ÜBERBLICK FIREWALL

Palo Alto Networks Next-Generation Firewall

Wesentliche Änderungen in Anwendungsnutzung und Benutzerverhalten sowie eine komplexe, unübersichtliche Netzwerkinfrastruktur bilden ein Bedrohungsszenario, das die Schwächen traditioneller, portbasierter Netzwerksicherheit offenlegt. Ihre Benutzer fordern den Zugriff auf immer mehr Anwendungen auf vielen verschiedenen Gerätetypen und sind sich der Sicherheitsrisiken oft kaum bewusst. Gleichzeitig müssen Sie aufgrund von Erweiterungen des Rechenzentrums, Netzwerksegmentierungen, Virtualisierungs- und Mobilitätsinitiativen überdenken. Sie müssen überlegen, wie Sie den Zugriff auf Anwendungen und Daten ermöglichen und dabei Ihr Netzwerk vor einer neuen Generation komplexer Bedrohungen schützen können, die herkömmliche Sicherheitsmechanismen umgehen.

Früher hatten Sie zwei Möglichkeiten: Entweder zum Schutz Ihres Netzwerks alles sperren oder im Interesse des Unternehmens alles aktivieren. Diese Möglichkeiten ließen wenig Raum für Kompromisse. Die Palo Alto Networks® Next-Generation Security Platform bietet Ihnen eine Möglichkeit, die Anwendungen, die Ihre Benutzer benötigen, auf sichere Weise zu aktivieren. Sie können den Zugriff ermöglichen und Cybersicherheitsbedrohungen abwenden.

Unsere Next-Generation Firewall ist das Herzstück unserer Next-Generation Security Platform, die dafür gemacht ist, die komplexesten Bedrohungen zu finden. Unsere Next-Generation Firewall überwacht den gesamten Datenverkehr – einschließlich sämtlicher Anwendungen, Bedrohungen und Inhalte – und ordnet ihn dem jeweiligen Benutzer zu, unabhängig von dessen Standort oder der Art des verwendeten Geräts. Dadurch werden Anwendung, Inhalte und Benutzer – also die Kernkomponenten Ihres Geschäftsbetriebs – zu integralen Bestandteilen der Sicherheitsstrategie Ihres Unternehmens. So können Sie Sicherheit mit Ihren wichtigsten Geschäftsvorhaben in Einklang bringen. Mit unserer Next-Generation Security Platform reduzieren Sie die Reaktionszeit auf Zwischenfälle, entdecken unbekannte Bedrohungen und optimieren den Einsatz von Sicherheitsnetzwerken.

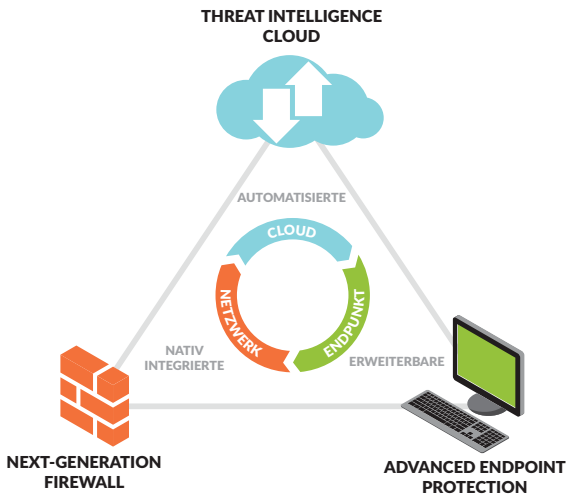

Abbildung 1: Palo Alto Networks Next-Generation Security Platform

- Aktivieren Sie Anwendungen, Benutzer und Inhalte auf sichere Weise durch die Klassifizierung von Datenverkehr, Bestimmung des Geschäftsgebrauchs und Zuweisung von Strategien zum Gewähren und Schützen von Zugang zu relevanten Anwendungen, inklusive SaaS-Anwendungen.
- Beugen Sie durch die Löschung ungewollter Anwendungen Bedrohungen vor. Wenden Sie außerdem gezielte Sicherheitsstrategien an, um das Ausnutzen von Sicherheitslücken zu verhindern und Viren, Spyware, Botnets und unbekannte Malware zu blockieren (APTs).
- Schützen Sie Ihre Rechenzentren durch Validierung von Anwendungen, Isolation von Daten, Kontrolle über defekte Anwendungen und ultraschnelle Abwehr von Bedrohungen.
- Sichern Sie öffentliche und private Cloud-Computing-Umgebungen mit erhöhter Sichtbarkeit und Kontrolle. Stellen Sie Sicherheitsstrategien mit der gleichen Geschwindigkeit wie Ihre virtuellen Maschinen bereit, setzen Sie sie durch und behalten Sie sie bei.
- Fördern Sie sichere mobile Computernutzung durch die Erweiterung der Next-Generation Security Platform auf Benutzer und Geräte unabhängig vom Standort.

- Optimieren Sie mit intuitiven Verwaltungsfunktionen Geräte-, Netzwerk- und Strategienverwaltung – angepasst an Ihre Organisationsstruktur.

Die Next-Generation Security Platform unterstützt Ihr Unternehmen dabei, ein Spektrum an Sicherheitsanforderungen zu erfüllen, die auf einem gemeinsamen Prinzip basieren. Durch die Nutzung einer ausgewogenen Kombination von Netzwerksicherheit und intelligenter Bedrohungserkennung sowie Endpoint Protection können Sie geschäftliche Initiativen unterstützen und gleichzeitig Ihre gesamte Sicherheitslage verbessern sowie die Reaktionszeit bei Sicherheitsvorfällen reduzieren.

Nutzung von Sicherheit zur Stärkung Ihres Unternehmens

Unsere Next-Generation Security Platform ermöglicht Ihnen, Ihr Unternehmen mit Strategien zu Anwendungen, Benutzern und Inhalten zu rüsten. Sie nutzt ein positives Kontrollmodell und ein einzigartiges Design, das es Ihnen ermöglicht, bestimmte Anwendungen oder Funktionen zu aktivieren und alles andere indirekt oder direkt zu blockieren. Die Next-Generation Firewall führt eine vollständige Stack- und Single-Pass-Überprüfung Ihres gesamten Datenverkehrs über alle Ports durch. Dadurch kann für jede Anwendung der gesamte Kontext berücksichtigt werden, einschließlich aller relevanten Inhalte und Benutzeridentitäten. Auf diese Weise entsteht eine solide Basis für die Entscheidung zu Sicherheitsstrategien.

- Klassifizieren Sie permanent alle Anwendungen auf allen Ports. Heutzutage können Anwendungen und ihr zugehöriger Inhalt eine portbasierte Firewall unter Anwendung verschiedener Techniken ohne Probleme umgehen. Unsere Next-Generation Security Platform wendet mannigfaltige Klassifizierungsmechanismen auf den Datenverkehr an, um Anwendungen, Bedrohungen und Malware zu identifizieren. Der gesamte Datenverkehr wird klassifiziert, unabhängig von Port, Verschlüsselung (SSL oder SSH) oder Ausweichmethoden. Nicht identifizierte Anwendungen, die normalerweise einen kleinen Prozentsatz ausmachen, aber ein hohes Risiko bergen, werden automatisch für systematisches Management klassifiziert.

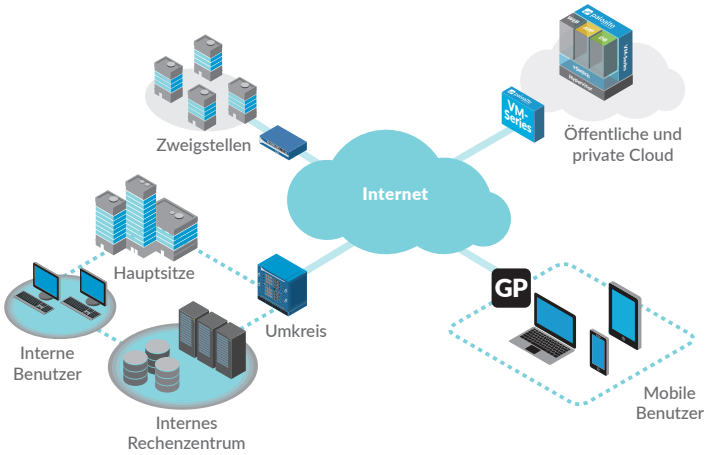

Abbildung 2: Wenden Sie in Ihrem gesamten Unternehmen sichere Umsetzungsstrategien an.

- Bedrohungsprofil verbessern, Cyberattacken vorbeugen. Wenn der Datenverkehr erst einmal vollständig klassifiziert ist, können Sie das Bedrohungsprofil des Netzwerks verbessern, indem Sie bestimmte Anwendungen zulassen und alle anderen ablehnen. Nun kann koordinierte Prävention von Cyberattacken angewandt werden, um bekannte Malwareseiten zu blockieren und das Ausnutzen von Sicherheitslücken, Viren, Spyware und schädliche DNS-Anfragen zu verhindern. Jegliche individuelle oder unbekannte Malware wird analysiert und identifiziert, indem die Dateien ausgeführt und direkt in einer virtuellen Sandkastenumgebung auf ihr schädliches Verhalten hin beobachtet werden. Wenn neue Malware entdeckt wird, wird automatisch eine Signatur für die infizierende Datei erstellt und zugehöriger Malwaredatenverkehr wird automatisch generiert und Ihnen bereitgestellt.
- Ordnen Sie Anwendungsdatenverkehr und dazugehörige Bedrohungen Benutzern und Geräten zu. Um Ihre Sicherheitslage zu verbessern und Vorfallreaktionszeiten zu verringern, ist es

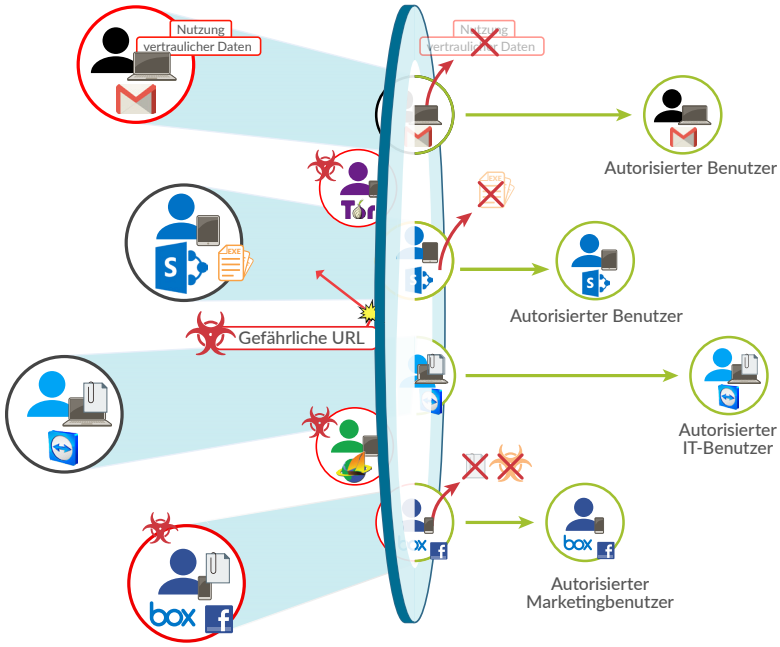

Abbildung 3: Anwendungen, Inhalte, Benutzer und Geräte – alles unter Kontrolle.

Abbildung 4: Die Anwendungsaktivität wird in einem übersichtlichen, leserlichen Format angezeigt. Fügen Sie Filter hinzu oder entfernen Sie diese, um mehr darüber zu erfahren, was die Anwendung beinhaltet, welche Funktionen sie hat und wer sie nutzt.

wichtig, die Anwendungsnutzung Benutzern und Gerätetyp zuzuordnen – und diesen Kontext auf Ihre Sicherheitsstrategien zu übertragen. Die Integration einer großen Bandbreite an Benutzerrepositorys des Unternehmens gibt die die Identität des Microsoft® Windows®-, Mac® OS X®-, Linux®-, Android®- oder iOS-Benutzers, der auf die Anwendung zugreift, sowie den Gerätetyp preis. Die Sichtbarkeit von und Kontrolle über Benutzer und Geräte ermöglicht die sichere Aktivierung von jeglicher Anwendung, die sich mit Ihrem Netzwerk kreuzt, ganz gleich, wo sich der Benutzer befindet oder was für ein Gerät er nutzt.

Die Bestimmung des Kontexts der genutzten Anwendungen, der Inhalte oder Bedrohungen, die sie mit sich bringen könnten und des dazugehörigen Benutzers oder Geräts helfen Ihnen, die Strategieverwaltung zu optimieren, Ihre Sicherheitslage zu verbessern und die Untersuchung von Vorfällen zu beschleunigen.

Vollständiger Kontext bedeutet strengere Sicherheitsstrategien

Best Practices im Bereich Sicherheit besagen, dass die Entscheidungen, die Sie in Bezug auf Strategien treffen, Ihre Fähigkeiten in der Berichterstattung über Netzwerkaktivitäten und Ihre forensische Kapazität vom Kontext abhängen. Gemeint ist der Kontext der genutzten Anwendung, der besuchten Webseite, der dazugehörigen Nutzlast und des Benutzers. Dies sind wertvolle Daten, die Sie zum Schutz Ihres Netzwerks benötigen. Wenn Sie genau wissen, welche Anwendungen Ihr Internetgateway kreuzen, in Ihrem Rechenzentrum oder Ihrer Cloud in Betrieb sind oder von Benutzern angewandt werden, können Sie bestimmte Strategien und gezielten Schutz vor Bedrohungen darauf anwenden. Das Wissen, wer der Benutzer über die IP hinaus ist, ist ein weiteres Kontextelement, das Sie dazu befähigt, Ihre Strategien feiner abzustimmen.

Eine große Bandbreite an interaktiven Visualisierungs- und Logfiltertools liefert Ihnen den Kontext der Anwendungsaktivität, der dazugehörigen Inhalte oder Bedrohungen, der Identität des Benutzers und des Gerätetyps. Jeder dieser Datenpunkte bildet einen Teil Ihres Netzwerks ab und zusammen ergeben sie ein Gesamtbild der potentiellen Sicherheitsrisiken. Dies hilft Ihnen dabei, fundierte Entscheidungen hinsichtlich der Sicherheitsstrategie zu treffen. Der gesamte Datenverkehr wird permanent klassifiziert. Wenn sich der Status ändert, werden alle Änderungen für die Analyse protokolliert und die grafischen Zusammenfassungen aktualisiert. Die Informationen werden über eine benutzerfreundliche, webbasierte Schnittstelle angezeigt.

- Im Internetgateway können Sie neue oder ungewöhnliche Anwendungen suchen und erhalten eine Kurzbeschreibung dieser mit den charakteristischen Verhaltensweisen sowie den Benutzern. Zusätzliche Sichtbarkeit bei URL-Kategorien, Bedrohungen und Datenschemata vervollständigen das Bild des Datenverkehrs, der in das Netzwerkgateway hinein fließt.
- Alle Dateien, die von WildFire™ auf unbekannte Malware analysiert wurden, werden integriert protokolliert. Dabei ist voller Zugriff auf alle Details, inklusive genutzte Anwendung, Benutzer, Dateityp, Ziel-OS und beobachtete gefährdende Verhaltensweisen gewährt.
- Verifizieren Sie innerhalb des Rechenzentrums alle genutzten Anwendungen und stellen Sie sicher, dass diese nur von autorisierten Benutzern verwendet werden. Zusätzliche Sichtbarkeit von Aktivitäten des Rechenzentrums kann bestätigen, dass keine falsch konfigurierten Anwendungen oder fehlerhaften Nutzungen von SSH oder RDP bestehen.
- Bedrohungsanalyse, Forensik und Verfolgung werden mit dem Autofocus™-Threat-Intelligence-Service beschleunigt. Dieser liefert individuelle kontextuelle Bedrohungsdaten direkt über PAN-OS® vom Gerät.
- Setzen Sie in öffentlichen und privaten Cloudumgebungen Strategien durch und schützen Sie Anwendungen mit der Next-Generation Platform. Gleichzeitig halten Sie Schritt mit der Erstellung und Bewegung Ihrer virtuellen Server.
- In allen Anwendungsszenarios können unbekannte Anwendungen, die üblicherweise einen kleinen Teil in jedem Netzwerk ausmachen, für Analysen und systematisches Management kategorisiert werden.

Häufig ist Ihnen nicht vollständig bewusst, welche Anwendungen in Benutzung sind, wie häufig sie genutzt werden und von wem. Vollständige Sichtbarkeit der unternehmensrelevanten Aspekte Ihres Netzwerkdatenverkehrs – nämlich Anwendungen, Inhalte und Benutzer – ist der erste Schritt zu einer Kontrolle, die auf mehr Wissen basiert.

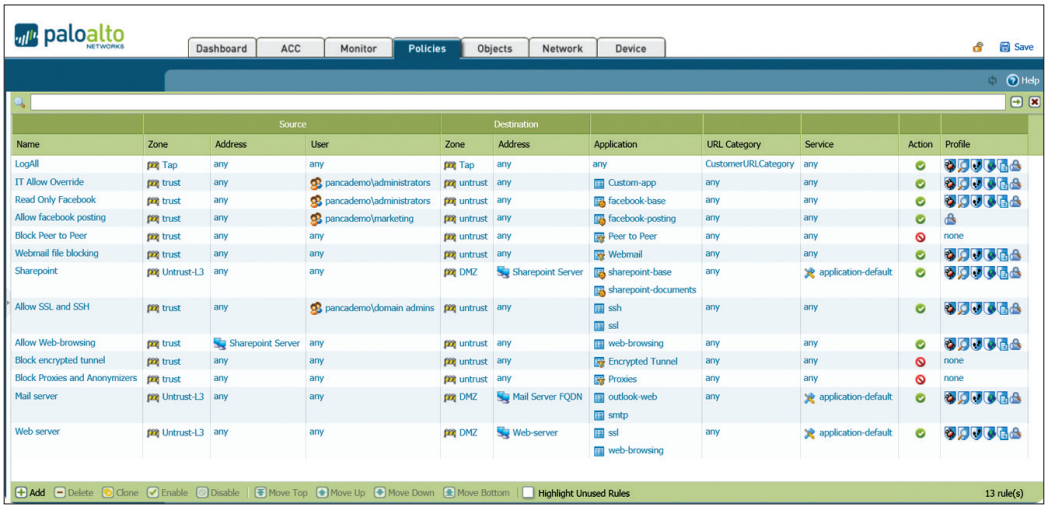

Abbildung 5: Der einheitliche Strategieneditor ermöglicht schnelle Erstellung und schnellen Einsatz von Strategien, die Anwendungen, Benutzer und Inhalte kontrollieren.

Reduzierung von Risiken durch Aktivierung von Anwendungen

Früher bedeutete der Prozess der Risikoreduzierung, dass der Zugriff auf Netzwerkdienste eingeschränkt werden musste und somit wurde das Unternehmen evtl. behindert. Heutzutage bedeutet Risikoreduzierung die sichere Aktivierung von Anwendungen mit einem unternehmenszentrierten Ansatz, der Sie dabei unterstützt, das Gleichgewicht zwischen dem früheren Alles-oder-Nichts-Prozess herzustellen.

- Nutzen Sie Anwendungsgruppen und SSL-Entschlüsselung, um Webmail und Instant Messaging auf wenige bestimmte Anwendungsvarianten zu beschränken. Untersuchen Sie diese auf alle Bedrohungen und laden Sie unbekannte verdächtige Dateien bei WildFire hoch (EXE, DLL, ZIP-Dateien, PDF-Dokumente, Office-Dokumente, Java®- und Android®-APK), um sie zu analysieren und Signaturen zu entwickeln.
- Kontrollieren Sie das Surfen im Internet für alle Benutzer, indem Sie unternehmensrelevante Webseiten zulassen und den Datenverkehr scannen sowie den Zugriff auf offensichtlich nicht arbeitsbezogene Webseiten sperren. „Trainieren“ Sie den Zugriff auf fragwürdige Webseiten durch individuelle Sperrseiten.
- Blockieren Sie alle Peer-zu-Peer-Datentransferanwendungen bei allen Benutzern durch dynamische Anwendungsfilter.
- Verschaffen Sie sich einen Überblick über die Nutzung von SaaS-Anwendungen in Ihrem Unternehmen und etablieren Sie detailgenauen Zugriff und Nutzungskontrollen für jede Anwendung. Verhindern Sie außerdem die Auslieferung von Malware durch diese Anwendungen.
- Fördern Sie mobile Geräte durch die Erweiterung Ihrer Internetgatewaystrategien und Fähigkeiten zur Abwehr von Bedrohungen auf Benutzer in aller Welt mit dem mobilen Sicherheitsservice GlobalProtect™.

Nutzen Sie im Rechenzentrum Kontext, um zu bestätigen, dass Ihre Rechenzentrumsanwendungen auf ihren Standardports laufen, finden Sie fehlerhafte Anwendungen, validieren Sie Benutzer, isolieren Sie Daten und schützen Sie unternehmensrelevante Daten vor Bedrohungen. Beispiele können Folgendes beinhalten:

- Isolieren Sie unter Verwendung von Sicherheitszonen das Verzeichnis der Kreditkartennummern auf der Grundlage von Oracle®, indem Sie den Oracle-Datenverkehr über seine Standardports erzwingen. Währenddessen untersuchen Sie den Datenverkehr auf eingehende Bedrohungen und beschränken den Zugang nur auf die Finanzgruppe.
- Erstellen Sie eine globale Managementanwendungsgruppe (z. B. SSH, RDP, Telnet) nur für die IT-Abteilung zur Nutzung im Rechenzentrum.
- In unserem virtuellen Rechenzentrum können Sie dynamische Objekte für die automatisierte Sicherheitsstrategieerstellung nutzen. Dabei werden virtuelle Sharepoint®-Maschinen erstellt, entfernt oder bewegen sich durch Ihre virtuelle Umgebung.

Schutz aktivierter Anwendungen und Inhalte

Wenn Sie Strategien zur Abwehr von Bedrohungen und zum Scannen von Inhalten anwenden, werden der Kontext von Benutzer und Anwendung integrierte Bestandteile Ihrer Sicherheitsstrategie. Vollständiger Kontext innerhalb Ihrer Bedrohungsabwehrstrategie entschärft Umgehungstaktiken wie Port-Hopping und Tunneln. Reduzieren Sie die Angriffsfläche durch das Aktivieren von ausgewählten Anwendungen und wenden Sie dann die Strategien zur Bedrohungsabwehr und zum Scannen von Inhalten auf diesen Datenverkehr an.

Die in Ihrer Strategie verfügbaren Elemente zur Bedrohungsabwehr und zum Scannen von Inhalten beinhalten Folgendes:

- **Unterbinden Sie bekannten Bedrohungen durch Nutzung von IPS und Antivirensoftware/Antispyware im Netzwerk.** Der Schutz vor einer Reihe von Bedrohungen wird durch Single-Pass-Überprüfung erreicht. Dabei werden ein einheitliches Signaturformat und eine datenstrombasierte Scan-Technologie eingesetzt. Das Intrusion Prevention System (IPS) verfügt über Funktionen zur Blockierung von Sicherheitslücken auf Netzwerk- und Anwendungsebene, Pufferüberläufen, DoS-Angriffen und Port-Scans. Antivirensoftware/Antispyware blockiert Millionen von Malwarevarianten, darunter auch diejenigen, die in komprimierten Dateien oder Internetdatenverkehr versteckt sind (komprimiertes HTTP/HTTPS) sowie bekannte PDF-Viren. Für mit SSL verschlüsselten Datenverkehr können Sie selektiv strategiebasierte Entschlüsselung anwenden und den Datenverkehr dann unabhängig von Ports auf Bedrohungen überprüfen.
- **Blockieren Sie unbekannte oder zielgerichtete Malware mit WildFire.** Unbekannte oder zielgerichtete Malware (z. B. anspruchsvolle hartnäckige Bedrohungen), die in Dateien versteckt ist, kann mit WildFire in vielen Betriebssystemen und Anwendungsversionen analysiert werden. Unbekannte Dateien werden dabei direkt in einer virtuellen Sandkastenumgebung in der Cloud oder auf dem WF-500-Gerät untersucht. WildFire beobachtet mehr als 420 schädliche Funktionsweisen und wenn Malware gefunden wird, wird automatisch eine Signatur

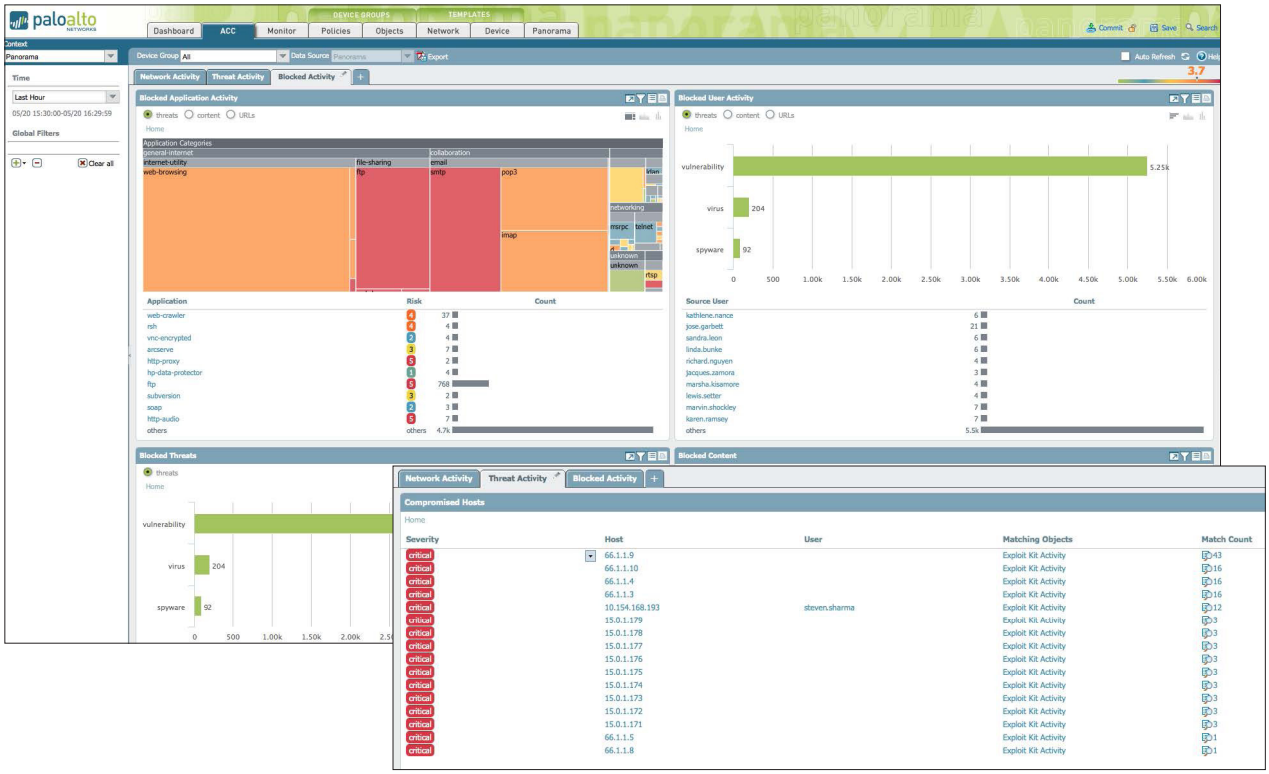

Abbildung 6: Inhalte und Bedrohungssichtbarkeit – URL-, Bedrohungs- und Datei-/Datentransferaktivitäten sowie infiltrierte Hosts in übersichtlichem, gut leserlichem und extrem anpassbarem Format anzeigen lassen. Filter hinzufügen und entfernen, um mehr über einzelne Elemente zu erfahren.

entwickelt und Ihnen in nur 5 Minuten zugestellt. Alle gängigen Dateitypen werden von WildFire unterstützt, darunter: PE-Dateien; Microsoft Office .doc, .xls und .ppt; Portable Document Format (PDF); Java Applet.

- **Identifizieren Sie botinfizierte Hosts und zerstören Sie die Netzwerkaktivität von Malware.** Eine vollständige, kontextuelle Klassifizierung von allen Anwendungen, in allen Ports, inklusive unbekanntem Datenverkehr, legt häufig Anomalien oder Bedrohungen in Ihrem Netzwerk offen. Verwenden Sie die Befehls- und Kontrollanwendung App-ID™, den Bericht zum Verhalten von Botnets, DNS-Sinkholing und passive DNS, um unbekannten Datenverkehr, verdächtige DNS- und URL-Abfragen schnell mit infizierten Hosts in Verbindung zu bringen. Wenden Sie globale Intelligenz an, um DNS-Abfragen für schädliche Domains abzufangen.
- **Beschränken Sie den nicht autorisierten Transfer von Dateien und Daten.** Funktionen zum Filtern von Daten ermöglichen es Ihren Administratoren, Strategien einzuführen, die Risiken im Zusammenhang mit unautorisiertem Datei- und Datentransfer reduzieren. Dateitransfers können gesteuert werden, indem in der Datei – und nicht nur in den Dateierweiterungen – gesucht wird. Daraufhin wird bestimmt, ob eine Transferaktion zulässig ist. Ausführbare Dateien, die typischerweise in Drive-by-Downloads gefunden werden, können gesperrt werden. So wird Ihr Netzwerk vor der unbemerkten Ausbreitung von Malware geschützt. Datenfilterfunktionen können den Fluss vertraulicher Datenmuster erkennen und steuern. Dazu gehören Kreditkarten- und Sozialversicherungsnummern sowie benutzerdefinierte Muster.
- **Das Surfen im Internet kontrollieren.** Eine voll integrierte, konfigurierbare URL-Filterfunktion ermöglicht es Ihren Administratoren, zusätzlich zur Anwendungssichtbarkeit fein abgestimmte Browsingstrategien einzuführen. Zusätzliche Kontrollstrategien schützen das Unternehmen außerdem vor einer großen Bandbreite von Risiken durch rechtliche Bestimmungen und Produktivität.
- **Gerätebasierte Strategie für den Anwendungszugriff.** Dank GlobalProtect können Unternehmen bestimmte Strategien nutzen, um zu kontrollieren, welche Geräte auf bestimmte Anwendungen und Netzwerkressourcen zugreifen können. Stellen Sie bspw. sicher, dass Laptops mit dem Firmenimage vereinbar sind, bevor Sie Zugriff auf das Rechenzentrum ermöglichen. Prüfen Sie, ob das mobile Gerät auf dem neuesten Stand, unternehmenseigen und repariert ist, bevor Sie auf sensible Daten zugreifen.
- **Bestätigen Sie infiltrierte Hosts automatisch.** Eine automatisierte Korrelationsfunktion sucht netzwerkübergreifend nach vorgegebenen Indikatoren für Infiltration, setzt Übereinstimmungen in Beziehung und reduziert dadurch die Notwendigkeit von manuellem Data-Mining.

Netzwerksicherheitsmanagement

Die Next-Generation Security Platform kann einzeln durch eine Command-Line-Schnittstelle (CLI) oder durch eine funktionsreiche, browserbasierte Schnittstelle verwaltet werden. Für groß angelegte Bereitstellungen können Sie Panorama™ verwenden, um global Sichtbarkeit, Strategiebearbeitung, Berichterstellung und Protokollierungsfunktionen für Ihre gesamte Hardware- und Virtual-Appliance-Firewalls bereitzustellen. Panorama bietet Ihnen ebenso viel kontextuelle Kontrolle über Ihre globale Bereitstellung wie Sie über eine einzelne Appliance haben.

Rollenbasierte Verwaltung ermöglicht es Ihnen, in Kombination mit Pre- und Post-Rules, die zentrale Kontrolle mit dem Bedarf an lokaler Bearbeitung von Richtlinien und Flexibilität der Gerätekonfiguration in Einklang zu bringen. Das Erscheinungsbild

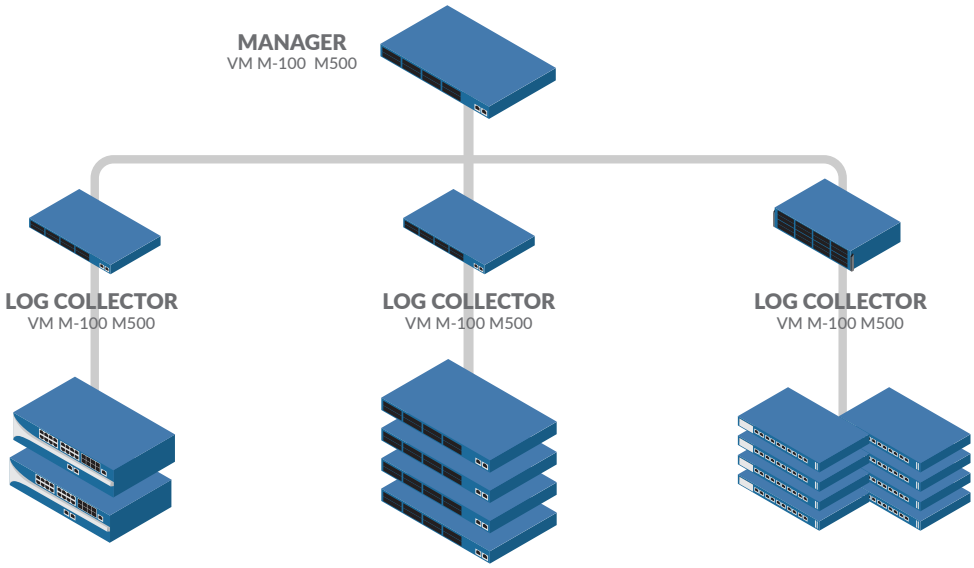

Abbildung 7: Panorama kann auf einer speziellen Appliance oder in gleichmäßiger Verteilung bereitgestellt werden, um die Skalierbarkeit zu maximieren.

der Schnittstelle ist bei der Weboberfläche und bei Panorama identisch, sodass bei einem Wechsel nichts neu erlernt werden muss. Ihre Administratoren können jede der bereitgestellten Schnittstellen nutzen, um jederzeit Änderungen vorzunehmen, ohne sich über Synchronisierungsprobleme Gedanken machen zu müssen. Zusätzlicher Support für standardbasierte Tools wie SNMP und REST-basierte APIs ermöglichen es Ihnen, Managementtools von Dritten zu integrieren.

Berichterstellung und Protokollierung

Die Best Practices im Sicherheitsbereich bedeuten, dass eine Balance zwischen kontinuierlichem Verwaltungsaufwand und Reaktionsfähigkeit gefunden werden muss. Das kann die Ermittlung und Analyse von Sicherheitsvorfällen oder die Generierung von täglichen Berichten beinhalten.

- **Berichterstattung:** Vorgefertigte Berichte können so wie sie sind verwendet, angepasst oder in einem Bericht zusammengefasst werden, um die spezifischen Anforderungen zu erfüllen. Alle Berichte können im CSV- oder PDF-Dateiformat exportiert, nach einem Zeitplan erstellt und per E-Mail verschickt werden.
- **Protokollierung:** Log-Filtering in Echtzeit vereinfacht eine schnelle Untersuchung jeder Sitzung, die Ihr Netzwerk kreuzt. Der vollständige Kontext der Anwendung, der Inhalte (inklusive der von WildFire aufgedeckten Malware) und der Benutzer können als Filterkriterien genutzt und die Ergebnisse können als CSV-Datei exportiert oder – für Offlinearchivierung oder eine zusätzliche Analyse – an einen Syslog-Server gesendet werden. Protokolle, die von Panorama gesammelt wurden, können ebenfalls zu Archivierungszwecken oder für eine zusätzliche Analyse an einen Syslog-Server gesendet werden.
- **Gefahrensuche:** Gefahrenerkennung durch den Service von AutoFocus wird direkt in PAN-OS zur Verfügung gestellt, sodass die Bedrohungsanalyse und die Suchabläufe ohne zusätzliche spezielle Ressourcen beschleunigt werden können. Wird eine weitere Analyse notwendig, können Benutzer zwischen AutoFocus und PAN-OS wechseln und die Suchvorschläge für beide Systeme nutzen.

Zusätzlich zu den Berichterstellungs- und Protokollierungsfunktionen der Palo Alto Networks Next-Generation Security Platform sind Integrationen mit SIEM-Tools von Dritten verfügbar, wie Splunk® für Palo Alto Networks. Diese Tools bieten erweiterte Berichterstellung und Datenvisualisierung und ermöglichen die Herstellung einer Beziehung zwischen Sicherheitsvorfällen in verschiedenen Systemen in Ihrem Unternehmen.

Speziell gefertigte Hardware oder virtualisierte Plattformen

Unsere Next-Generation Firewall ist entweder als speziell angefertigte Hardwareplattform verfügbar, die von der Zweigstelle des Unternehmens bis zu einem Hochgeschwindigkeitsrechenzentrum skalierbar ist, oder als virtualisierter Formfaktor, der Ihre cloudbasierten Datenverarbeitungsinitiativen unterstützt. Wir unterstützen eine große Bandbreite an virtuellen Plattformen, sodass wir Ihr vielfältiges, virtualisiertes Rechenzentrum sowie Anforderungen öffentlicher und privater Clouds abdecken. Die VM-Series Firewall Platform ist verfügbar für VMware® ESXiTM, NSXTM, Citrix® SDXTM, Microsoft Hyper-V®, Amazon® Web Services (AWS), Microsoft Azure™ und KVM-Hypervisor. Wenn Sie Ihre Plattform als Hardware oder virtuellen Formfaktor anwenden, können Sie Panorama für eine zentralisierte Verwaltung nutzen.

4401 Great America Parkway
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 898 9087

www.paloaltonetworks.com