FORRESTER®

Über die Cloud bereitgestellte Sicherheitsdienste von Palo Alto Networks verbessern die Sicherheit und ergänzen die Vorteile anderer Investitionen in die Netzwerksicherheit

Mit der steigenden Komplexität der Netzwerkarchitektur haben Sicherheitsteams zunehmend Schwierigkeiten, entsprechende Anpassungen vorzunehmen und für alle Geräte und Daten, die ihre Netzwerke und Clouds nutzen, eine durchgängige Sicherheit bereitzustellen. Abonnementbasierte Sicherheitsdienste werden bei den meisten Unternehmen zu einem immer beliebteren Bestandteil der Sicherheitsstrategie. Sie ermöglichen eine sofortige Skalierung mit topaktuellen Updates und vereinfachen die Bereitstellung und Verwaltung der Sicherheit. Obwohl der Preis für viele Unternehmen ein Hauptanliegen ist, müssen auch die spezifischen Funktionen jedes vorhandenen und neuen Sicherheitsprodukts berücksichtigt werden, um zu bewerten, wie diese Dienste in vorhandene Systeme und Workflows integriert werden und deren Effizienz steigern können.

Forrester sprach mit mehreren Palo Alto Networks-Kunden über ihre Investition in die über die Cloud bereitgestellten Sicherheitsdienste. Forrester führte diese Gespräche im Rahmen einer TEI-Studie (Total Economic Impact™), um den Wert und die Auswirkungen dieser Dienste auf die allgemeine Sicherheitsstrategie des Kunden zu ermitteln.

In Unternehmen findet man häufig eine Vielzahl punktueller Sicherheitslösungen und -dienste vor, die auf bestimmte Anforderungen zugeschnitten sind. Ressourceneinschränkungen und andere Faktoren verhindern, dass der Wert und die Möglichkeiten vieler dieser einzelnen Elemente vollständig genutzt werden.

Zu den **wichtigsten Herausforderungen** gehören:

- Erfolgreiche Verwaltung unübersichtlicher Sicherheitslösungen mit mehreren Anbietern, Plattformen und sich überschneidenden Funktionen
- Integration von über die Cloud bereitgestellten punktuellen Diensten, neuen Anwendungen oder Netzwerkkonfigurationen in vorhandene Cloud- oder On-Premise-Netzwerken und –Systemen

Vorteile der über die Cloud bereitgestellten Sicherheitsdienste

Zeit bis zur angemessenen Sicherheitslage im Vergleich zu einzelnen Punktlösungen

30 % schneller

Verringertes Risiko von Sicherheitslücken

45 %

Kosteneinsparungen bei der Sicherheitsinfrastruktur durch eine gemeinsame Plattform im Vergleich zu Punktlösungen

9,9 Millionen USD

- Effektive und effiziente Optimierung von Sicherheitsmaßnahmen, Prozessen und Richtlinien, um Lücken zu minimieren und gleichzeitig die Kontrolle zu behalten
- Analyse und Nachverfolgung von Lücken zwischen verschiedenen Anbietern mit ähnlichen Produkten, die in unterschiedlichen Infrastrukturen bereitgestellt werden

Darüber hinaus stellte Forrester fest, dass die Geschwindigkeit eine besonders große Rolle spielt – insbesondere, wenn es um die Abwehr von Angriffen geht, die längere Verweilzeiten benötigen, um sich im gesamten Netzwerk auszubreiten. Live-Dienste machen den entscheidenden Unterschied, um das Risiko für ein Unternehmen zu verringern.

Zu den in der Studie behandelten primären Diensten gehören Intrusion Detection and Prevention-Systeme (IPS/IDS), Malware-Analyse und Sandboxing, Web-Sicherheit (Secure Web Gateway [SWG]-Technologie, DNS-Sicherheit), Software-as-a-Service (SaaS)-Sicherheit (Cloud Access

Security Broker [CASB]) und Internet-of-Things (IoT)-Sicherheit.

Um die oben genannten wichtigsten Herausforderungen zu bewältigen, suchten Unternehmen nach einer einheitlichen Sicherheitslösung, die Folgendes ermöglicht:

- Automatische gemeinsame Nutzung von Informationen zur umfassenden Verteidigung
- Integration der gesamten vorhandenen Infrastruktur (Hardware, Software, Cloud und Abonnementdienste) in eine einzige Plattform
- Verwaltung über eine zentrale Konsole mit ähnlichem Erscheinungsbild

Palo Alto Networks bietet mehrere über die Cloud bereitgestellte Sicherheitsdienste, die speziell darauf ausgelegt sind, sich gegenseitig zu ergänzen und voneinander zu profitieren und dafür zu sorgen, dass Kunden den gesamten Datenverkehr über Netzwerke oder Clouds umfassend schützen können. Darüber hinaus unterstützen diese Sicherheitsfunktionen das Zero-Trust-Modell für Netzwerksicherheitsinitiativen.

Dieses Spotlight konzentriert sich ausschließlich auf die Nutzung der folgenden über die Cloud bereitgestellten Sicherheitsdienste von Palo Alto Networks durch die befragten Unternehmen sowie auf deren Wertschöpfung und Auswirkung auf die Unternehmen:

- Threat Prevention (für IPS)
- WildFire (für Malware-Analyse und Sandboxing)
- URL Filtering und DNS Security (für Web-Sicherheit oder SWG)
- IoT Security (für IoT-, IoMT- und OT-Sicherheit)
- Prisma SaaS (CASB- oder SaaS-Sicherheit)

Diese Lösungen werden mit den Next-Generation Firewalls (NGFW), der VM-Series und Prisma Access von Palo Alto Networks kombiniert, um eine lückenlose Sicherheit an allen Standorten zu gewährleisten, darunter Hauptsitz, Rechenzentrum, Zweigstellen und mobile Mitarbeiter.

Eine Beschreibung der einzelnen über die Cloud bereitgestellten Sicherheitsdienste finden Sie im Produktglossar.

DIE WICHTIGSTEN ERGEBNISSE

Zu den wichtigsten Ergebnissen der TEI-Studie gehören:

Effizienzsteigerungen von 6 Millionen USD für Sicherheitsabläufe und Endbenutzer. Die Teams des Security Operations Center (SOC) konnten die Anzahl der erweiterten Untersuchungen um 35 % reduzieren, die mittlere Lösungszeit (Mean-Time-to-Resolution, MTTR) um 20 % verbessern und die Anzahl der Geräte, für die ein neues Image erforderlich ist, um 50 % senken. Endbenutzer profitierten ebenfalls von diesen Vorteilen durch weniger und schnellere Interaktionen mit ihren Sicherheitsteams.

Die Einsparungen von 9,2 Millionen USD durch eine Reduzierung des Risikos von Sicherheitsverletzungen um 45 %. ML-Powered (Machine Learning-Powered) NGFW-Bereitstellung integrieren und erweitert diese, wodurch die Netzwerksicherheit und Funktionen verbessert werden und integrieren und ergänzt diese um Netzwerksicherheits- und andere Funktionen, während gleichzeitig die gesamte Angriffsfläche geschützt wird. Wenn es zu einer Verletzung der Datensicherheit kommt, müssen Unternehmen mit enorm hohen Kosten rechnen. Mit den über die Cloud bereitgestellten Sicherheitsdiensten von Palo Alto Networks wird das Auftreten eines Vorfalls von Anfang an verhindert, was auch dazu beiträgt, etwaige Folgekosten zu minimieren.

- **Weniger Bedrohungen im Zusammenhang mit Geräten und Aktivitäten von Mitarbeitern.** Dank des Zero-Trust-Ansatzes der über die Cloud bereitgestellten Sicherheitsdienste von Palo Alto Networks, die dem Zero Trust-Modell folgen, sind Unternehmen besser vor externen und internen Bedrohungen geschützt. Verschiedene Dienste arbeiten dabei zusammen, um den Webverkehr, den Anwendungsverkehr, Daten in SaaS-Anwendungen, Benutzer- und Entitätsanalysen, Datenexfiltration sowie Zero-Day-Exploits und Malware kontinuierlich zu überwachen. Ein besserer Schutz führt zu weniger Vorfällen, was sich wiederum in einer verbesserten Betriebszeit für Systeme und Mitarbeiter ausdrückt.
- **Entschärfung koordinierter Angriffe auf Anwendungen, Server und Standorte.** Mit den neuesten Erkennungsalgorithmen, Signaturen und Inline-Machine-Learning-Funktionen, die von den Produkten gemeinsam genutzt werden, können die über die Cloud bereitgestellten Sicherheitsdienste von Palo Alto Networks eine neu entdeckte Bedrohung in einem Unternehmen eines Kunden analysieren, deren Komponenten entpacken, die Informationen mit allen

Sicherheitsdiensten teilen und in Sekundenschnelle Präventivmaßnahmen übermitteln, sodass alle anderen Standorte oder Kunden an jedem Punkt des Angriffszyklus sicher vor diesem Zero-Day-Exploit bzw. dieser Variante geschützt werden. Ein einfaches Beispiel: Eine neue Malware, die versucht, eine Verbindung zu einer unbekannten Domain herzustellen, wird automatisch analysiert. Daraufhin erhalten die Lösungen Threat Prevention, WildFire, URL Filtering und DNS Security alle Updates mit diesen Informationen, um diese Vorgehensweise sowie jede einzelne Taktik in Zukunft bei allen Kunden zu verhindern. Dieser einzigartige Aspekt bietet einen deutlich verbesserten grundlegenden Schutz vor Zero-Day-Exploits und Bedrohungen gegenüber älteren und isolierten Cloud-basierten Punktlösungen.

Kosteneinsparungen bzw. -vermeidung von 9,9 Millionen USD bei Sicherheitsinfrastrukturen und weitere Effizienzsteigerungen von 1,9 Millionen USD bei der Verwaltung des Sicherheitsportfolios, wodurch Workloads um nahezu 50 % reduziert werden. Mit den über die Cloud bereitgestellten Sicherheitsdiensten von Palo Alto Networks können Unternehmen einen großen Teil ihres alten Sicherheitsportfolios rationalisieren und entfernen, wodurch die Anzahl der Anbieter in ihrer Umgebung und die Anzahl der Sicherheitslizenzen, die zum Schutz ihrer Netzwerke erforderlich sind, reduziert werden.

- **Weniger Verwaltungsaufwand durch reduzierte Komplexität.** Die befragten Unternehmen konnten nahezu die Hälfte ihres mit der Verwaltung der Sicherheitsinfrastruktur beauftragten Teams in anderen Bereichen einsetzen, da die über die Cloud bereitgestellten Sicherheitsdienste von Palo Alto Networks nahtlos in Panorama, dem Verwaltungstool für die Netzwerksicherheit von Palo Alto Networks, integriert sind und so ein einheitliches Erscheinungsbild über alle Produkte hinweg gewährleisten. Managementteams konnten auf eine „Shift Left“-Strategie umstellen, um Vorfälle zu vermeiden, die eine erweiterte Untersuchung erfordern und den Aufwand für Updates und Patching sowie für das Richtlinien- und Datenmanagement zu minimieren, indem sie einen zentralen Ort zur Verwaltung aller Sicherheitsrichtlinien nutzten.

  Ein Leiter der IT-Architektur in der Technologiebranche sagte: „Ich habe jetzt eine einheitlichere Sicherheitspolitik in meiner gesamten Infrastruktur weltweit. Anstelle von verschiedenen Anbietern mit unterschiedlichen Richtlinien und separaten Updates habe ich nun einen konsistenten Sicherheitsansatz für alle Umgebungen. Das lässt sich auf eine zentrale Ansicht zurückführen, aber auch ohne diese habe ich eine Sicherheitsrichtlinie, die ich nur einmal definieren muss und dann überall verwenden kann.“

- **Eine gemeinsame Plattform reduziert die Anzahl der Anbieter und Sicherheitslizenzen, sodass Unternehmen ihre Sicherheitslösungen konsolidieren und rationalisieren können.** Durch die Bereitstellung einer umfassenden Sicherheitssuite mit Produkten und Funktionen, die alle in eine zentralisierte Plattform integriert sind, konnten Unternehmen die Kosten ihres Sicherheitsportfolios erheblich senken, Punktlösungen beseitigen und die Anzahl der Anbieter und unterschiedlichen Technologien in ihren Umgebungen reduzieren. Ein weiterer Vorteil dieser Konsolidierung besteht darin, dass die über die Cloud bereitgestellten Sicherheitsdienste und NGFWs von Palo Alto Networks auf Zusammenarbeit ausgelegt sind. Die Befragten berichteten, dass sie ihr gesamtes Netzwerk, vom Rechenzentrum bis hin zu Endpunkten an entfernten Standorten, besser schützen können.

Dank den über die Cloud bereitgestellten Sicherheitsdiensten und Panorama können Sie **der Hälfte Ihres Sicherheitsteams neue Aufgaben zuweisen.**

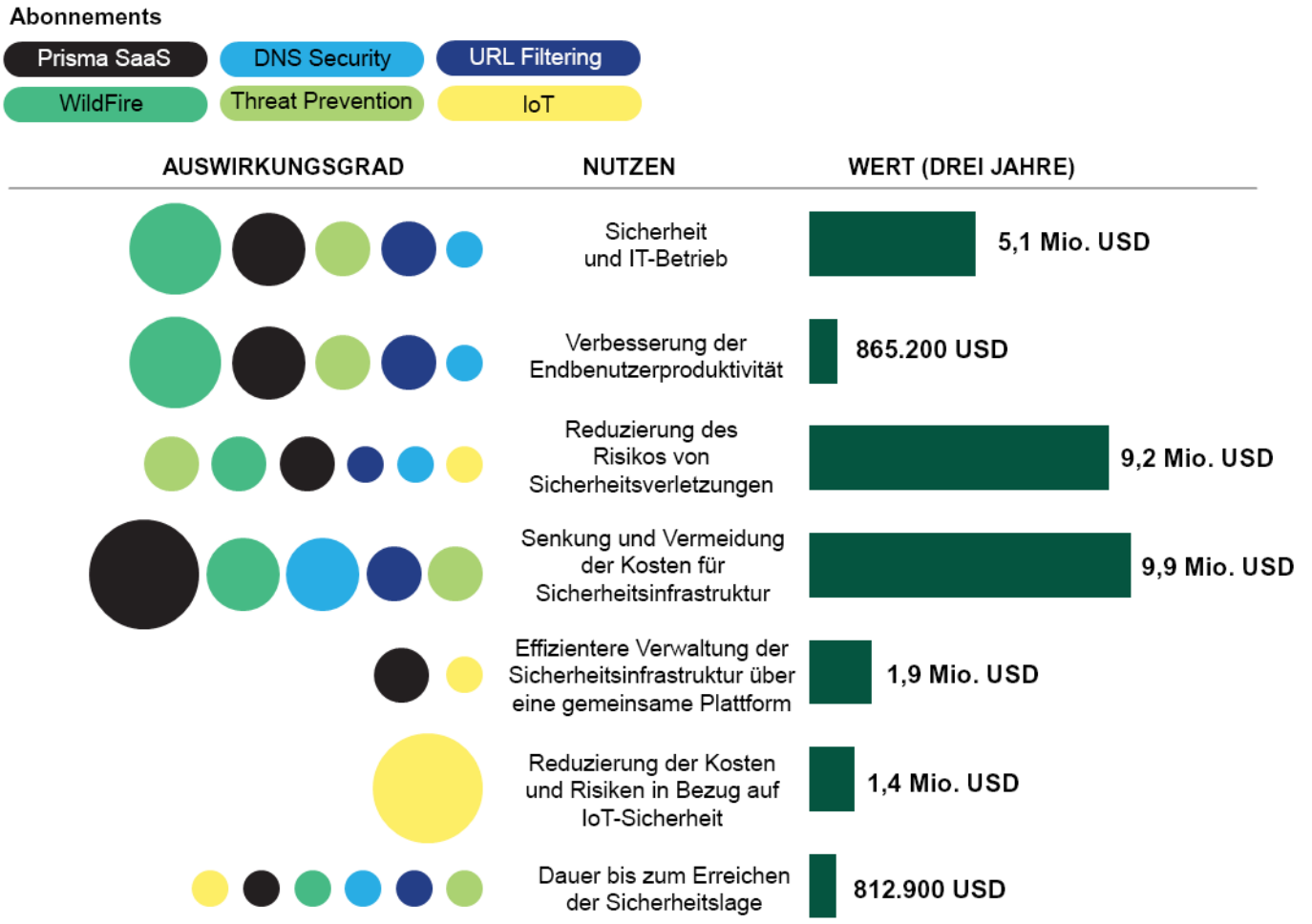
Einsparungen von 1,4 Millionen USD bei der IoT-Infrastruktur durch geringeren Managementaufwand und eine Reduzierung der Anzahl der neu erworbenen IoT-Geräte. Mit IoT Security konnten die Unternehmen alle ihre IoT-Geräte von einer zentralen Plattform aus identifizieren und schützen, den Zustand und Standort jedes einzelnen Geräts schnell ermitteln und den Wert und die Auslastung jedes Geräts mit den erweiterten Berichtsfunktionen maximieren. Dadurch konnten Neukäufe um 10 % reduziert werden.

Einsparungen von 812.000 USD durch das schnellere Erreichen der Sicherheitslage mit Palo Alto Networks, wodurch mehr Zeit für Verbesserungen zur Verfügung steht. Mit Palo Alto Networks konnten Unternehmen die Zeiten für Bereitstellung und Feineinstellung verkürzen. Die native Integration in NGFW-, VM-Series- und Prisma Access-Bereitstellungen sowie ergänzende Verwaltungsfunktionen machten es Unternehmen leichter, einen stabilen Zustand ihrer Sicherheitslösungen zu erreichen.

Ein leitender Direktor für Cybersicherheit in der Unterhaltungsbranche bemerkte: „Der enorm reduzierte Schulungsbedarf bedeutet insgesamt eine viel konsequentere und schnellere Pflege der Lösung. Mein Team ist in der Lage, die Dinge einfacher auf dem neuesten Stand zu halten, und das ist wichtig, weil Cyberkriminelle ständig an neuen Taktiken arbeiten."

- **Weniger Zeit für Schulung, Wartung und Untersuchung bedeutet mehr Zeit für die Weiterentwicklung von Projekten und für die Wertschöpfung des Unternehmens.** Ein leitender Netzwerkarchitekt in der Einzelhandels-/Fertigungsindustrie erklärte: „Seit dem Wechsel zu Palo Alto Networks arbeiten wir an viel mehr Projekten. Aktuell gibt es mehrere große Projekte, für die wir in der Vergangenheit einfach nicht über die erforderlichen Ressourcen verfügten. Dank Palo Alto Networks verbringen wir viel mehr Zeit mit Projekten und viel weniger Zeit mit der täglichen Pflege."

Relative Auswirkungen der über die Cloud bereitgestellten Sicherheitsdienste von Palo Alto Networks



Quelle: Tabellen zur Berechnung der Vorteile aus „The Total Economic ImpactTM of Palo Alto Networks for Network Security and SD-WAN" (Der Total Economic ImpactTM von Palo Alto Networks für Netzwerksicherheit und SD-WAN), einer von Forrester Consulting im Auftrag von Palo Alto Networks im November 2020 durchgeführten Studie

DIE AUSWIRKUNGEN DER EINZELNEN ÜBER DIE CLOUD BEREITGESTELLTEN SICHERHEITSDIENSTE

Im Folgenden finden Sie eine Beschreibung der einzelnen über die Cloud bereitgestellten Sicherheitsdienste sowie deren relative Auswirkungen auf die oben aufgeführten Vorteile.

Prisma SaaS bietet Sicherheit und Compliance für SaaS-Umgebungen und Cloud-Daten. Prisma SaaS ermöglicht eine sicherere Cloud-Nutzung durch Transparenz, Compliance-Kontrollen und Sicherheit für SaaS-Anwendungen und sensible Daten. Der Dienst hilft Unternehmen dabei, die Schatten-IT einzudämmen, SaaS-Unternehmensanwendungen zu schützen, das Risiko eines Verstoßes oder einer versehentlichen Datengefährdung in der Cloud zu verringern und den Datenschutz und die Compliance zu verbessern.

Mit Prisma SaaS erhalten Unternehmen durchgehende Cloud-Sicherheit und Datensicherheit für genehmigte und nicht genehmigte SaaS-Anwendungen. Als integrierter Bestandteil des Sicherheitspakets von Palo Alto Networks ist der Dienst eng in das unternehmensweite Cybersicherheitsprogramm integriert und bietet eine optimierte Bereitstellung, die es ermöglicht, die punktuellen Kontrollen abzulösen, wie die integrierten Sicherheitsfunktionen CASB und SaaS.

Durch die Sicherung des Webzugriffs werden Warnmeldungen und Untersuchungen reduziert. URL Filtering erkennt und blockiert alle webbasierten Bedrohungen und sendet Warnmeldungen und Daten an Panorama, um bei Bedarf eine Sekundäranalyse und Richtlinienüberprüfung durchzuführen. URL Filtering von Palo Alto Networks ermöglicht Benutzern den sicheren Zugriff auf das Internet, indem sie vor Phishing-Angriffen, Malware, Exploit-Kits und anderen schädlichen Websites geschützt werden. Der URL Filtering-Dienst lässt sich nativ in alle physischen, virtuellen und über die Cloud bereitgestellten NGFWs integrieren, sodass Sicherheitsteams nur einen einzigen Richtliniensatz verwalten und bereitstellen müssen.

Mit URL Filtering reduzieren Unternehmen die Anzahl der Sicherheitsvorfälle, die eine erweiterte Untersuchung erfordern, verringern die Wahrscheinlichkeit einer Verletzung der Datensicherheit und nehmen veraltete Websicherheitstechnologien außer Betrieb.

WildFire schützt Ressourcen vor Zero-Day-Bedrohungen. WildFire bietet Cloud-basierte Malware-Erkennung und Sandboxing mit Echtzeit-Updates zum Schutz vor schwer zu erfassenden und bisher unbekannten Bedrohungen, einschließlich schnelllebiger polymorpher Malware. Zusätzlich zum Echtzeit-Streaming von Updates unterstützt WildFire eine Inline-Machine-Learning-Funktion, die die meisten neuen dateibasierten Bedrohungen sofort blockiert. WildFire wurde schnell zu einem Schlüsselelement für die Sicherheitslage der befragten Unternehmen, da dieser Dienst sofortigen Schutz bietet, Informationen zur Verbesserung anderer Dienste verteilt, die Anzahl der Ereignisse pro Analystenstunde durch detaillierte Einblicke in das Verhalten identifizierter Bedrohungen reduziert und das SOC mit praxistauglichen Warnmeldungen versorgt.

Mit WildFire verbessern Unternehmen die Effizienz von IT- und SOC-Teams, verringern die Wahrscheinlichkeit von Datenverstößen und legen veraltete Sandboxing-Technologien still.

DNS Security blockiert schädliche Domains und wendet vorausschauende Analysen an, um Angriffe zu unterbinden, die DNS zur Kontrollübernahme oder zum Datendiebstahl verwenden. Die Lösung überwacht den DNS-Datenverkehr und verhindert Tunneling, Algorithmen zur Domain-Generierung und andere DNS-basierte Bedrohungen, die es Angreifern ermöglichen könnten, sich im gesamten Netzwerk auszubreiten.

DNS Security verhindert Bedrohungen auf DNS-Ebene, bevor sie Schaden anrichten können, und entlastet Ihre anderen Sicherheitsgeräte und Mitarbeiterressourcen.

Reduzierte jährliche Ausgaben für neue IoT-Geräte

10 %

Threat Prevention stoppt bekannte Bedrohungen und Schwachstellen früher. Threat Prevention von Palo Alto Networks umfasst IPS- und Suchfunktionen zur Erkennung von Bedrohungen, um alle bekannten Bedrohungen und Schwachstellen über den gesamten Datenverkehr in einem einzigen Durchgang zu verhindern. Der Dienst verbessert die Funktionen von NGFW--Bereitstellungen, indem er automatisch die neuesten Bedrohungsdaten für alle NGFW-Formfaktoren bereitstellt. Exploits, Spyware, Malware und andere Bedrohungen werden frühzeitig verhindert, um Infektionen und die entsprechende Erstellung und Untersuchung von Warnmeldungen zu vermeiden. In Verbindung mit WildFire für den Schutz vor unbekannten Bedrohungen kann Threat Prevention Malware früher blockieren, indem alle Sicherheitskontrollen gemeinsam genutzt werden, um Schutz nahezu in Echtzeit zu gewährleisten.

Mit Threat Prevention reduzieren Unternehmen die Anzahl der Sicherheitsvorfälle, die eine erweiterte Untersuchung erfordern, verringern die Wahrscheinlichkeit einer Verletzung der Datensicherheit und nehmen veraltete IPS-Lösungen außer Betrieb.

IoT Security reduziert den Verwaltungsaufwand und verlängert den Lebenszyklus von Geräten. Palo Alto Networks IoT Security lässt sich mit den NGFWs, der VM-Series und der Prisma Access-Verwaltungskonsole von Palo Alto Networks integrieren und bietet Unternehmen einen zentralen Ort zum Anzeigen und Verwalten von Richtlinien für alle IoT-Geräte. Nach der Implementierung von IoT Security konnten die befragten Unternehmen bisher unbekannte oder verlorene Geräte für die Segmentierung leicht aufspüren und den gesamten Geräteverkehr überwachen. Darüber hinaus stellte Palo Alto Networks IoT Security empfohlene Vertrauensrichtlinien bereit, um Sicherheitskontrollen einfacher auf IoT-Geräte anzuwenden, die Unternehmenssicherheit zu verbessern, die Angriffsfläche für potenzielle Täter zu verringern und Risiken genauer zu kontrollieren.

> **„Ich habe jetzt eine einheitlichere Sicherheitspolitik in meiner gesamten Infrastruktur weltweit.“**
>
> *Leiter IT-Architektur, Technologie*

WARUM UNTERNEHMEN SICH FÜR DIE ÜBER DIE CLOUD BEREITGESTELLTEN SICHERHEITSDIENSTE VON PALO ALTO NETWORKS ENTSCHIEDEN HABEN

Die Befragten gaben mehrere Gründe für die Auswahl der über die Cloud bereitgestellten Sicherheitsdienste von Palo Alto Networks an, darunter:

- **Nahtlose Integration in eine zentrale Ansicht mit Palo Alto Networks Panorama.** Alle diese Dienste lassen sich nahtlos in die NGFW und Panorama, die zentrale Verwaltungsplattform von Palo Alto Networks, integrieren und reduzieren so den Arbeitsaufwand für die IT und das SOC-Team, indem eine gemeinsame Plattform mit einer gemeinsamen Schnittstelle für alle Sicherheitstechnologien und -dienste bereitgestellt wird. Ein Netzwerksicherheitsmanager in der Einzelhandelsbranche sagte: „Für uns spielt URL Filtering eine große Rolle bei unserer Sicherheitslage, und die Warnmeldungen von WildFire können sofort in entsprechende Maßnahmen umgesetzt werden.“

  Ein Senior VP in der Finanzdienstleistungsbranche erklärte: „Unser Hauptvorteil war unsere verbesserte Sicherheitslage vor allem rund um den Internetzugang. Mit Palo Alto Networks können wir erkennen, welcher Datenverkehr gerade übertragen wird, sodass wir den Zugriff auf das beschränken können, was uns wirklich wichtig ist, und alles andere blockieren können. Das ist sowohl für URLs als auch für Anwendungen möglich.“

  Ein VP für Cybersicherheit in der Unterhaltungsbranche fügte hinzu: „Einer der wichtigsten Vorteile ist die Konsistenz innerhalb der Plattform. Jemand, der Prisma SaaS, Prisma Cloud usw. verwaltet, sieht bei all diesen Tools und Services eine ähnliche Oberfläche. Jetzt muss ich keine Leute mehr zu verschiedenen Schulungen schicken, um herauszufinden, wie wir unsere Tools verwenden müssen. Und alles andere gibt es in Panorama, d. h. Threat Prevention, WildFire, URL Filtering, DNS Security, die Firewall-Richtlinien und Entschlüsselungsregeln – alles in Panorama. Es läuft alles auf diese gemeinsame Benutzeroberfläche hinaus.“

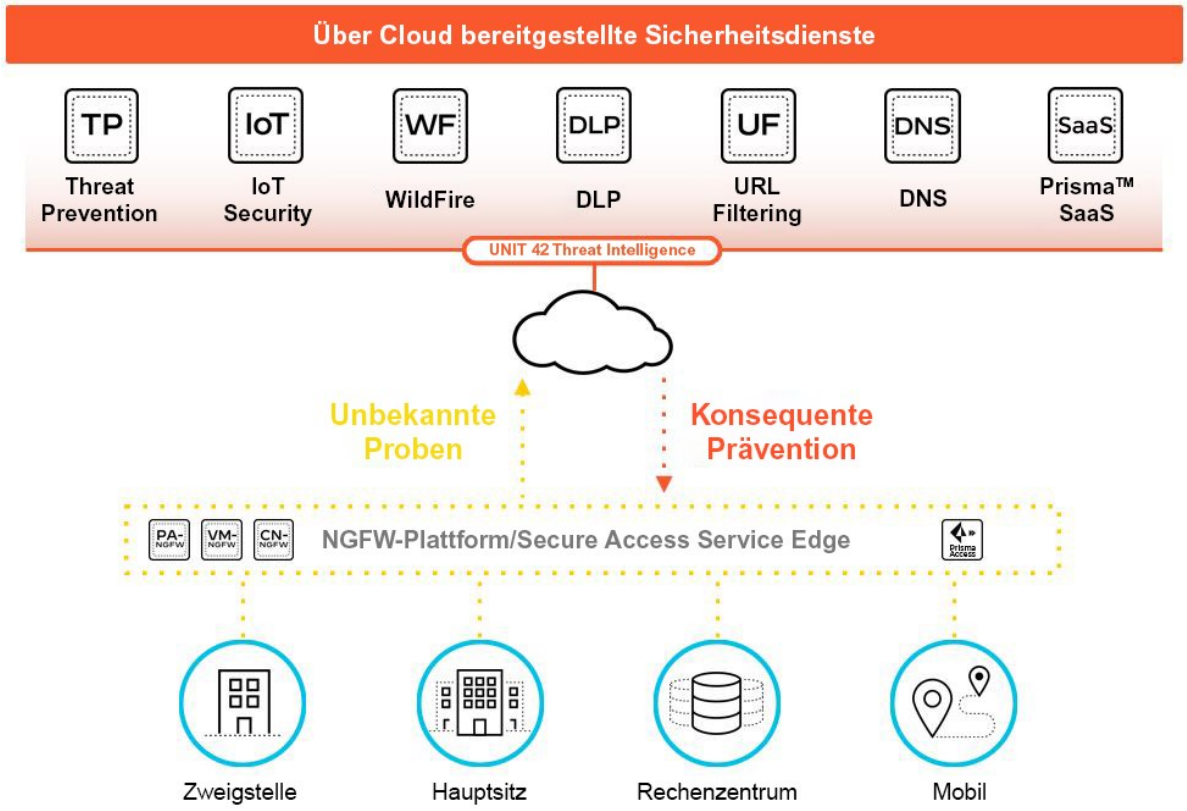
- **Sicherheit ohne Leistungseinbußen.** Die Befragten stellten fest, dass sich die Sicherheitsbranche im Allgemeinen auf ein abonnementbasiertes Dienstmodell zubewegt und dass die Palo Alto Networks-Technologie mit ihren parallelen Verarbeitungsfunktionen speziell darauf ausgelegt ist, die Konkurrenz in dieser Art von Umgebung zu übertreffen. Darüber hinaus verbessern sich die Sicherheitsangebote durch Inline-Machine-Learning von Palo Alto Networks kontinuierlich und bieten einen besseren Schutz.

  Ein CISO im Einzelhandel sagte: „Wir wussten, dass die Sicherheitsbranche zukünftig mehr Abonnements mit bestehender Hardware nutzen wird. Und nach dieser Annahme gehen wir vor. Palo Alto Networks ist die einzige Firewall, die mit einer Architektur für parallele Verarbeitung entwickelt wurde. Wenn alle Funktionen aktiv sind, so wie wir es für unseren Betrieb benötigen, gibt es keinen Leistungsverlust wie bei den anderen Technologien.“

Glossar: Palo Alto Networks-Produkte

Die folgenden Informationen werden von Palo Alto Networks bereitgestellt. Forrester hat die Angaben nicht geprüft und spricht weder eine Empfehlung für Palo Alto Networks noch für die Angebote des Unternehmens aus.

- **CLOUDGENIX SD-WAN:** Anwendungsdefinierte und autonome SD-WAN-Lösung der nächsten Generation, eine Cloud-basierte Servicebereitstellung an Filialstandorten ermöglicht.
- **DNS SECURITY:** Ein Cloud-basierter Dienst, der vorausschauende Analysen anwendet, um Angriffe, die DNS für C2 oder Datendiebstahl verwenden, sofort bei ihrem Auftreten zu unterbrechen.
- **ENTERPRISE DATA LOSS PREVENTION (DLP):** Die branchenweit erste über die Cloud bereitgestellte DLP-Lösung für Unternehmen, die vertrauliche Daten in allen Netzwerken, Clouds und bei allen Benutzern durchgehend schützt. (Enterprise DLP wurde nicht in die TEI-Analyse einbezogen.)
- **IOT SECURITY:** Das branchenweit einzige komplette IoT-Sicherheitsprodukt mit Transparenz, Prävention und Durchsetzung für jedes IoT- und OT-Gerät.
- **NEXT-GENERATION FIREWALLS (NGFW):** Branchenführende Produktfamilie von physischen (PA-Serie), virtualisierten (VM-Serie) und containerisierten (CN-Serie) Firewalls, die maschinelles Lernen für proaktiven Schutz nutzen.
- **PANORAMA:** Zentralisierte Lösung für das Management der Netzwerksicherheit für Ihre Palo Alto Networks Next-Generation Firewalls – alle Formfaktoren und alle Standorte.
- **PRISMA ACCESS:** Eine SASE-Lösung (Secure Access Service Edge) für Netzwerke und Sicherheit in einer speziell auf die Cloud abgestimmten Infrastruktur.
- **PRISMA SAAS:** Umfassende Transparenz, Sicherheit und Compliance für die branchenweit größte Palette an SaaS-Anwendungen und Ihre Daten.
- **THREAT PREVENTION:** Das marktführende fortschrittliche Intrusion Prevention System (IPS) prüft den gesamten Datenverkehr auf Bedrohungen und blockiert automatisch bekannte Schwachstellen.
- **UNIT 42:** Das Global Threat Team von Palo Alto Networks, die anerkannte Autorität im Bereich Cyberbedrohungen, liefert Sicherheitsteams Einblicke und durchdachte Schutzmechanismen im gesamten Produktportfolio, indem es detaillierte Untersuchungen zu Bedrohungsakteuren, deren Tools, Techniken und Verfahren durchführt.
- **URL FILTERING:** Über die Cloud bereitgestellte Websicherheit, die vor webbasierten Bedrohungen wie Phishing, Malware und Command-and-Control-Angriffen schützt.
- **WILDFIRE:** Branchenführende fortschrittliche Malware-Analyse-Engine, die unbekannte dateibasierte Bedrohungen identifiziert und Schutz davor bietet.



ZUSÄTZLICHE RESSOURCEN

Forrester entwickelte zusätzliche Ressourcen, um die Auswirkungen und Vorteile der in dieser Studie genannten Lösungen genauer zu analysieren. Weitere Informationen und Zugang zu diesen zusätzlichen Ressourcen finden Sie hier:

- The Total Economic Impact™ von Palo Alto Networks für Netzwerksicherheit und SD-WAN
- Zusammenfassung:TEI™ von Palo Alto Networks für Netzwerksicherheit und SD-WAN
- TEI-Spotlight: CloudGenix SD-WAN
- TEI Spotlight: Prisma Access

TOTAL ECONOMIC IMPACT-ANALYSE

Um weitere Informationen zu erhalten, laden Sie den vollständigen Bericht „The Total Economic Impact™ of Palo Alto Networks For Network Security And SD-WAN“ herunter, der von Palo Alto Networks in Auftrag gegeben und von Forrester Consulting bereitgestellt wurde.

UNTERSUCHUNGSERGEBNISSE

Forrester befragte neun Entscheidungsträger in verschiedenen Unternehmen, die Erfahrungen mit den NGFWs von Palo Alto Networks und über die Cloud bereitgestellten Sicherheitsdienste gesammelt hatten, und fasste die Ergebnisse in einer dreijährigen Finanzanalyse eines Modellunternehmens zusammen. Auf der Basis des ermittelten Risikobarwerts wurden dabei folgende Vorteile identifiziert:

- Einsparungen von insgesamt 5,1 Millionen USD durch Effizienzsteigerungen bei Sicherheits- und IT-Vorgängen, einschließlich einer 35%-igen Reduzierung der Sicherheitsvorfälle, die eine erweiterte Untersuchung erfordern, und einer Reduzierung der MTTR um 20 %.
- Risikoreduzierung in Bezug auf Datenmissbrauch um 45 % und Einsparungen von 9,2 Millionen USD.
- Einsparungen von insgesamt 11,7 Millionen US-Dollar durch Kostenvermeidung und effizientere Verwaltung der Sicherheitsinfrastruktur.

Return on investment (ROI)

247 %

Net Present Value (NPV, Nettobarwert)

28,5 Millionen USD

HAFTUNGSAUSSCHLUSS

Der Leser sollte Folgendes beachten:

- Die Studie wurde von Palo Alto Networks in Auftrag gegeben und von Forrester Consulting erstellt. Sie ist keine Marktanalyse.
- Forrester trifft keine Annahmen zum potenziellen ROI, den andere Unternehmen erzielen können. Forrester empfiehlt dringend, dass Leser ihre eigenen Schätzungen innerhalb des im Bericht bereitgestellten Bezugsrahmens verwenden, um die Angemessenheit einer Investition in Palo Alto Networks zu ermitteln.
- Palo Alto Networks hat die Studie geprüft und Forrester entsprechendes Feedback gegeben. Forrester behält jedoch die redaktionelle Kontrolle über die Studie und ihre Ergebnisse und akzeptiert keine Änderungen, die im Widerspruch zu den Ergebnissen von Forrester stehen oder den Sinngehalt der Studie verfälschen.
- Die Namen der befragten Kunden wurden von Palo Alto Networks bereitgestellt, Palo Alto Networks selbst nahm jedoch nicht an den Befragungen teil.

ÜBER TEI

Total Economic Impact™ (TEI) ist eine von Forrester Research, Inc. entwickelte Methodik, die die technologiebezogenen Entscheidungsprozesse von Unternehmen optimieren und Anbieter dabei unterstützen soll, Kunden das Nutzenversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die TEI-Methodik unterstützt Unternehmen darin, den materiellen Wert von IT-Initiativen gegenüber der Geschäftsführung und anderen wichtigen Entscheidungsträgern im Unternehmen aufzuzeigen, zu begründen und zu veranschaulichen. Die TEI-Methodik umfasst vier Komponenten, mit denen der Investitionswert eingeschätzt wird: wirtschaftlicher Nutzen, Kosten, Risiken und Flexibilität.


FORRESTER®