Sophos revolutioniert IT-Sicherheit mit offenem Ökosystem

SOPHOS

Herausforderungen ....

SOPHOS

Sophos Adaptive Cybersecurity Ecosystem

Sophos Central

Security management and SecOps threat hunting

SOFTWARE

XDR Endpoint EDR Mobile Server Email Encryption Firewall WiFi Cloud

HARDWARE

Firewall Switch RED AP

SERVICES

MTR Rapid Response Professional Services

Open APIs

Industry/Developer

Service Provider

Administrator

Security Operations

THREAT INTELLIGENCE

SOPHOS ARTIFICIAL INTELLIGENCE

SOPHOS LABS

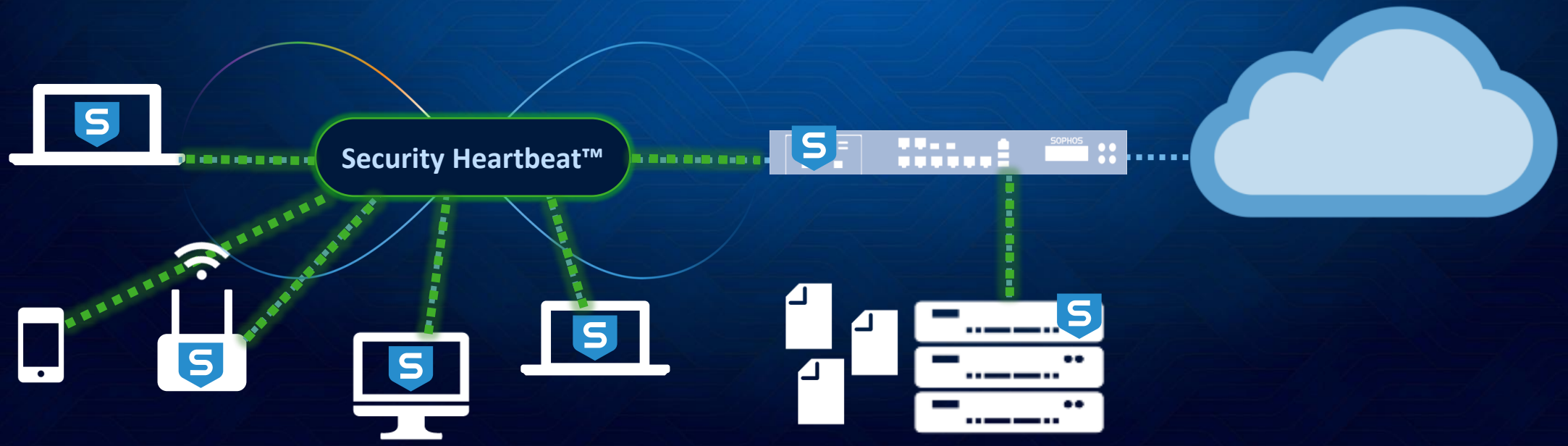
SOPHOS SECURITY OPERATIONS

Data Lake

SOPHOS

Synchronized Security

Clients, Server, Mobilgeräte, WLAN-APs und Firewall kommunizieren per SecurityHeartbeat direkt miteinander

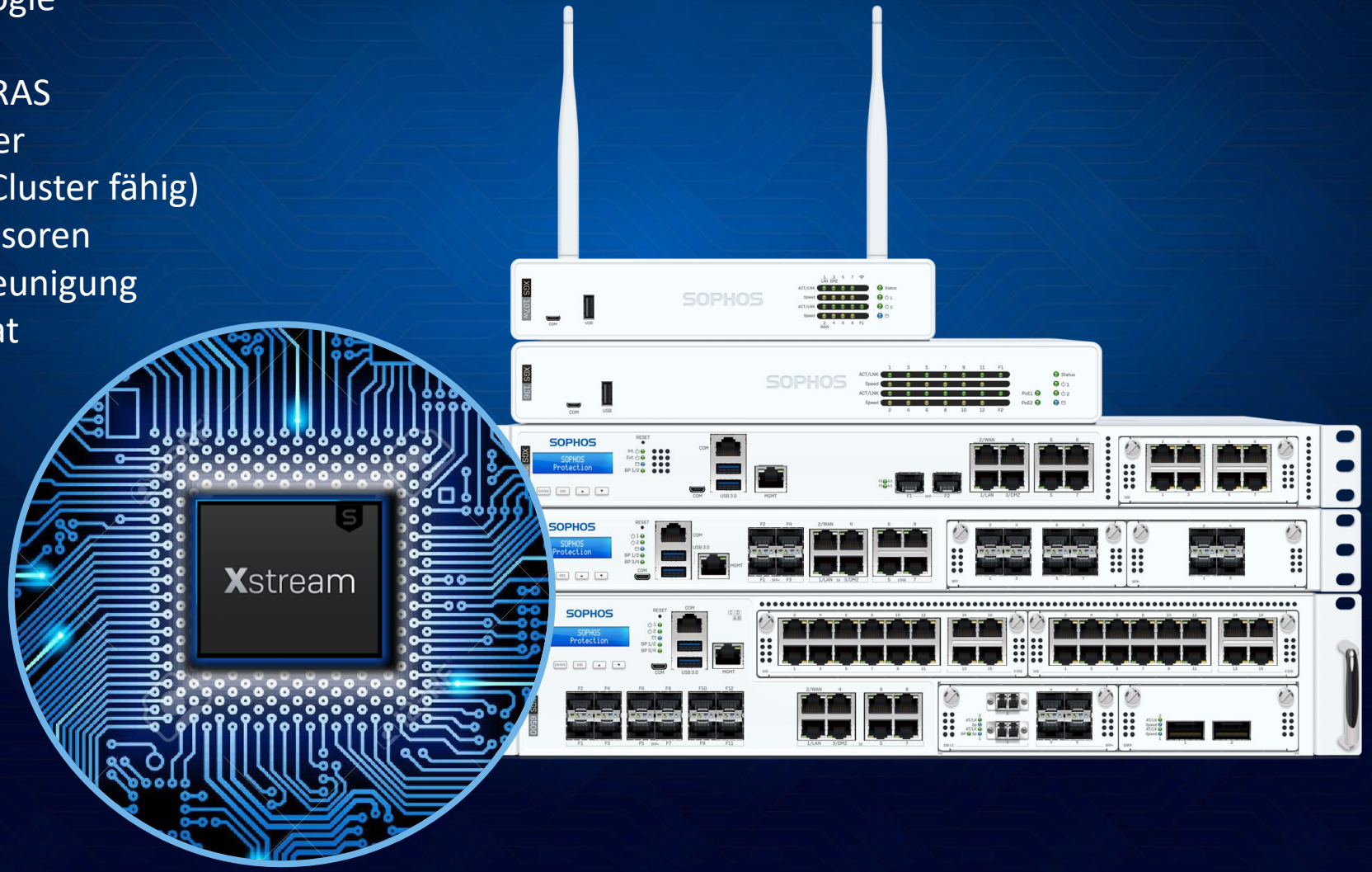


Schutzmöglichkeiten im Überblick

SOPHOS

Sophos Firewall

- Network-, Web-, Mail- und Webserver Protection
- Sandbox Technologie
- IPS, ATP
- VPN für S2S und RAS
- Wireless Controller
- High Availabilty (Cluster fähig)
- Multi Core Prozessoren
- Hardware Beschleunigung
- Security Heartbeat
- FIPS Ready



SOPHOS

Endpoint und Server Schutz

Intercept X Advanced &

Intercept X Advanced for Server

sind **Technologien**

zum Schutz vor Bedrohungen auf Endpoints & Servern

Web Control

Peripheral Control

App Control

Windows Firewall Monitoring

Anti Ransomware

Exploit Prevention

Deep Learning

Server File Integrity Monitoring

Server Lockdown

Active Adversary Mitigations

XDR (EDR)

SOPHOS

Maximaler Schutz - Erkennung + Reaktion

Intercept X Advanced with XDR

(eXtended Detection and Response)*

Technologie & Werkzeug zugleich

für Endpoints, Server, Firewall & Email

- Beinhaltet EDR Funktionen
- Stoppt und bereinigt Bedrohungen
- Erkennt Hackeraktivität ...
- … durch Korrelation von Ereignissen über viele Produkte und Technologien wie Endpoint, Server, Firewall, Email,...

*ersetzt EDR und entspricht dem “Stand der Technik”

XDR vs. EDR

XDR verbessert nicht nur die Produktivität von Sicherheitsabläufen sondert erhöht die Erkennungs- und Reaktionsfähigkeit, in dem mehrere Sicherheitskomponenten in ein einheitliches Ganzes integriert werden.

- Endpoint
- Server

- EDR

- Firewall
- E-Mail
- Cloud
- Mobile

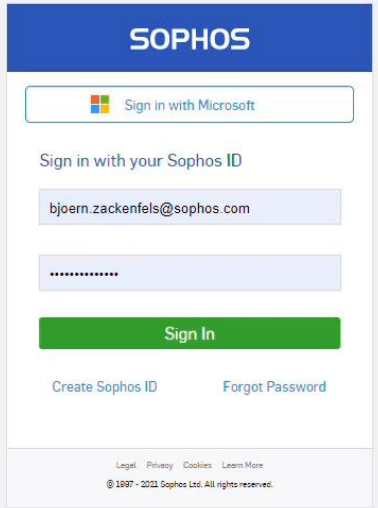
- XDR

- Produktübergreifende Datenquellen
- Produktübergreifende Abfragen
- Sophos Data Lake
- 30 Tage Data Lake Aufbewahrungsfrist
- Aufbewahrungsfrist für On-Disk-Daten
- SQL-Abfragebibliothek
- Alle Intercept X Produktionsfunktionen

XDR - IT Operations

SOPHOS

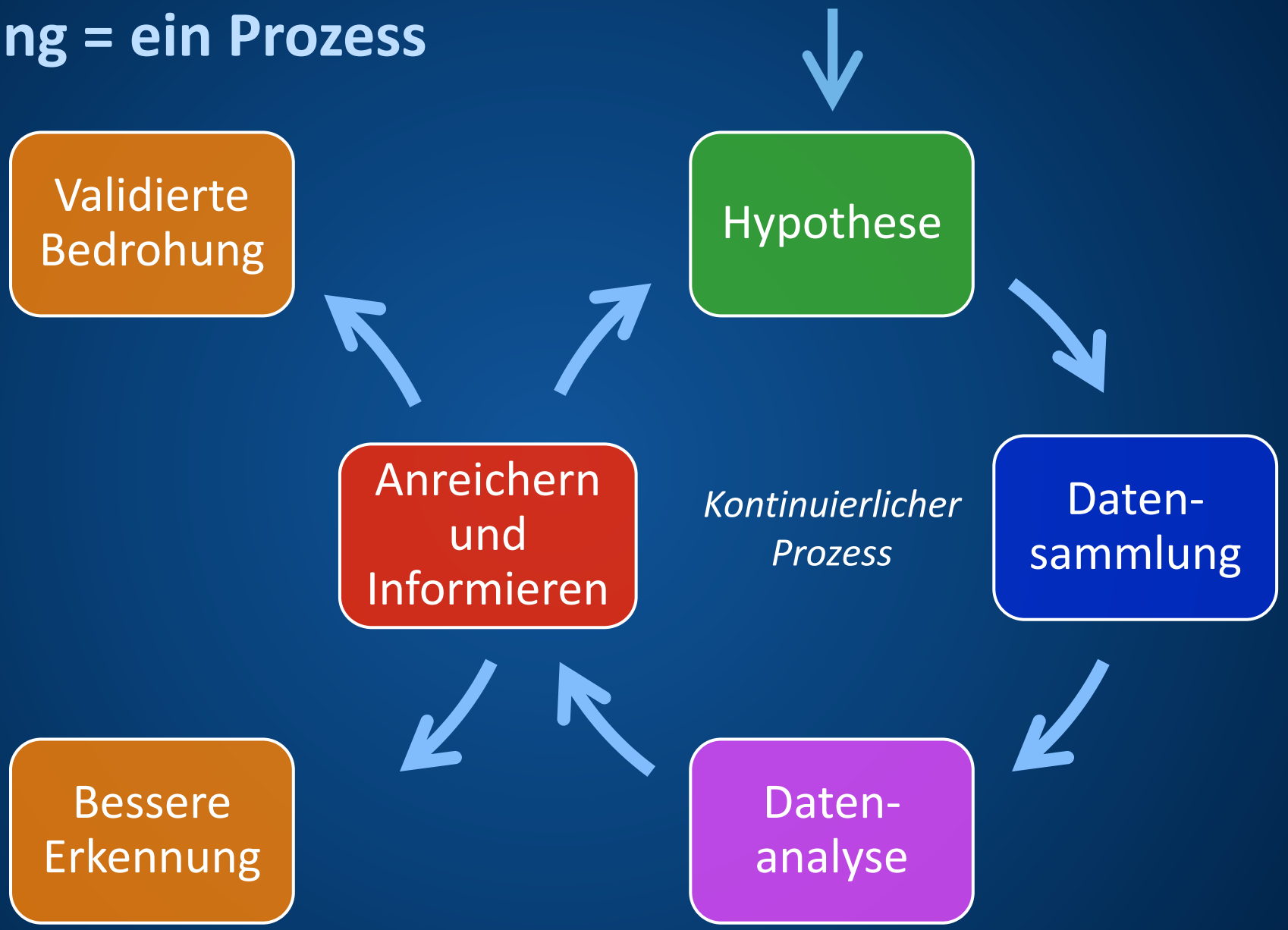
XDR IT Operations



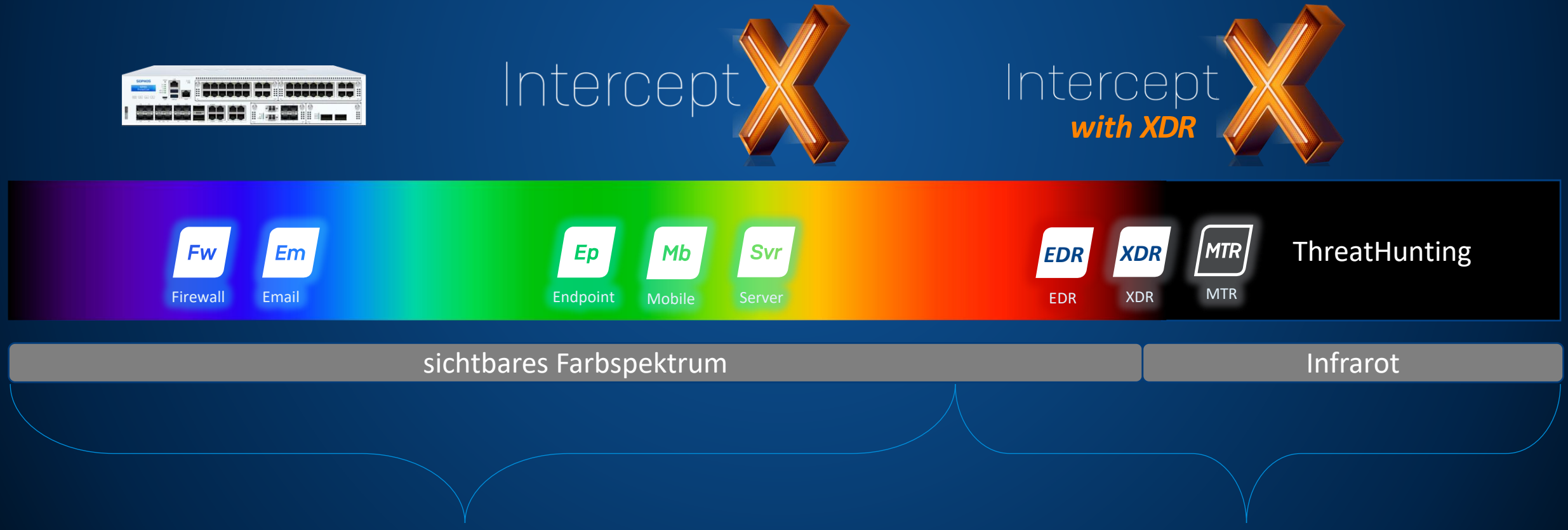
XDR - Threat Hunting

SOPHOS

Threat Hunting = ein Prozess



Bedrohungsspektrum



MTR

SOPHOS

Managed Service - Schutz vor Angriffen

Sophos Managed Threat Response

Intercept X with **XDR + Service von Sophos**

- 24/7 Angriffserkennung
- 24/7 Stoppen und Bereinigung von Bedrohungen
- 24/7 Threat Hunting
- Proaktive Verbesserung der Sicherheit

24/7 team of analysts	Average time to detect ~2 minutes	Average time to respond ~20 minutes	Average time to resolve ~35 minutes

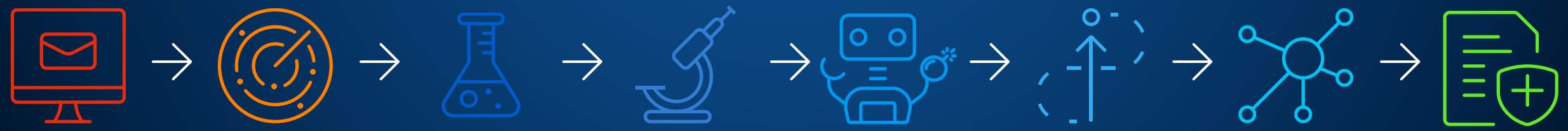
Ein Fallbeispiel

Bei der Jagd nach einer Ransomware

kommt ein historischer Bank Trojaner zu Tage

Unentdeckte · Entdeckt · Triage/Analyse · Eingrenzung/Neutralisierung

START	15 Min	38 Min	1 Std 11 Min	1 Std 32 Min	1 Std 45 Min	1 Std 52 Min	2 Std 6 Min
Ein Kunde meldet sich per E-Mail und teilt mit, dass sein Lieferant von Ransomware betroffen ist. Das Sophos MTR-Team beginnt sofort mit der Untersuchung, um festzustellen, ob der Kunde ein entsprechendes Ziel ist.	Das MTR-Team findet keine Hinweise auf Ransomware, aber eine verhaltensbasierte Erkennung für ein stark verschleiertes .js-Skript, das Sophos zuvor bei der Ausführung blockiert hatte.	Das MTR-Team sendet Dateisamples zur Analyse an die SophosLabs und fordert Indicators of Compromise (IOCs) an, um die Suche fortzusetzen.	Proaktive Suche nach potenziellen Bedrohungen und Vorfällen und deren Validierung Es wird eine neue Erkennung für das .js-Skript erstellt, um alle Kunden zu schützen.	Mithilfe der IOCs lokalisiert das MTR-Team einen Prozess, der zuvor einen C2 angerufen hat. Das Team ist sehr zuversichtlich, dass es sich bei dieser Bedrohung um eine Qbot-Variante handelt.	Die SophosLabs stellen weitere IOCs von Dateipfaden und Details eines geplanten Tasks bereit, mit dem das Skript interagierte. Das MTR-Team setzt seine Ermittlungen fort.	Das MTR-Team nutzt die IOCs, um historische Ausführungen zu lokalisieren, und den Aktualisierungs- und Persistenzmechanismus der Bedrohung.	Der Fall ist abgeschlossen. Das MTR-Team hat alle verbleibenden Artefakte vom Host entfernt und den Kunden über alle Einzelheiten informiert.



1 2 3 4 5 6 7 8

SOPHOS

https://news.sophos.com/en-us/2020/08/18/mtr-casebook-the-ransomware-hunt-that-unearthed-a-historic-banking-trojan/

Sophos Cybersecurity Ecosystem

Sophos Central
Security management and SecOps threat hunting

SOFTWARE

XDR Endpoint EDR Mobile Server Email Encryption Firewall WiFi Cloud

HARDWARE

Firewall Switch RED AP

SERVICES

MTR Rapid Response Professional Services

Open APIs

Industry/Developer
Service Provider
Administrator
Security Operations

THREAT INTELLIGENCE

SOPHOS ARTIFICIAL INTELLIGENCE

SOPHOS LABS

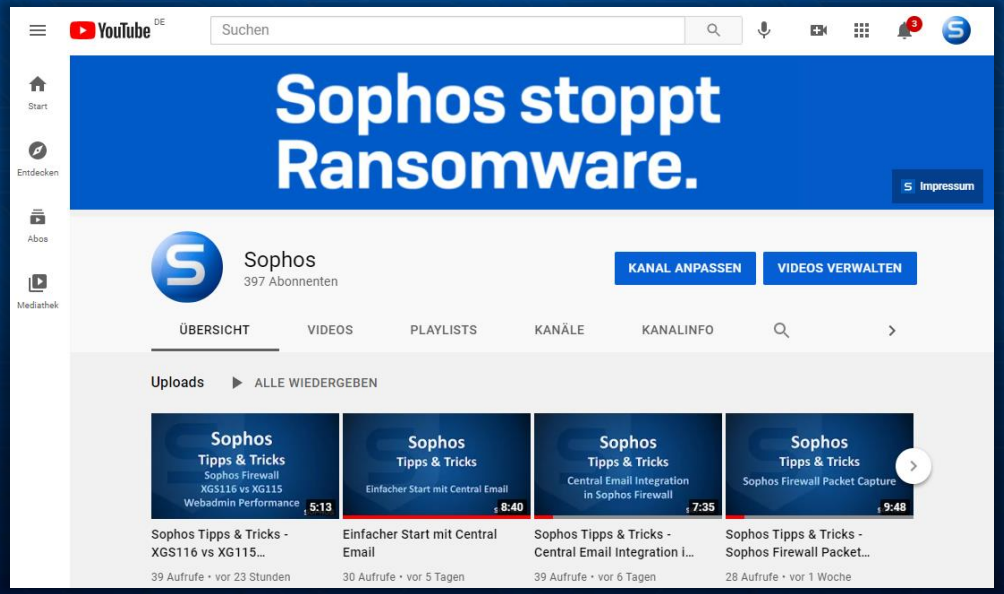
SOPHOS SECURITY OPERATIONS

Data Lake

Weitere Informationen

Deutscher Sophos YouTube-Channel mit aktuellen News sowie Tipps & Tricks

https://www.youtube.com/channel/UC1bWjHhlBPp8TRCzRY1BxA



Endpoint Security – Funktionen im Überblick

	Intercept X Essentials	Intercept X Advanced	Intercept X with XDR	Sophos Managed Threat Response Standard	Sophos Managed Threat Response Advanced
Device / Web / App Control / DLP		✓	✓	✓	✓
Live Protection / Host-IPS / AV-Signaturen / AMSI-Scan	✓	✓	✓	✓	✓
Malicious Traffic Detection (MTD) / Netzwerk-IPS	✓	✓	✓	✓	✓
Deep Learning, Exploit Prevention	✓	✓	✓	✓	✓
Anti-Hacker-Technologien (Anti-Passwortdiebstahl etc.)	✓	✓	✓	✓	✓
Anti-Ransomware (Dateien/Festplatten/Netzlaufwerke)	✓	✓	✓	✓	✓
Mehrere Richtlinien für unterschiedliche Geräte/Nutzergruppen		✓	✓	✓	✓
Grafische Ursachenanalyse		✓	✓	✓	✓
Malware-Analyse per DeepLearning und SophosLabs			✓	✓	✓
Live-Discover Abfragen für Threat Hunting und IT Operations			✓	✓	✓
Live-Response für Remote-Terminal-Zugriff			✓	✓	✓
Unternehmensweite Suche und Eindämmung von Bedrohungen			✓	✓	✓
Security Heartbeat inkl. automatischer Client-Isolation	✓	✓	✓	✓	✓
Manuelle Client-Isolation			✓	✓	✓
Lokale Speicherung von Ereignissen bis zu 90 Tagen			✓	✓	✓
Sophos Data Lake (Cloud-Datenspeicher) für 30 Tage			✓	✓	✓
Produktübergreifende Datenquellen (Endpoint, Firewall, Email, Cloud..)			✓	✓	✓
24/7 Angriffserkennung durch Sophos				✓	✓
24/7 indizienbasiertes Threat Hunting durch Sophos Spezialisten				✓	✓
24/7 Beseitigung und Bereinigung von Bedrohungen				✓	✓
24/7 indizienloses Threat Hunting durch Sophos Spezialisten					✓
Proaktive Verbesserung der Sicherheit, persönlicher Ansprechpartner					✓

SOPHOS

Server Security – Funktionen im Überblick

	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Sophos Managed Threat Response Standard	Sophos Managed Threat Response Advanced
Device / Web / App Control / DLP		✓	✓	✓	✓
Live Protection / Host-IPS / AV-Signaturen / AMSI-Scan	✓	✓	✓	✓	✓
Malicious Traffic Detection (MTD) / Netzwerk-IPS	✓	✓	✓	✓	✓
Deep Learning, Exploit Prevention, Anti-Hacker-Technologien	✓	✓	✓	✓	✓
Anti-Ransomware (Dateien/Festplatten/Netzlaufwerke)	✓	✓	✓	✓	✓
Server Lockdown - automatisiertes Whitelisting		✓	✓	✓	✓
Mehrere Richtlinien für unterschiedliche Servergruppen		✓	✓	✓	✓
Grafische Ursachenanalyse		✓	✓	✓	✓
Malware-Analyse per DeepLearning und SophosLabs			✓	✓	✓
Live-Discover Abfragen für Threat Hunting und IT Operations			✓	✓	✓
Live-Response für Remote-Terminal-Zugriff			✓	✓	✓
Unternehmensweite Suche und Eindämmung von Bedrohungen			✓	✓	✓
Security Heartbeat inkl. automatischer Client-Isolation	✓	✓	✓	✓	✓
Manuelle Client-Isolation			✓	✓	✓
Lokale Speicherung von Ereignissen bis zu 90 Tagen			✓	✓	✓
Sophos Data Lake (Cloud-Datenspeicher) für 30 Tage			✓	✓	✓
Produktübergreifende Datenquellen (Endpoint, Firewall, Email, Cloud..)			✓	✓	✓
24/7 Angriffserkennung durch Sophos				✓	✓
24/7 indizienbasiertes Threat Hunting durch Sophos Spezialisten				✓	✓
24/7 Beseitigung und Bereinigung von Bedrohungen				✓	✓
24/7 indizienloses Threat Hunting durch Sophos Spezialisten					✓
Proaktive Verbesserung der Sicherheit, persönlicher Ansprechpartner					✓

SOPHOS