SOPHOS
Security made simple.

Erfolgreiche Umstellung auf Next-Gen Endpoint Security

Von **Marty Ward**, VP Product Marketing, Sophos

Bedrohungen werden immer dynamischer und industrialisierter: Unternehmen müssen heutzutage neben herkömmlicher Malware auch neue Angriffe mit hohem Gefährdungspotenzial abwehren. Um die innovativen Abwehrmechanismen zu erhalten, die hierzu notwendig sind, haben schon viele Unternehmen auf Next-Gen Endpoint Protection von Sophos umgestellt. In diesem Solution Brief zeigen wir, wie Ihnen Sophos Next-Gen Endpoint Protection auf innovative Weise Schutz, Benutzerfreundlichkeit und Support bietet, sodass Sie den immer raffinierter werdenden Bedrohungen auch weiterhin einen Schritt voraus sind.

„Intelligentere, schnellere Hacker sorgen für starken Anstieg von Cyberangriffen."[1]

Schlagzeilen über gravierende Datenpannen sind mittlerweile alltäglich und auch die neuesten Statistiken sprechen eine eindeutige Sprache:
Cyberbedrohungen sind dynamischer als je zuvor. Der Verizon 2015 Data Breach Investigations Report[2] zeichnet ein beunruhigendes Bild der Bedrohungslandschaft. Nicht nur steigt die Zahl der Angriffe stetig an, die Angriffe werden auch zunehmend schneller und raffinierter.

- 2014 nahmen Sicherheitsvorfälle um 26 % zu, bestätigte Datenverluste sogar um 55 %.
- In 60 % aller Fälle gelang es den Angreifern innerhalb von Minuten, ein Unternehmen zu kompromittieren.
- 70 bis 90 % aller Malware-Samples wurden speziell zum Angriff eines bestimmten Unternehmens entwickelt.

Gleichzeitig nehmen das öffentliche Bewusstsein und die Sensibilisierung von Vorstandsetagen für das Thema Cyberbedrohungen immer weiter zu. Ein weiteres Zitat aus dem Verizon-Bericht: „Die New York Times [widmete] dem Thema Datenpannen mehr als 700 Artikel, im Vorjahr waren es weniger als 125." Auch das Bewusstsein für Cyberbedrohungen innerhalb von Unternehmen steigt – sowohl in der breiten Mitarbeiterschaft als auch in der Vorstandsetage.

Wachsende IT-Ausgaben, von denen manche bereut werden

Vor dem Hintergrund des wachsenden öffentlichen Bewusstseins und der zunehmenden Sensibilisierung von Vorstandsetagen ist es kaum verwunderlich, dass Unternehmen ihre IT-Sicherheitsausgaben immer weiter aufstocken. Der Ponemon-Studie „Ponemon 2015 Global Study on IT Security Spending & Investments"3 zufolge gaben 46 % aller Unternehmen in den letzten zwei Jahren mehr für IT-Sicherheit aus und 50 % planen, ihr IT-Sicherheitsbudget in den kommenden zwei Jahren aufzustocken.

Die Ponemon-Studie wirft jedoch auch die Frage auf, wie sinnvoll diese Sicherheitsausgaben im Einzelnen sind: „Unternehmen räumen ein, dass sie mit einigen der von ihnen erworbenen Technologien unzufrieden sind. Die Befragten gaben an, dass in den letzten zwei Jahren durchschnittlich 37 % der von ihnen getätigten Investitionen in IT-Sicherheitstechnologien ihren Erwartungen nicht gerecht wurden."

Auf die Frage hin, warum sie diese Investitionen in IT-Sicherheit bereuen, fielen die in der Ponemon-Studie von Unternehmen am häufigsten genannten fünf Probleme in die drei folgenden Kategorien:

1. Schutz (Systemeffektivität)
2. Benutzerfreundlichkeit (Systemkomplexität, Personal und fehlendes internes Fachwissen, Installationskosten
3. Support (Anbieter-Support)

Wenn wir neue Sophos-Endpoint-Protection-Kunden fragen, was der Grund für den Wechsel von ihrer bisherigen Endpoint-Security-Lösung zu Sophos war, ähneln viele Antworten den in der Ponemon-Studie geschilderten Problemen. Insbesondere herrscht Unzufriedenheit mit anhaltenden Malware-Ausbrüchen trotz bestehender Sicherheitssoftware, mangelnder Performance, mehreren Agenten, Produktkomplexität, schlechtem Kunden-Support und Schwierigkeiten bei der Eingliederung verschiedenster integrierter Abwehrmechanismen.

Unaufhaltsame Weiterentwicklung von Bedrohungen

Die oben genannten Probleme sind darauf zurückzuführen, dass Kunden trotz unaufhaltsamer Weiterentwicklung von Bedrohungen immer noch versuchen, sich mit technisch längst überholten Endpoint-Lösungen zu schützen. Herkömmliche Endpoint-Security-Software ist darauf ausgelegt, Viren, Trojaner und Würmer abzufangen. Mittlerweile sind jedoch Ransomware, speicherbasierte Angriffe und Bedrohungen im Umlauf, die gezielt Schwachstellen ausnutzen. Sowohl die Bedrohungen selbst als auch ihre Ziele haben sich in den letzten Jahren stark verändert.

In Abbildung 1 haben wir einige der wichtigsten Bedrohungstrends aufgeführt. Hieraus geht hervor, dass es sich bei der Mehrheit aller Bedrohungen mittlerweile um unbekannte Zero-Day-Angriffe handelt. Wir konnten auch einen Trend von einfacher Malware hin zu industrialisierten Angriffen beobachten, die sehr koordiniert ablaufen und oft auf verschiedensten Angriffsmethoden und Kommunikationsmechanismen basieren. Da traditionelle Endpoint-Security-Software herkömmliche Malware mittlerweile gut abwehren kann, haben Hacker ihren Fokus stattdessen darauf verlagert, Zugangsdaten zu kompromittieren, um sich unter dem Deckmantel eines legitimen Benutzers oder Administrators innerhalb von Systemen ungehindert bewegen zu können. Auf solche neuartigen Gefahren ist traditionelle Endpoint-Security-Software nicht ausgelegt.

Abbildung 1: Entwicklung von Bedrohungstrends

Bedrohungen	Ziele
Bekannt und unbekannt 75 % der Malware innerhalb eines Unternehmens ist speziell auf das Unternehmen zugeschnitten. (Quelle: SophosLabs)	**Große und kleine Unternehmen** 70 % aller Unternehmen meldeten in den letzten 12 Monaten eine Kompromittierung. (Quelle: SophosLabs)
Einfach und industrialisiert Da „Malware-as-a-Service"-Plattformen sich zunehmender Beliebtheit erfreuen, werden Payloads im Dark Web unter den gleichen Marktzwängen angeboten, die auch in jeder anderen Branche herrschen. (Quelle: FBI/InfoSec London)	**Flächendeckend und gezielt** Exploit-Kits sind für mehr als 90 % aller Datenpannen verantwortlich. (Quelle: NSS Labs)
Malware und Hacking 63 % aller Datenpannen resultieren aus gestohlenen Zugangsdaten. (Quelle: Verizon DBIR)	**Beliebig und schwachstellenfokussiert** Die durchschnittliche Dauer zur Behebung von Schwachstellen beträgt 193 Tage. (Quelle: WhiteHat Security)

Auch die Ziele der Angriffe haben sich verändert. Anstatt nur Großunternehmen ins Visier zu nehmen, haben Hacker erkannt, dass kleine und mittelständische Unternehmen über genauso wertvolle Daten verfügen und oft mit Großunternehmen zusammenarbeiten. Zwischen Unternehmen werden also beträchtliche Datenmengen ausgetauscht und Cyberkriminelle können diesen Übertragungsweg relativ leicht „anzapfen" um an die gewünschten Daten zu gelangen.

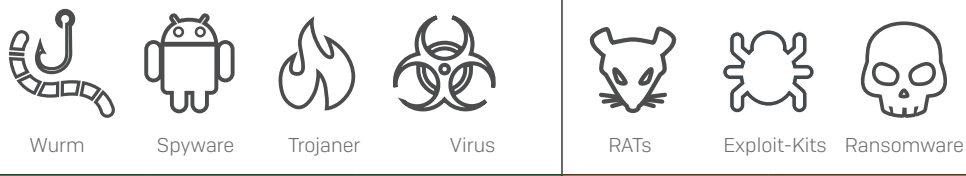
Exploit-Kits sind nichts anderes als „Hacking as a service"-Tools, die von jedem genutzt werden können, und mittlerweile für 90 % aller Datenpannen verantwortlich. Mit Exploit-Kits lassen sich Angriffe sehr gezielt steuern und Hacker können die von ihnen gewünschten Demografien genau festlegen, um die Effektivität ihrer Handlungen zu maximieren. Da es in vielen Unternehmen immer noch ein halbes Jahr dauert, bis bekannte Schwachstellen gepatcht werden, verabschieden sich viele Hacker von ungezielten Großangriffen und nutzen stattdessen die mangelnde Patch-Bereitschaft aus.

Die Weiterentwicklung von Endpoint Security

Genau wie die Hackerfraktion entwickelt sich aber auch die Sicherheitsbranche stetig weiter und bringt immer neue Innovationen hervor. In dieser bereits seit Jahrzehnten andauernden „Schachpartie" zwischen Hackern und Sicherheitsanbietern folgt auf jeden Angriff ein Gegenangriff und jede Seite versucht, der anderen zuvorzukommen. Die Sicherheitsbranche war schon immer von der Vorstellung eines Allheilmittels fasziniert. Nicht umsonst gibt es mittlerweile über 1000 Sicherheitstechnologie-Anbieter weltweit, von denen viele auf nur eine einzige Technologie setzen, die ihrer Meinung nach die Lösung für alle Probleme ist. Tatsächlich ist dieses „Allheilmittel" jedoch nicht mehr als eine Wunschvorstellung.

Genau wie bei einer Schachpartie verschiedene Figuren und Schachzüge eine Rolle spielen, sind auch mehrere Technologien erforderlich, um Ihre Endpoints umfassend zu schützen. Die herkömmlichen, in Abbildung 2 aufgeführten Sicherheitsmodelle wie Exposure Prevention, Analysen vor Ausführung und Dateiscans sind zur Abwehr traditioneller Malware nach wie vor wichtig. Chet Wisniewski, Principal Research Scientist bei Sophos, sagt gerne: „Wenn man den Heuhaufen abbrennt, findet man die Nadel viel leichter."

Abbildung 2: Die Weiterentwicklung von Endpoint Security
Von Anti-Malware zu Anti-Exploit



Herkömmliche Sicherheit			Hochentwickelte Sicherheit	
Exposure Prevention	**Analysen vor Ausführung**	**Dateiscans**	**Laufzeit**	**Exploit-Erkennung**
URL-Blockierung Web/App/Dev Ctrl Download Rep	Generische Abgleiche Heuristiken Kernregeln	Bekannte Malware Malware-Bestandteile	Verhaltensanalysen Laufzeitverhalten	Technik-Identifizierung

Diese „Nadel" tritt sehr wahrscheinlich in Form eines komplexen speicherbasierten Angriffs oder Exploits in Erscheinung. Aus diesem Grund sollte Ihre Endpoint-Lösung über eine Laufzeit-Erkennung und -Abwehr sowie eine Exploit-Erkennung verfügen. Diese leistungsstarken (und signaturlosen) Abwehrtechnologien suchen nach Exploit-Techniken und -Verhaltensweisen, um unbekannte Angriffe zu stoppen.

Wir sind nach wie vor davon überzeugt, dass umfangreiche Abwehrmaßnahmen Teil einer erfolgreichen Schutzstrategie sein sollten. Den wirklichen Durchbruch (also eine Lösung, die dem „Allheilmittel" am nächsten kommt), kann jedoch nur eine Integration dieser Technologien zu einem koordinierten Sicherheitssystem bringen, das noch ausgeklügelter ist als die komplexen Angriffe selbst.

Sophos bietet zukunftsweisende Endpoint Protection

Um einen Vorsprung im Kampf gegen moderne Bedrohungen zu gewinnen, müssen Sie in leistungsstarke IT-Sicherheitslösungen investieren, die mit Ihrem bestehenden Personal und Know-how effizient betrieben werden können. Sophos Next-Gen Endpoint Protection vereint nicht nur eine Vielzahl hochentwickelter Sicherheitstechnologien. Die Lösung ist auch intelligent konzipiert und wird von einem erstklassigen Support-Team unterstützt, das dafür sorgt, dass Sie alle Sicherheitstechnologien erfolgreich in Ihrem Unternehmen implementieren können.

Innovativer Schutz

Sophos kombiniert neueste Advanced Threat Protection mit bewährten Anti-Malware-Technologien:

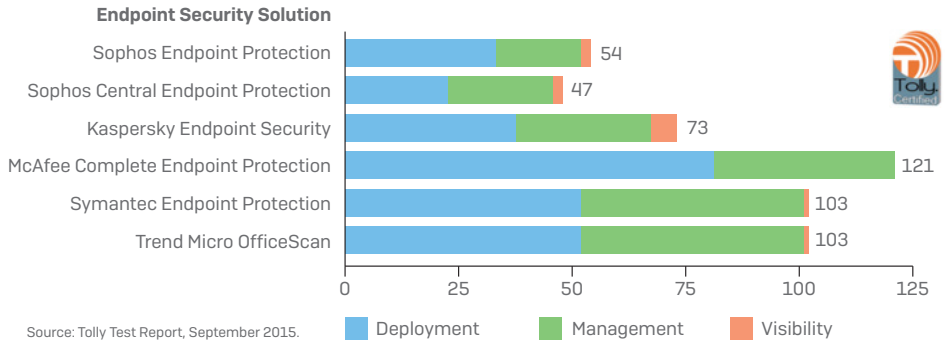
ABWEHR		ERKENNUNG	REAKTION
Vor Erreichen des Geräts	**Vor Ausführung auf dem Gerät**	**Stoppen von Bedrohungen bei Ausführung**	**Analyse und Beseitigung**
Web Security Blockiert Schadskripts und Umleitungen, die zur Übermittlung von Bedrohungen eingesetzt werden. **Download Reputation** Warnt Benutzer unter Verwendung verschiedener Variablen vor Dateien, die zwar nicht erwiesenermaßen schädlich, aber ggf. nicht vertrauenswürdig sind. **Web Control** Web-Filterung auf Basis von Kategorien; wird sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks durchgesetzt. **Device Control (z. B. USB)** Steuert den Zugriff auf Wechselmedien und mobile Geräte und beugt mit vorkonfigurierten oder individuellen Regeln Datenverlusten vor. **Application Control** Point-and-Click-Blockierung von Anwendungen basierend auf Kategorie oder Name. **Browser Exploit Prevention** Erkennt und blockiert Versuche, Schwachstellen auszunutzen, mit denen der Web-Browser kompromittiert werden könnte.	**Anti-Malware-Dateiscans** Wird aktiv auf einem Endpoint ausgeführt, um bekannte Malware und verdächtige Dateien zu identifizieren und anschließend deren Ausführung zu verhindern. **Live Protection** Kommuniziert in Echtzeit mit den SophosLabs, um Signaturen verdächtiger Dateien zu überprüfen, URL- und Download-Reputationsdaten abzufragen und hochverdächtige Dateien zur weiteren Sandbox-Analyse an die Labs zu übermitteln. **Verhaltensanalysen vor Ausführung/HIPS** Blockiert die Ausführung von potenziell schädlichem Computercode mittels Sophos Behavioral Genotype Protection. **Blockierung potenziell unerwünschter Anwendungen (PUAs)** Blockiert Programme, die nicht unbedingt schädlich sind, jedoch im Allgemeinen als ungeeignet für Unternehmensnetzwerke eingestuft werden. **Exploit Prevention** Erkennt und blockiert Versuche, Sicherheitslücken in Anwendungen oder Betriebssystemen auszunutzen.	**Laufzeit-Verhaltensanalyse/HIPS** Analysiert das Verhalten von Programmen, die auf dem System ausgeführt werden, dynamisch, um potenziell schädliche Aktivitäten zu erkennen und zu blockieren. **Malicious Traffic Detection (MTD)** Erkennt und informiert Sie in Echtzeit, wenn Malware versucht, mit „Command and Control"-Servern zu kommunizieren. **CryptoGuard Ransomware Protection** Erkennt schädliche Spontanverschlüsselungen von Dateien, stoppt Angriffe und setzt betroffene Dateien in ihren sicheren Zustand zurück.	**Automatisierte Malware-Entfernung** Entfernt Malware ohne Interaktion des Administrators von Endpoints und gibt dann eine Alarmmeldung aus, wenn ein manuelles Eingreifen erforderlich ist. **Synchronized Security** Endpoints und Firewall kommunizieren über einen erweiterten Security Heartbeat™, um die Erkennung von Bedrohungen zu beschleunigen und die Reaktion auf Vorfälle zu automatisieren. **Ursachenanalyse** Verfolgt den gesamten Entwicklungsprozess eines Angriffs, von der Anwendung, die für die Zustellung des Angriffs verwendet wurde, bis hin zum Punkt, an dem der Angriff aufgedeckt wurde. Gibt auch Bereinigungs- und Best-Practice-Tipps. **Sophos Clean** Gründliche forensische Maßnahmen zur Bereinigung komplexer Bedrohungen beseitigen Malware sowie alle Überreste und Registry-Schlüssel rückstandslos.

Einfache Bedienung

Um eine erfolgreiche Implementierung und Nutzung dieser Abwehrmaßnahmen in Ihrem Unternehmen zu ermöglichen, sind die Maßnahmen auf eine einfache Konfiguration, Bereitstellung und Verwaltung ausgelegt. Sinnvolle Standardrichtlinien und „Point-and-Click"-Funktionalität erleichtern die Bereitstellung. Dazu erhalten Sie mit dem intuitiven, benutzerfreundlichen Dashboard eine klare Übersicht über Ihre Umgebung und schnellen Zugriff auf Routine-Verwaltungsaufgaben.

Unabhängige Usability-Tests von Tolly[4] bestätigen, dass Sophos weit benutzerfreundlicher ist als andere Endpoint-Security-Lösungen (Abbildung 3).

Abbildung 3: Anzahl der zur Bereitstellung, Verwaltung und Visibility erforderlichen Schritte (je kleiner der Wert, desto besser).



Sophos Central Endpoint Protection hieß früher Sophos Cloud Endpoint Protection.

Unterstützung von Experten

Egal, wie benutzerfreundlich Ihre Lösung ist: Es wird Situationen geben, in denen Sie Hilfe von außen in Anspruch nehmen müssen. Bei Sophos steht Ihnen ein ausschließlich mit internen Mitarbeitern besetztes, weltweit präsentes Expertenteam 24 Stunden am Tag an 7 Tagen in der Woche beratend zur Seite. Für das Sophos-Supportteam hat Kundenzufriedenheit höchste Priorität. Sie können sich daher darauf verlassen, dass wir Sie optimal unterstützen, wenn Sie bei der Nutzung neuer Sicherheitsfunktionen in Sophos Endpoint Protection Hilfe benötigen.

„Früher wurden Schädlinge oftmals nur zufällig entdeckt, wenn die Fernwartung mal aktiviert war. Heute haben wir mit Sophos Endpoint Protection alles in Echtzeit im Blick und können entsprechend schnell sowie ohne großen Personalaufwand reagieren."

DR. PAUL LANDWICH
Leiter IT-Abteilung Evangelische Kirche der Pfalz

„Die Security-Komponenten konnten enorm schnell installiert werden und geben uns einen Rundum-Sorglos-Schutz, den wir zuvor nicht kannten und mit unseren Ressourcen und anderen Lösungen nicht erreicht hätten."

KARL-HEINZ SCHULZ
IT-Leiter bei Grasdorf

Umstellung auf Sophos Next-Gen Endpoint – ein fünfstufiger Prozess

Für die meisten Unternehmen sind die größte Hürde beim Wechsel auf Next-Gen Endpoint Security die befürchteten Umstellungsschwierigkeiten. Wir bei Sophos haben über die Jahre hinweg mit Tausenden von Kunden zusammengearbeitet und den Migrationsvorgang immer weiter verbessert. Meist kann die Migration innerhalb weniger Tage oder sogar Stunden erfolgreich abgeschlossen werden.

1. Management-Konsole auswählen und installieren
Die Verwaltung kann bei Sophos wahlweise in der Cloud oder lokal erfolgen.

- **Sophos Central** bietet den schnellsten Weg zur Implementierung einer voll funktionsfähigen Management-Konsole. Nach Aktivierung eines Sophos-Central-Accounts kann die Software in weniger als fünf Minuten eingerichtet und bereitgestellt werden.
- Kunden, die eine herkömmliche, lokale Management-Konsole bevorzugen, können die **Sophos Enterprise Console** sowie zugehörige Verwaltungskomponenten installieren und konfigurieren.

2. Endpoint-Bereitstellungspaket vorbereiten
Im Sophos-Bereitstellungspaket ist ein Removal Tool für Fremdsoftware enthalten, das speziell konfiguriert werden kann, um die bisherige Endpoint-Software vollständig zu entfernen. Nach Entfernung der alten Endpoint-Security-Software schließt das Sophos Endpoint Protection Installationspaket die Bereitstellung der Sophos Endpoint Protection Software ab. Der Prozess beinhaltet Optionen zur interaktiven oder unbeaufsichtigten Installation. Mit letzterer Option wird der Bereitstellungsvorgang transparent, um die Endbenutzer so wenig wie möglich zu beeinträchtigen.

3. Sophos-Endpoint-Protection-Richtlinien konfigurieren
Sophos Endpoint Protection verfügt über einige Endpoint-Security-Funktionen, die in Ihrer bisherigen Software eventuell nicht enthalten waren. Beginnen Sie damit, Endpoint-Protection-Richtlinien für die Sicherheitsfunktionen zu konfigurieren, die in Ihrer vorherigen Lösung aktiviert waren, z. B. Antivirus.

Neue Sicherheitsfunktionen in Sophos Endpoint Protection (z. B. Malicious Traffic Detection, Application Control und Web Control) können Sie wahlweise gleich bei der Bereitstellung aktivieren oder nach und nach hinzufügen.

4. Rollout starten
Wie bei jedem Rollout von Endpoint-Software sollte auch bei Sophos Endpoint Protection die neue Software zunächst auf einer begrenzten Zahl von Endpoints installiert werden, um den Bereitstellungsprozess zu testen und sicherzustellen, dass die neue Endpoint-Security-Software problemlos ausgeführt wird. Wählen Sie Test-Endpoints aus, die leicht zugänglich sind und aktiv genutzt werden, damit Sie die Bereitstellung schnell testen und die problemlose Ausführung überprüfen können.

5. Rollout im gesamten Unternehmen abschließen
Nach dem anfänglichen Test-Rollout können Sie Sophos Endpoint Protection im gesamten Unternehmen bereitstellen. In größeren Unternehmen kann dieser Vorgang basierend auf Standort, Organisationseinheit oder einer anderen für Ihr Unternehmen geeigneten Methode weiter unterteilt werden.

Wie bei jeder neuen Technologie-Bereitstellung ist auch die Implementierung von Sophos Endpoint Protection mit einem gewissen Lernprozess verbunden, bis der normale Alltagsbetrieb reibungslos funktioniert. Die meisten finden unsere Lösung jedoch so benutzerfreundlich, dass sich die im Vorfeld investierte Zeit später mehr als bezahlt macht – sowohl durch Einsparungen bei der Verwaltung als auch durch den Vorteil, mehr Sicherheitsfunktionen auf Endpoint-Ebene nutzen zu können.

Fazit

Da Cyberbedrohungen sich mit rasender Geschwindigkeit weiterentwickeln, müssen Unternehmen neue Wege beschreiten, um ihre Investitionen in IT-Sicherheit optimal zu nutzen. Um die optimale Lösung für Ihr Unternehmen zu finden, sollten Sie bei der Wahl eines Endpoint-Produkts die folgenden Punkte beachten:

1. **Schutz** – erhalten Sie alle Sicherheitsfunktionen, die Sie benötigen, um moderne Bedrohungen abzuwehren, zu erkennen und zu bekämpfen?
2. **Benutzerfreundlichkeit** – können Sie die Lösung mit dem bei Ihnen zur Verfügung stehenden Personal und Kenntnisstand in Ihrem IT-Sicherheitsteam bereitstellen und verwalten?
3. **Support** – erhalten Sie bei Problemen fachkundige Hilfestellung von Sicherheitsexperten?

Viele Unternehmen erhalten mit Sophos Next-Gen Endpoint eine zukunftsfähige Lösung, die ihnen den erforderlichen Schutz und Support sowie die notwendige Benutzerfreundlichkeit bietet. Wenn Sie mit Ihrem derzeitigen Anbieter nicht komplett zufrieden sind, ist es vielleicht auch für Sie an der Zeit, sich den Tausenden von Kunden anzuschließen, die bereits zu Sophos gewechselt haben.

Weitere Informationen zu Sophos Next-Gen Endpoint Protection sowie eine kostenlose Testversion erhalten Sie auf **www.sophos.de/endpoint**.

Quellenangaben

1. „Smarter, faster hackers cause huge spike in cyberattacks", USA Today, 15. April 2015.
2. 2015 Data Breach Investigations Report, Verizon Enterprise Solutions, April 2015.
3. 2015 Global Study on IT Security Spending & Investments, Ponemon Institute LLC, Mai 2015.
4. Tolly Test Report, September 2015.

Sophos Next-Gen Endpoint Protection

Kostenlose 30-Tage-Testversion unter www.sophos.de/endpoint

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

Oxford, GB

2016-09-22 SB-DE (NP)

SOPHOS