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

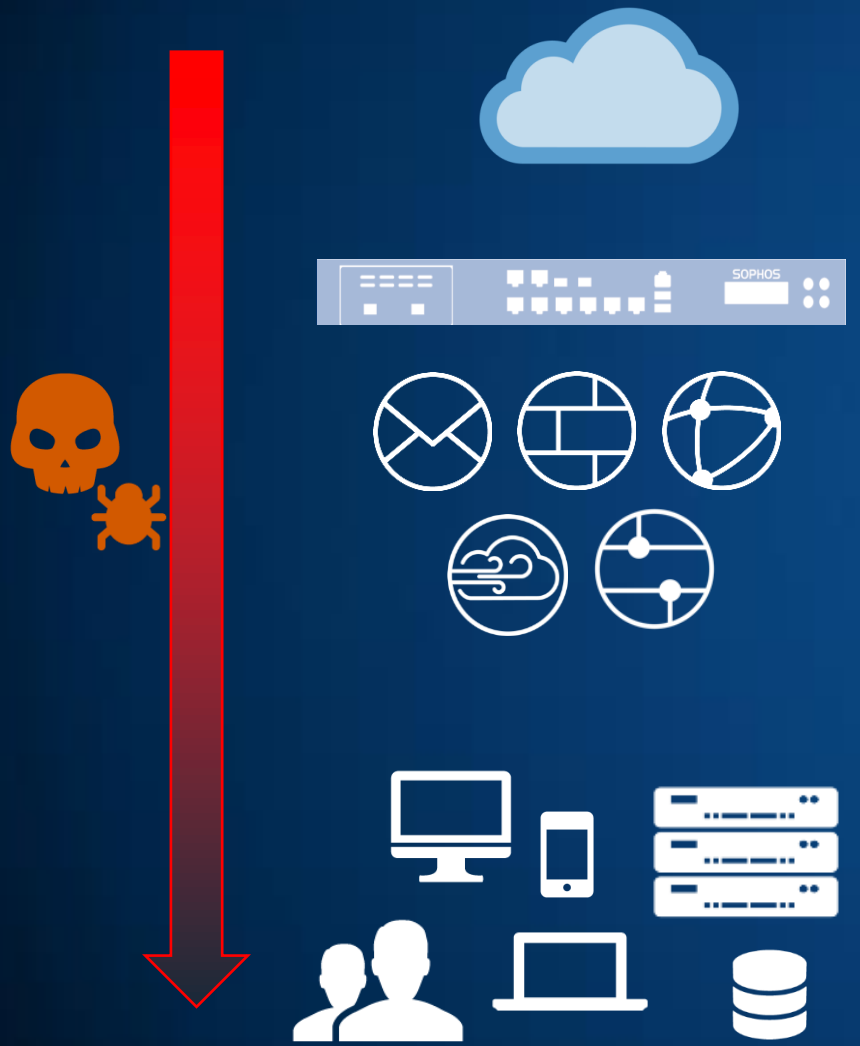
Vertrauliche Daten überall

SOPHOS

Schutz gegen Hackerangriffe über das Netzwerk

XG - NextGen Firewall

Technologien zum Schutz gegen Bedrohungen



Gateway-Technologien

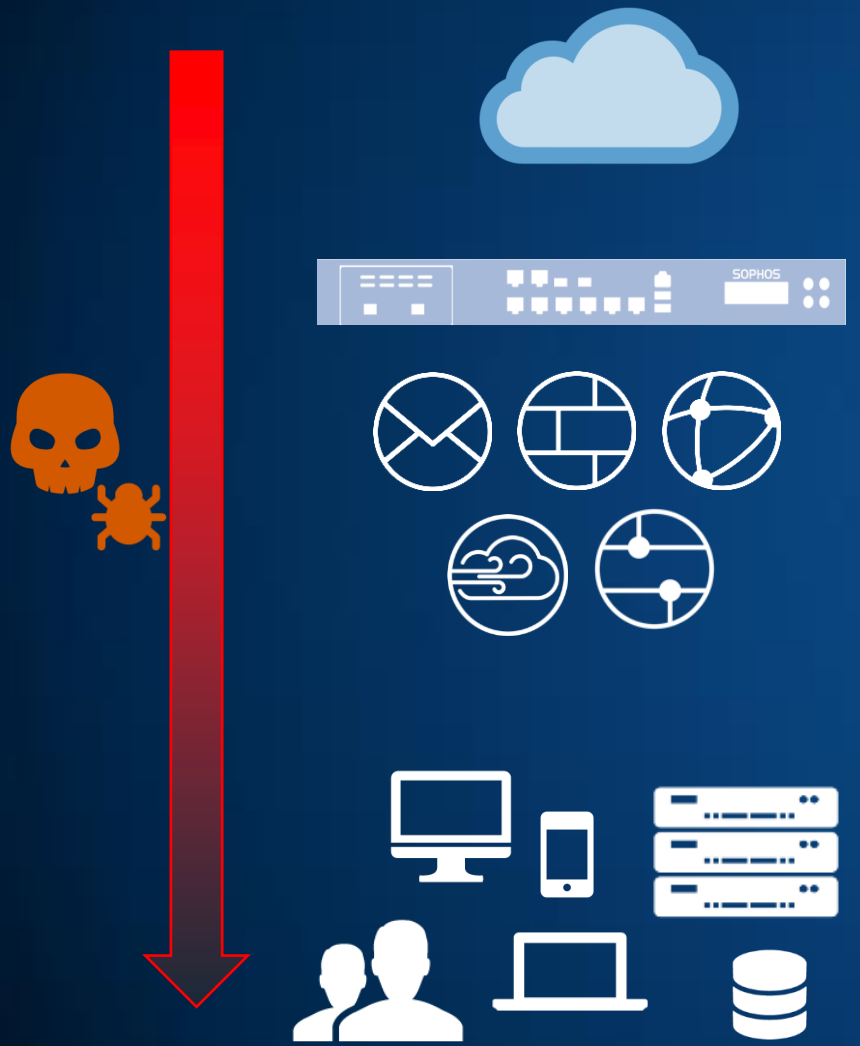
- Firewall / Netzwerksegmentierung
- Botnet-C&C-Erkennung
- Intrusion Prevention
- Web- und Emailfilterung
- Anti-Virus
- Web Application Firewall

Endpoint-Technologien

- Anti-Virus
- Webfilter
- Device Control
- Application Control
- Verschlüsselung
- Whitelisting
- HIPS

SOPHOS

Schutz gegen unbekannte Bedrohungen



Gateway-Technologien

- Firewall / Netzwerksegmentierung
- Botnet-C&C-Erkennung
- Intrusion Prevention
- Web- und Emailfilterung
- Anti-Virus
- Web Application Firewall
- Next-Generation Sandbox

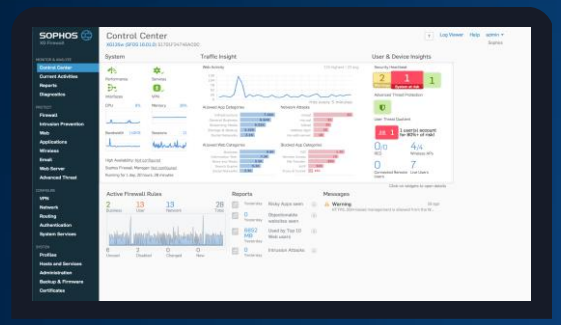
Endpoint-Technologien

- Anti-Virus
- Webfilter
- Device Control
- Application Control
- Verschlüsselung
- Whitelisting
- Machine Learning
- HIPS
- Verhaltenserkennung
- Exploit Prevention

SOPHOS

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

Schutz gegen Ransomware und Malware

XG - NextGen Firewall

NextGen Endpoint & Server Protection / Intercept X

SOPHOS

Endpoint Technologien

Anti-Virus

Vor der Ausführung

Bank

SOPHOS

Endpoint Technologien

Bank

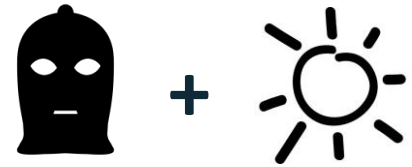
Anti-Virus

Machine Learning

Vor der Ausführung

SOPHOS

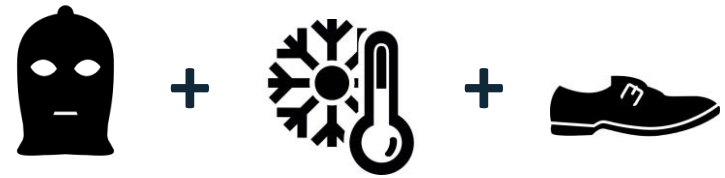
Machine Learning



= verdächtig

= ?

= unverdächtig



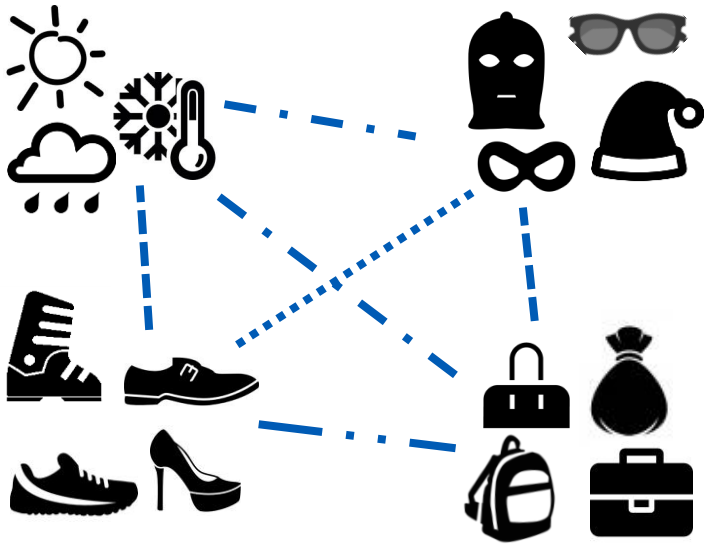
= ?

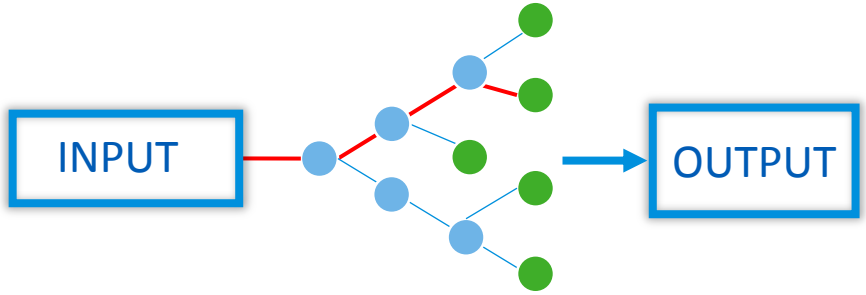
= verdächtig

= unverdächtig

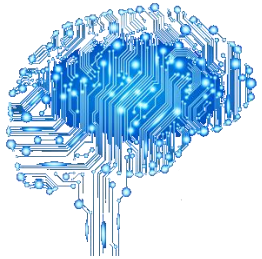
Konventionelles Machine Learning

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

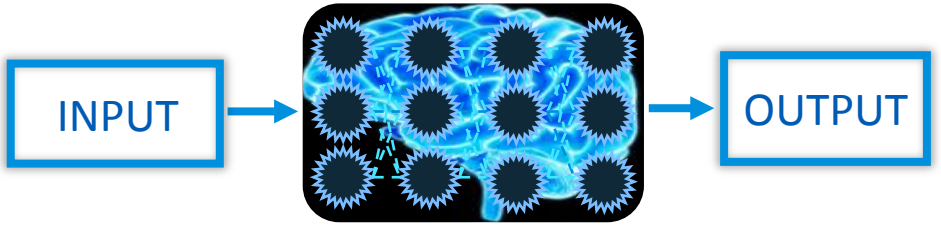




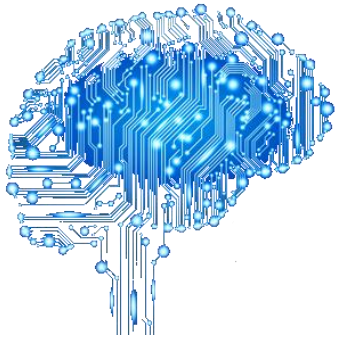
SOPHOS Deep Learning



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



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

Machine Learning

Exploit Prevention

Vor der Ausführung

Während der Ausführung

SOPHOS

Schutz vor unbekannter Malware über Exploit-Prevention

Hersteller-Patches

Exploit Prevention

Exploit Prevention | Hersteller-Patches

Anti-Virus / IPS Signaturen

1,000*n /Jahr

Sicherheits-lücken

25

Exploit-Techniken

?

Zero-Day-Exploits

100*n /Jahr

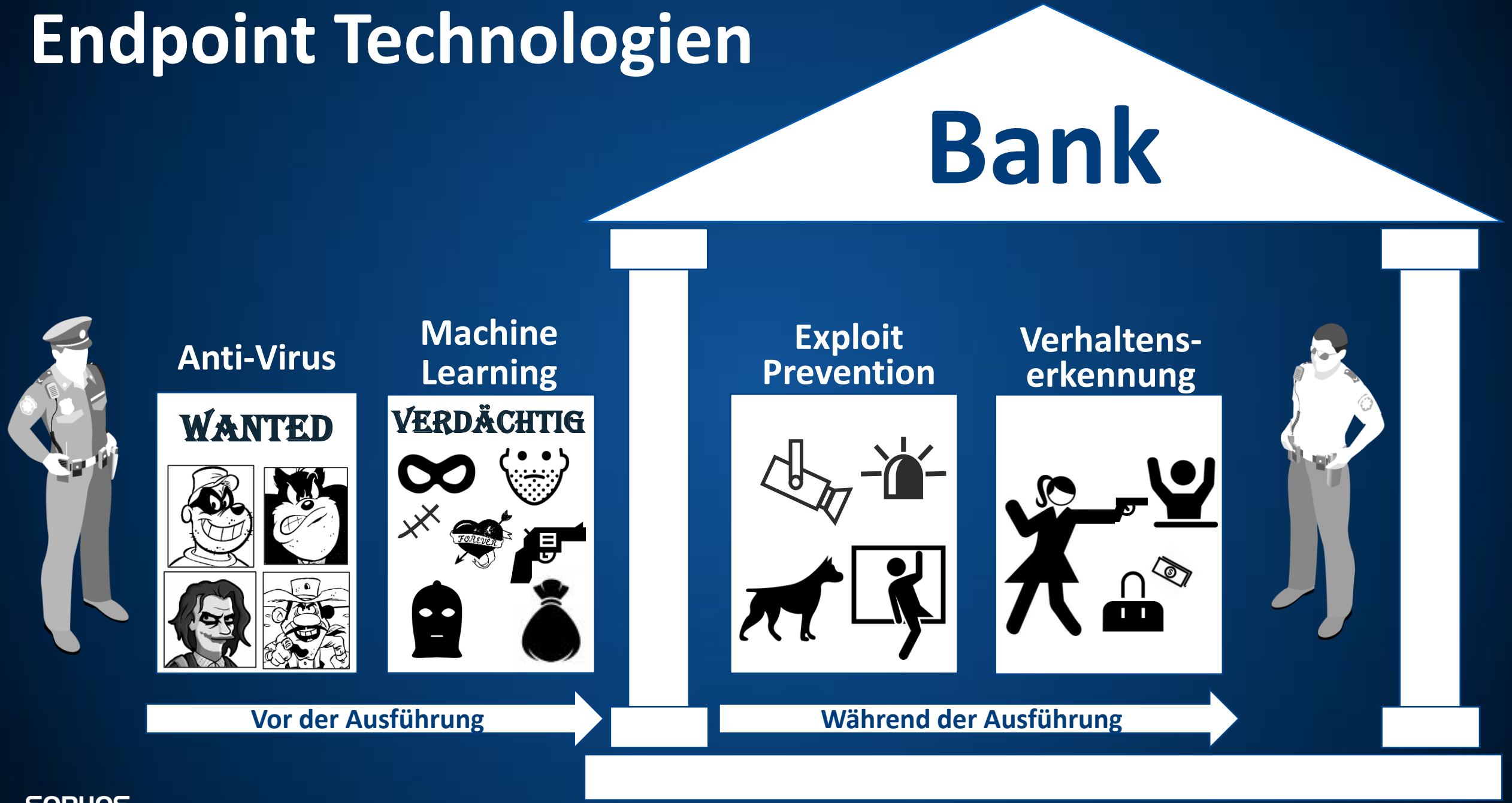
Bekannte Exploits

Malware

100.000.000 /Jahr

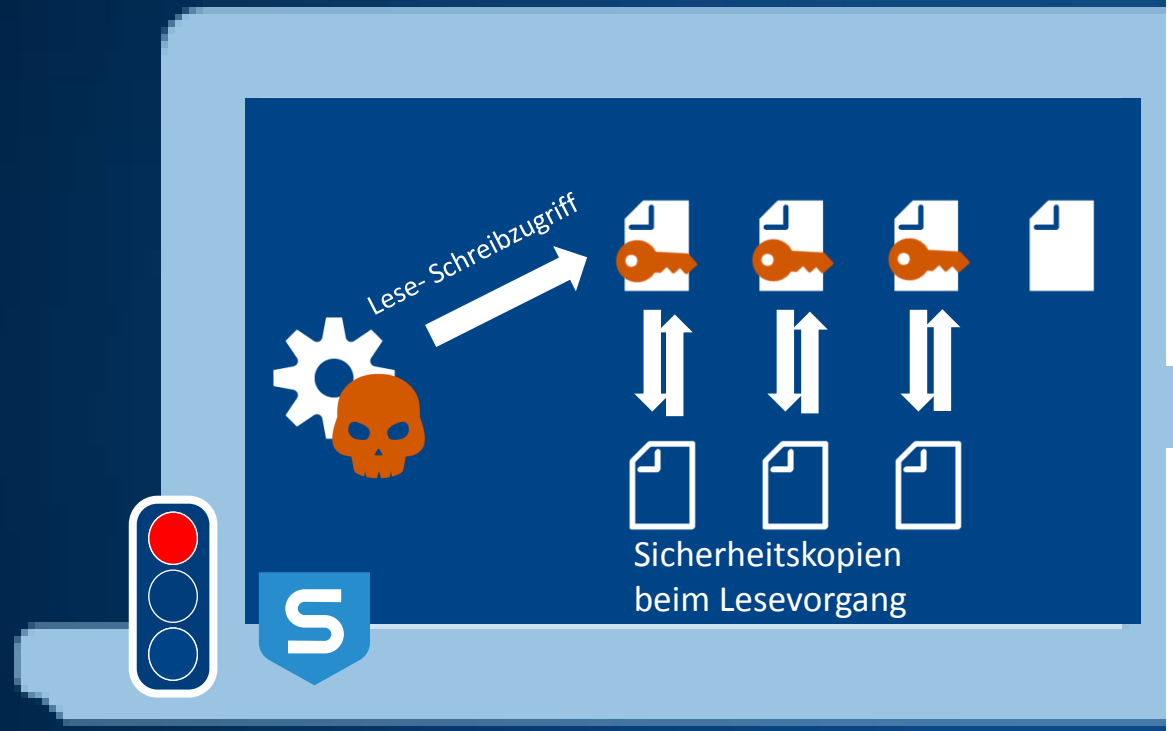
SOPHOS

Endpoint Technologien



SOPHOS

Verhaltenserkennung am Beispiel CryptoGuard



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7B	5C	72	74	66	31	5C	61	6E	73	69	5C	61	6E	73	69	{\rtf1\ansi\ansi
00000010	63	70	67	31	32	35	32	5C	64	65	66	66	30	5C	64	65	cpg1252\deff0\de
00000020	66	6C	61	6E	67	31	30	34	33	7B	5C	66	6F	6E	74	74	flang1043{\fontt
00000030	62	6C	7B	5C	66	30	5C	66	6E	69	6C	5C	66	63	68	61	bl{\f0\fnil\fcha
00000040	72	73	65	74	30	20	56	65	72	64	61	6E	61	3B	7D	7D	rset0 Verdana;}}
00000050	5C	72	5C	6E	5C	76	69	65	77	6B	69	6E	64	34	5C	75	\r\n\viewkind4\u
00000060	63	31	5C	70	61	72	64	5C	73	61	32	30	30	5C	73	6C	c1\pard\sa200\sl
00000070	32	37	36	5C	73	6C	6D	75	6C	74	31	5C	6C	61	6E	67	276\slmult1\lang
00000080	39	5C	66	30	5C	66	73	32	32	20	54	68	65	20	71	75	9\f0\fs22 The qu
00000090	69	63	6B	20	62	72	6F	77	6E	20	66	6F	78	20	6A	75	ick brown fox ju
000000A0	6D	70	73	20	6F	76	65	72	20	74	68	65	20	6C	61	7A	mps over the laz
000000B0	79	20	64	6F	67	2E	7D										y dog.}

Unverschlüsselte Datei vor Schreibvorgang

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7D	EB	10	B2	FD	8E	EB	B9	D1	F6	D8	DE	CC	9B	F6	CB	}ë.²ýŽë¹ÑöØÞÌ›öË
00000010	C4	D9	C3	F6	CB	C4	D9	C3	C9	DA	CD	9B	98	9F	98	F6	ÄÙÃöËÄÙÃÉÚÍ›˜Ÿ˜ö
00000020	CE	CF	CC	CC	9A	F6	CE	CF	CC	C6	CB	C4	CD	9B	9A	9E	ÎÏÌÌšöÎÏÌÆËÄÍ›šž
00000030	99	D1	F6	CC	C5	C4	DE	DE	C8	C6	D1	F6	CC	9A	F6	CC	™ÑöÌÅÄÞÞÈÆÑöÌšöÌ
00000040	C4	C3	C6	F6	CC	C9	C2	CB	D8	D9	CF	DE	9A	8A	FC	CF	ÄÃÆöÌÉÂËØÙÏÞšŠüÏ
00000050	D8	CE	CB	C4	CB	91	D7	D7	F6	D8	F6	C4	F6	DC	C3	CF	ØÎËÄË'××öØöÄöÜÃÏ
00000060	DD	C1	C3	C4	CE	9E	F6	DF	C9	9B	F6	DA	CB	D8	CE	F6	ÝÁÃÄÎžößÉ›öÚËØÎö
00000070	D9	CB	98	9A	9A	F6	D9	C6	98	9D	9C	F6	D9	C6	C7	DF	ÙË˜šš öÙÆ˜.œöÙÆÇß
00000080	C6	DE	9B	F6	C6	CB	C4	CD	93	F6	CC	9A	F6	CC	D9	98	ÆÞ›öÆËÄÍ"öÌšöÌÙ˜
00000090	98	8A	FE	C2	CF	8A	DB	DF	C3	C9	C1	8A	C8	D8	C5	DD	˜ŠþÂÏŠÛßÃÉÁŠÈØÅÝ
000000A0	C4	8A	CC	C5	D2	8A	C0	DF	C7	DA	D9	8A	C5	DC	CF	D8	ÄŠÌÅÒŠÀßÇÚÙŠÅÜÏØ
000000B0	8A	DE	C2	CF	8A	C6	CB	D0	D3	8A	CE	C5	CD	84	D7		ŠÞÂÏŠÆËÐÓŠÎÅÍ„×

Verschlüsselte Datei nach Schreibvorgang

- Ursachenanalyse
- Erweiterte Bereinigung mit Sophos Clean

SOPHOS

INTERCEPT X

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**

SOPHOS

Schutz von Smartphones und Tablets

XG - NextGen Firewall

NextGen Endpoint & Server Protection / Intercept X

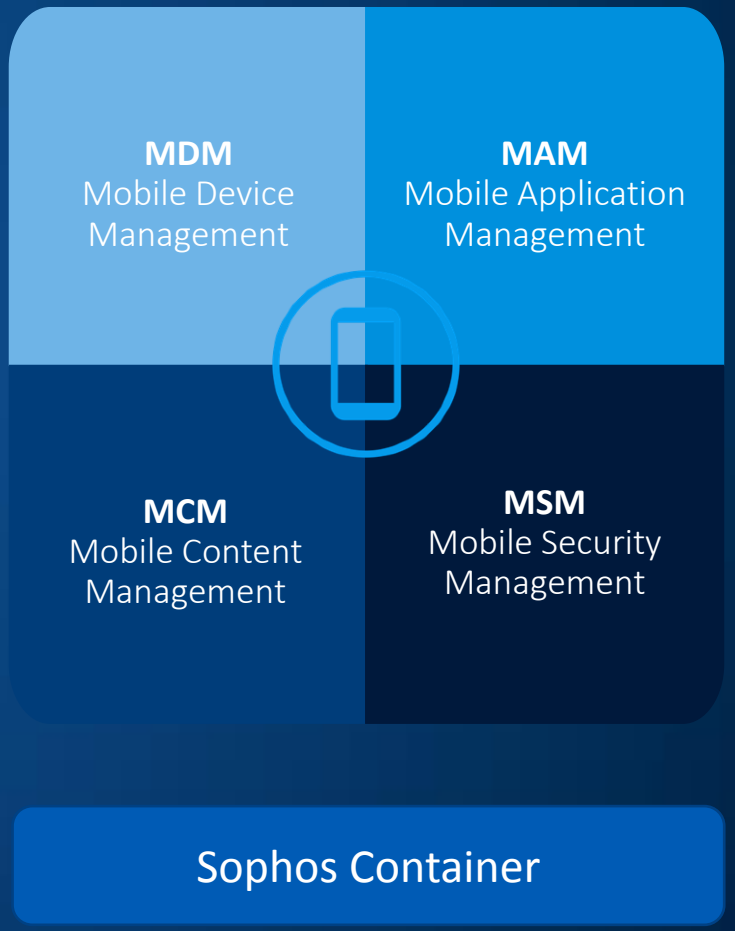
Sophos Mobile

SOPHOS

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



Vertraulichkeit und Schutz vor Datenabfluss per Email

XG - NextGen Firewall

NextGen Endpoint & Server Protection / Intercept X

Sophos Mobile

Email Appliance

SOPHOS

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

Schutz gegen Diebstahl + Verlust von PCs und Macs

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

SOPHOS

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

SOPHOS

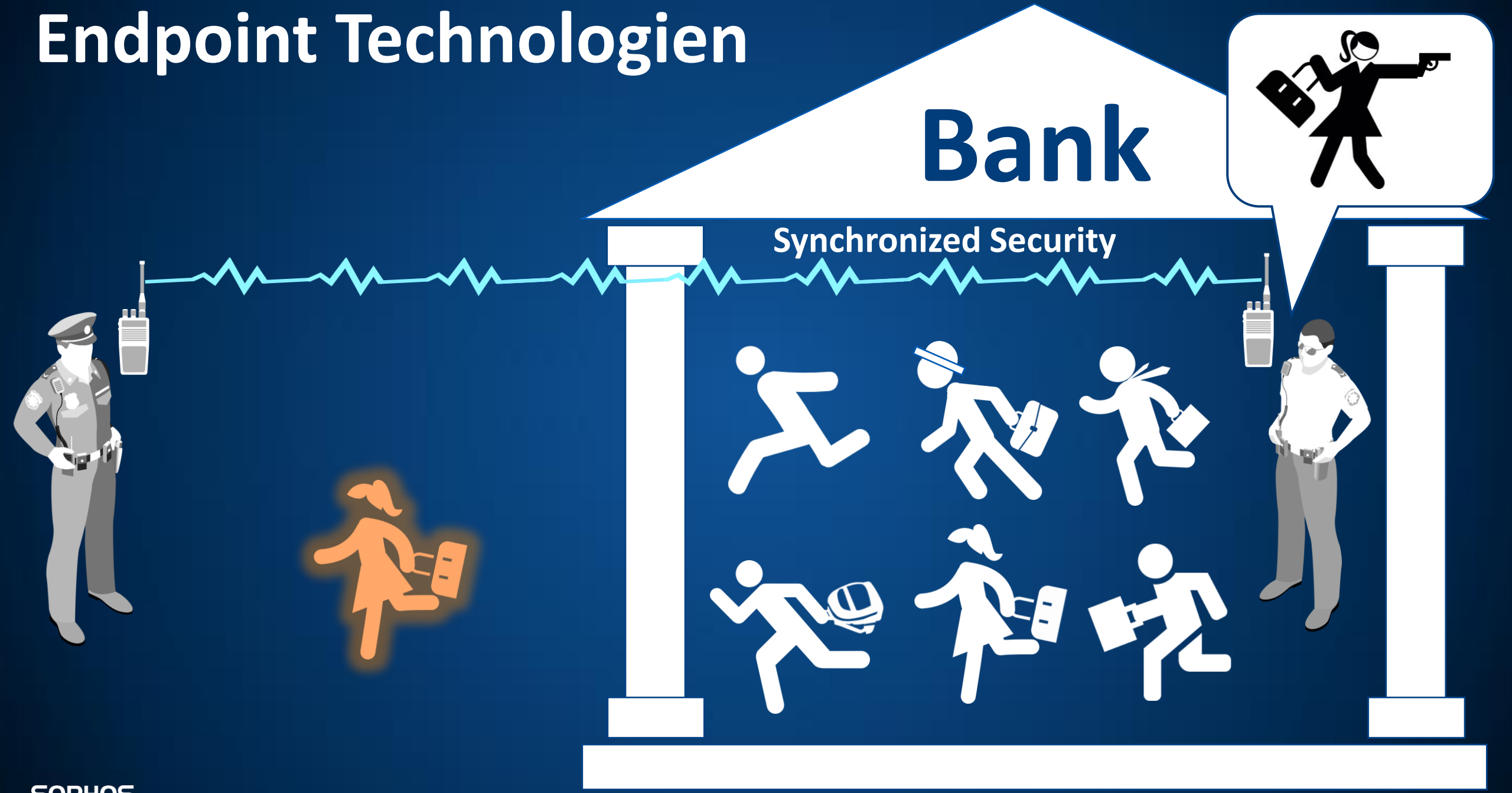
SafeGuard Enterprise – Verschlüsselung überall

Finale Verteidigungslinie
Sicherheit als System

Synchronized Security

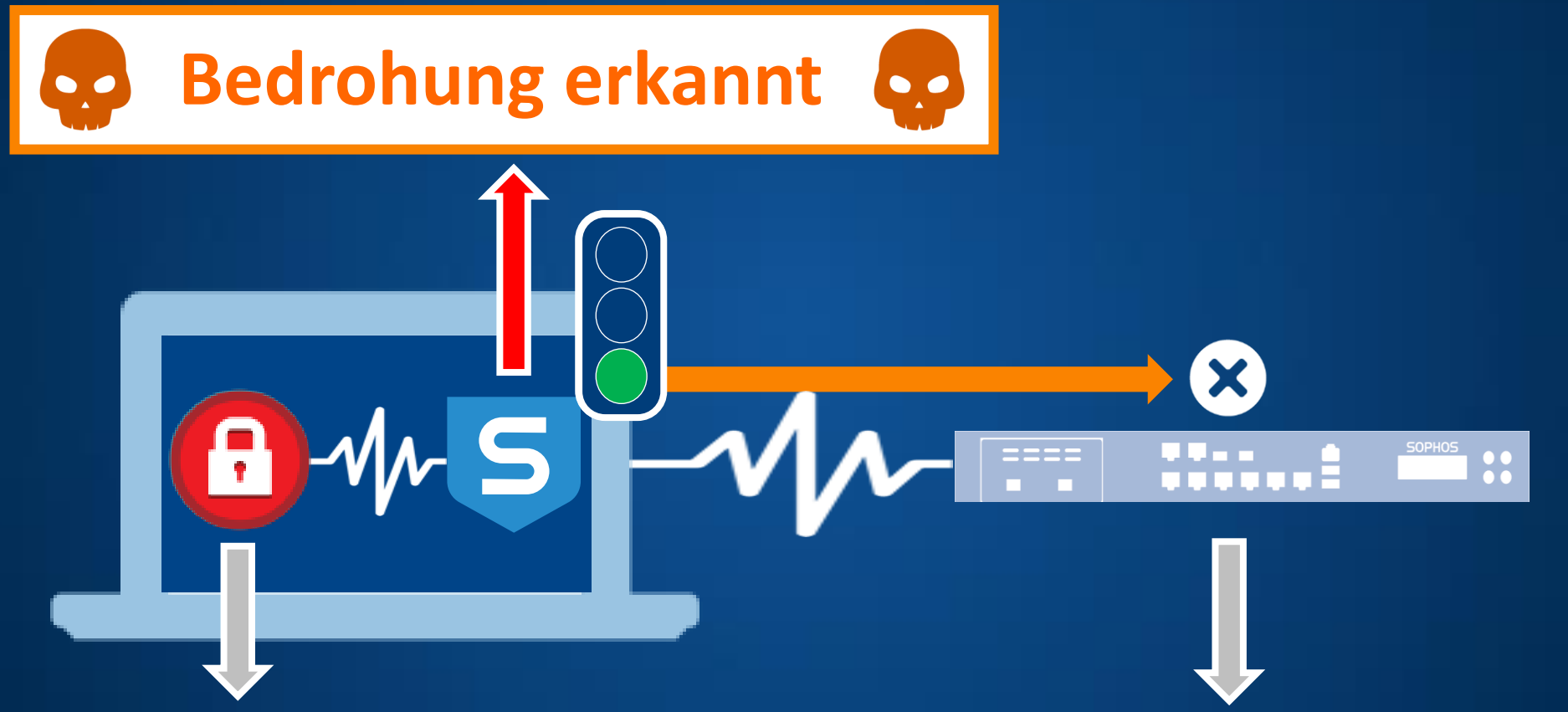
SOPHOS

Endpoint Technologien

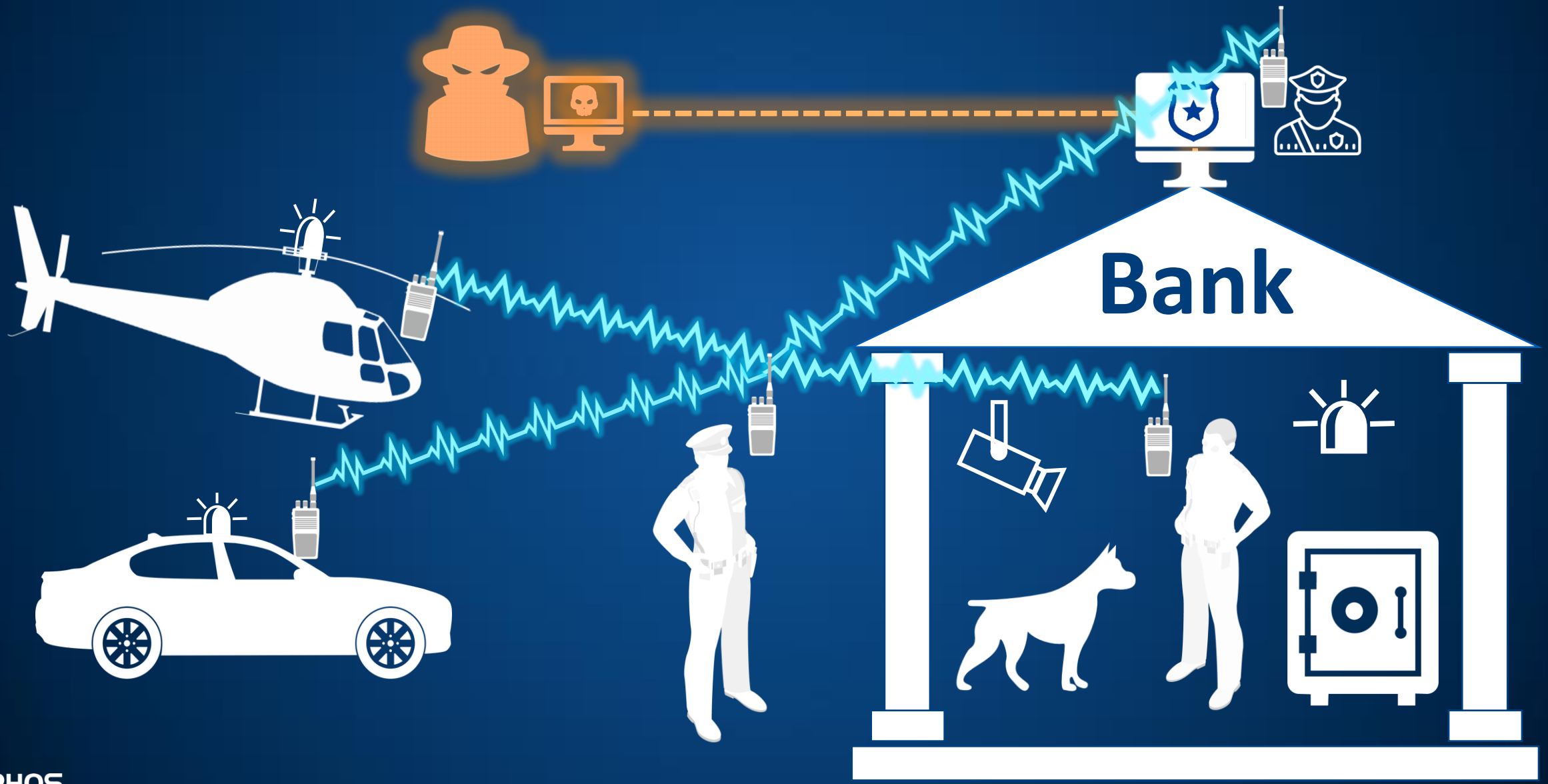


SOPHOS

Security Heartbeat – Zusammenspiel von Endpoint und Gateway



Sicherheit als System ersetzt Einzellösungen



SOPHOS

Synchronized Security – Teamplay statt Best-of-Breed

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

Fragen?

SOPHOS

SOPHOS

Security made simple.