Entdecken Sie neue Wege im Kampf gegen Cyberkriminelle!

Mario Winter
Senior Sales Engineer

SOPHOS

Sophos – mehr als 30 Jahre Erfahrung

1985
GRÜNDUNG
OXFORD, UK

632.1
UMSATZ
(FY17)

3.000
MITARBEITER

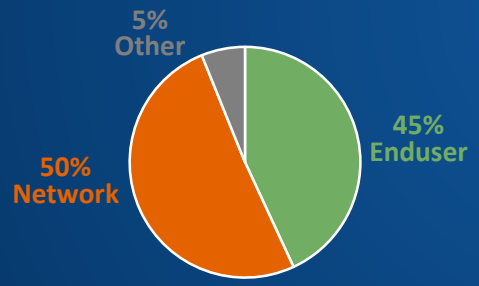
400
in DACH

HQ
ABINGDON, UK

200,000+
KUNDEN

100M+
ANWENDER

20,000+
CHANNEL
PARTNER



- Akquisition u.a. von Utimaco 2009, Astaro 2011, Dialogs 2012, Cyberoam 2014, Mojave 2014, Reflexion 2015, SurfRight 2015, Barricade 2016, Invincea 2017
- Gartner: Marktführer in den Bereichen Endpoint, Verschlüsselung & UTM

Warum sind Krypto-Trojaner so erfolgreich?

SOPHOS

Gründe für Infektionen trotz Best-of-Breed Security

- Office-Dokumente und PDFs in E-Mails oft zugelassen
- Technologisch fortgeschrittene Schädlinge
- Patch-Strategie der Unternehmen
- Hochprofessionelle Angreifer
- Geschicktes Social Engineering
- Sicherheitssysteme fehlen oder sind falsch konfiguriert
- Sicherheitssysteme agieren nicht als System

Neue Sicherheitskonzepte sind notwendig

SOPHOS

Technologien zum Schutz gegen Bedrohungen

Gateway-Technologien

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

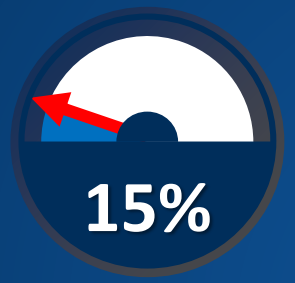
Endpoint-Technologien

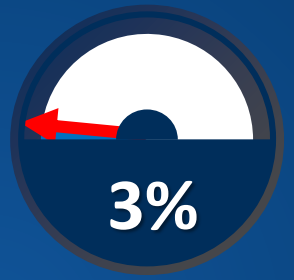
- Anti-Virus
- Webfilter
- Device Control
- Application Control
- Verschlüsselung
- Whitelisting
- Machine Learning
- HIPS
- CryptoGuard
- Exploit Prevention

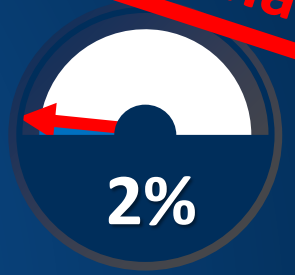
SOPHOS

Wo Malware heute am Endpoint aufgehalten wird

400.000 neue Schädlinge / Tag







Einfallsweg schließen	Analyse vor Ausführung	Exploit-Vehinderung	Verhaltens-Erkennung
• URL-Filterung • Download Reputation • Device Control • App Control	• Signaturen • Heuristiken • Machine Learning	• Einbruchstechniken erkennen/verhindern • Rechteausweitung verhindern	• Verschlüsselung • Hacker-Aktivität • Passwort- und Datendiebstahl

SOPHOS

Sophos INTERCEPT X

Anti-Ransomware

Stoppt Krypto-Trojaner

- Erkennt und verhindert Verschlüsselung
- Stellt Originaldateien wieder her

Anti-Exploit

Stoppt unbekannte Malware

- Signaturloser Schutz vor Zero-Day-Angriffen
- Keine Performanceeinbußen

Erweiterte Bereinigung

Entfernt die Bedrohung

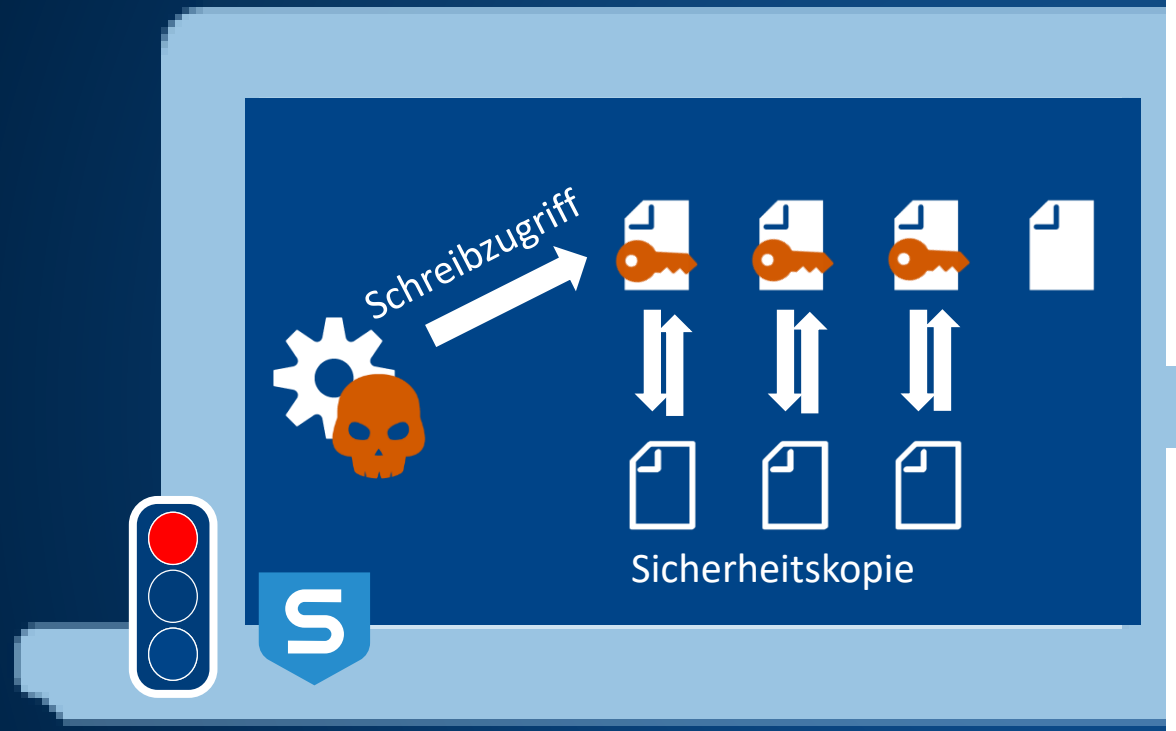
- Signaturlose Erkennung und Entfernung von bisher unbekannter Malware

Ursachenanalyse

Analysiert den Angriff

- Was ist passiert?
- Was ist gefährdet?
- Wie verhindere ich das zukünftig?

CryptoGuard – Schutz vor lokaler Ransomware



Ursachenanalyse

Erweiterte Bereinigung

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.}

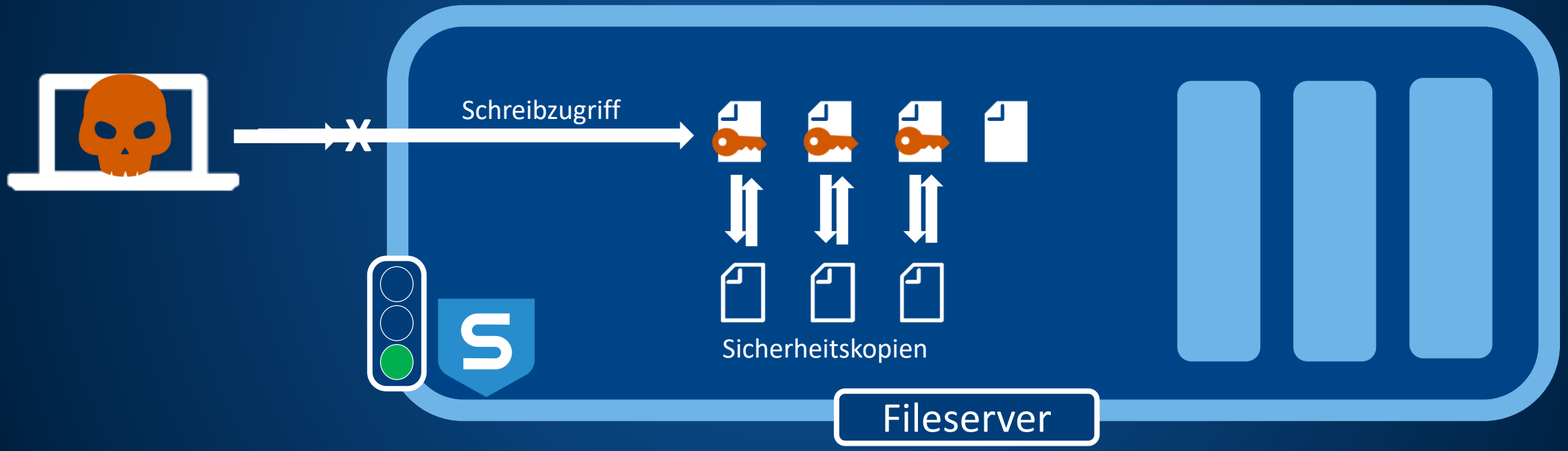
Unverschlüsselte Datei vor Schreibvorgang

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

SOPHOS

CryptoGuard – Schutz vor Clients mit Ransomware



Wo lauert die größere Gefahr?

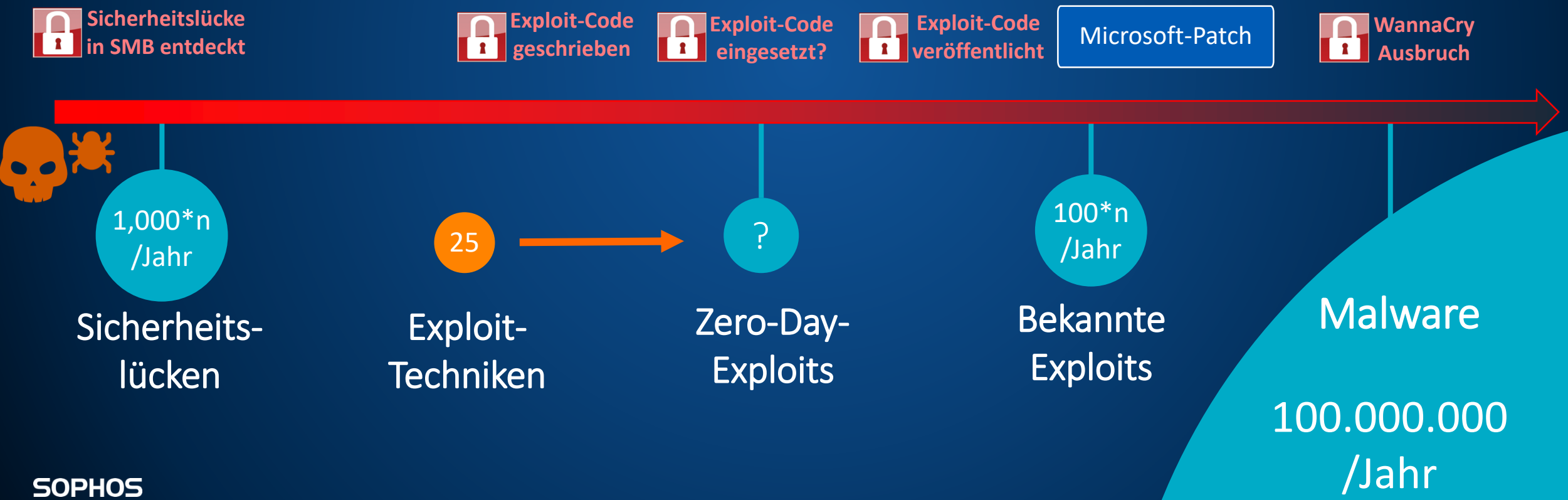
Schutz vor unbekannter Malware über Exploit-Prevention

Hersteller-Patches

Exploit Prevention

Exploit Prevention | Hersteller-Patches

Anti-Virus / IPS Signaturen



SOPHOS

Sophos Clean – der „Tatortreiniger“

- Signaturloser on-demand Malwarescanner
- Forensische Erkennung bisher unbekannter Malware
- Nutzt Verhaltensanalyse und Cloud-Intelligenz (Internet-Verbindung notwendig)
- Entfernt persistente Malware
- Ersetzt infizierte Windows-Resourcen durch sichere Originalversionen

Ursachenanalyse

Was ist passiert?

Analyse des Vorfalls

- Identifikation betroffener Prozesse, Registry-Keys, Dateien, Kommunikation
- Grafische Darstellung der Ereigniskette
- Eintrittspunkte der Malware ins Netzwerk

Was ist gefährdet?

Betroffene Ressourcen

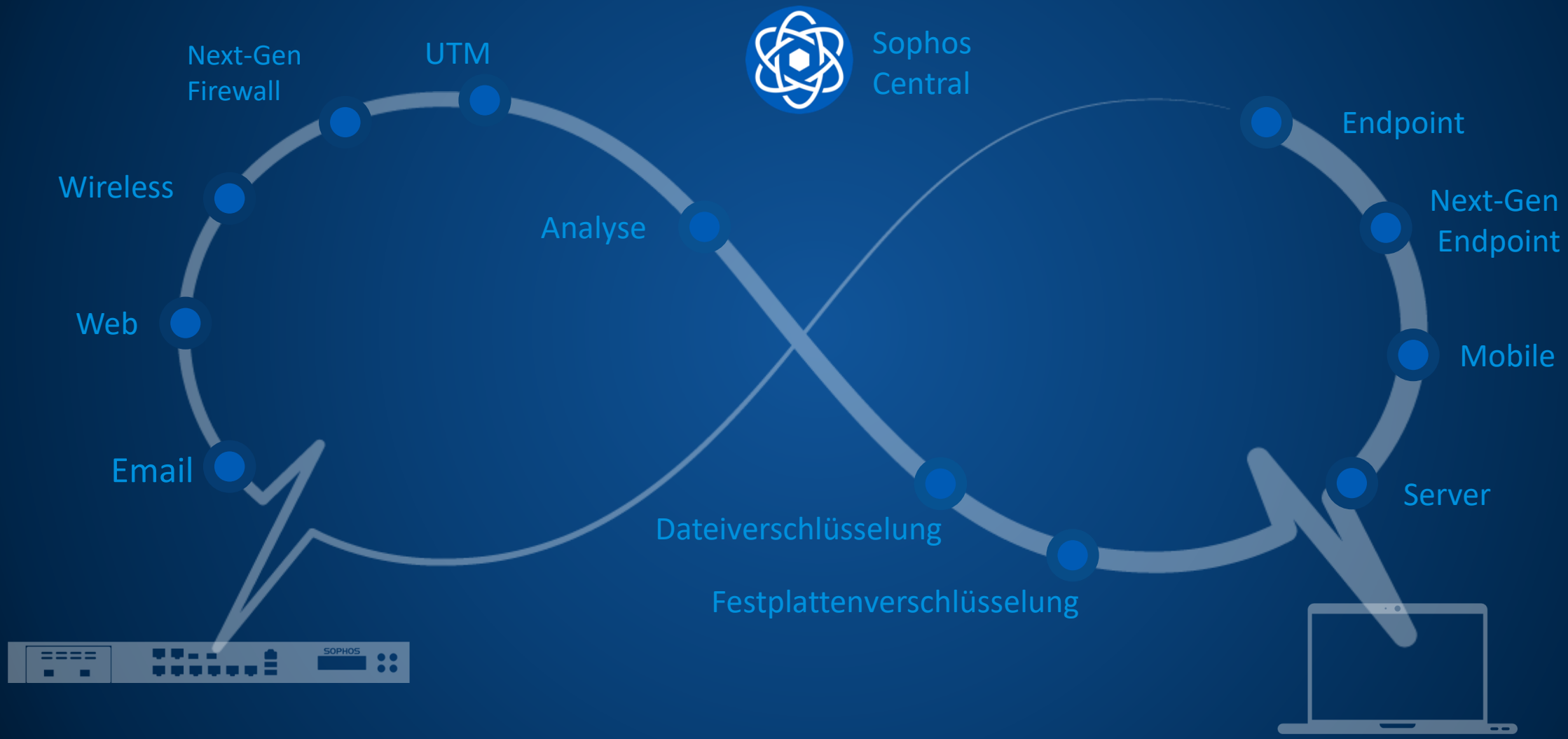
- Welche Dateien und Systeme sind betroffen?
- Auf welche Netzlaufwerke oder Wechselmedien wurde zugegriffen?
- Welche Systeme muss ich noch bereinigen?

Wie verhindere ich das zukünftig?

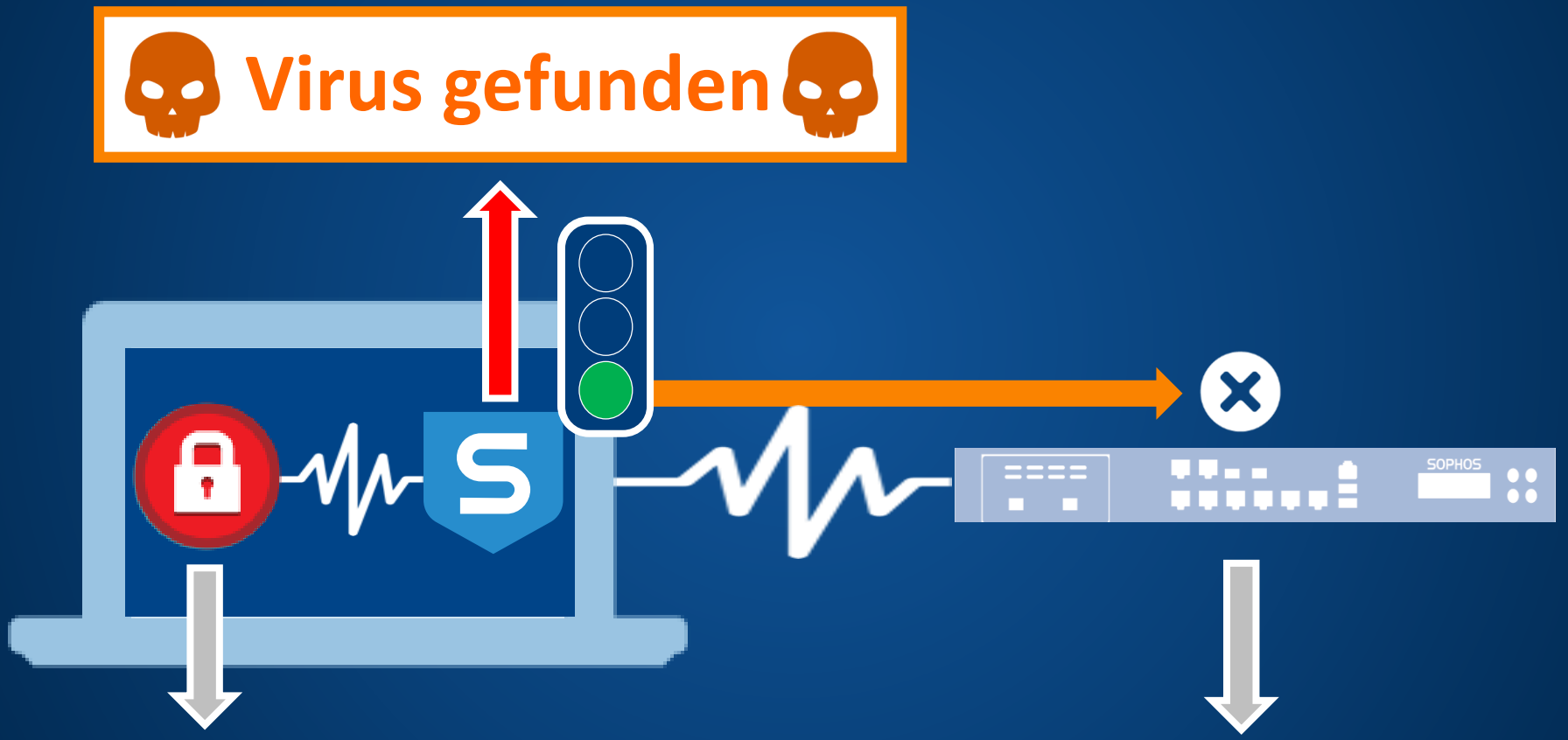
Konsequenzen

- Welche Einfallswege für Malware muss ich schließen?
- Wie kann ich eine Verbreitung im Netzwerk zukünftig verhindern?

Synchronized Security – Teamplay statt Best-of-Breed



Security Heartbeat - Vireninfektion



Demo

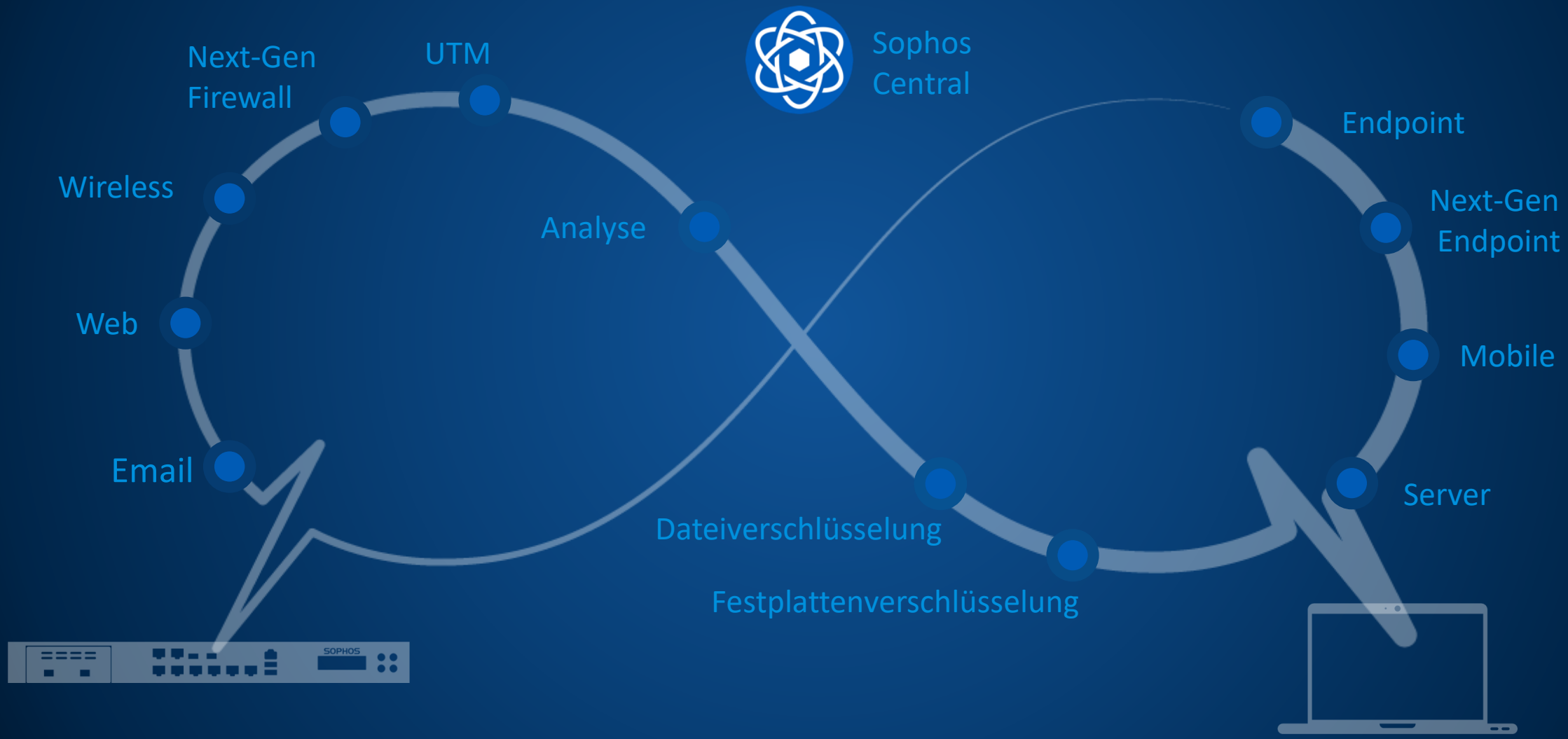
Synchronized Security

Das Video hierzu finden Sie unter: https://www.youtube.com/watch?v=dEyUGn-qtTw

SOPHOS


Papierkorb
Microsoft Word 2010
geheim.docx
Acrobat Reader DC
Microsoft Outlook 2010
Google Chrome
Dokumente
prog
Vertraulich
INTERCEPT
DEU
16:48
20.01.2017

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 hochentwickelter Bedrohungen
- Identifizierung kompromittierter Systeme
- Automatische Reaktion auf Vorfälle
- Analyse der Infektions- und Verbreitungswege
- voraus. kommend: verbesserter Schutz durch Machine Learning
  Security Heartbeat auf Smartphones & Tablets

SOPHOS

Security made simple.