesterday
- 394 MB Used by Top 10 Web users Yesterday
- 0 Intrusion Attacks Yesterday

### Messages

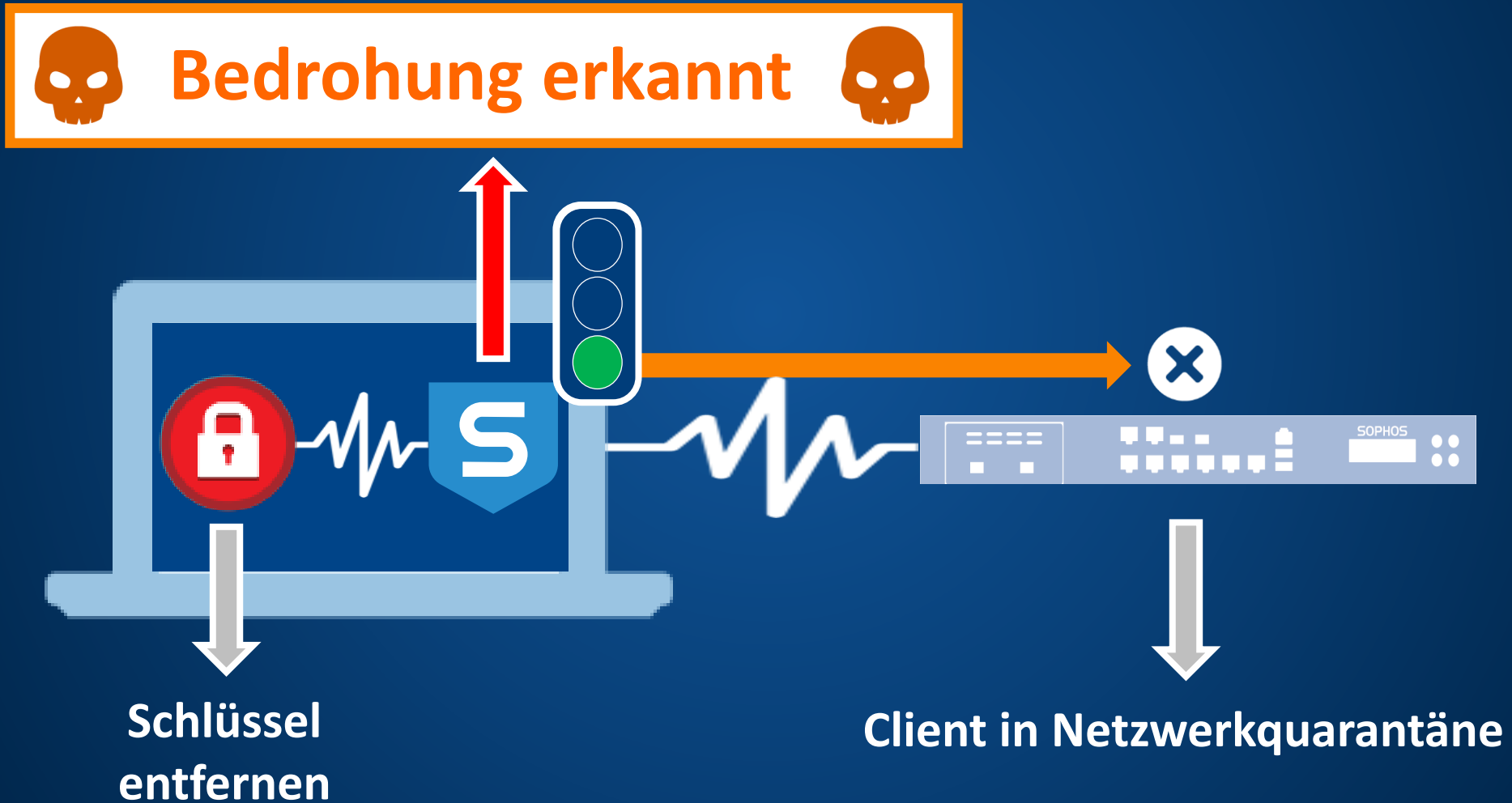
**Warning** 15:24  
HTTPS, SSH-based management is allowed from the ...



# Sophos XG Firewall Technologiemodule



# Security Heartbeat Beispiel: Bedrohung auf Rechner



# Live Demo – Power of Synchronized Security

( Video für Offline Betrachtung: <https://vimeo.com/253967041/6bf44dc5ff> )

**SOPHOS**  
Security made simple.