FIREWALL-ÜBERSICHT

Palo Alto Networks-Firewall der nächsten Generation

Aufgrund der signifikanten Veränderung der Anwendungsnutzung und des Benutzerverhaltens sowie der deutlich gestiegenen Komplexität verschachtelter Netzwerkinfrastrukturen ist eine Bedrohungslandschaft entstanden, in der herkömmliche Sicherheitsmaßnahmen für Netzwerke keinen ausreichenden Schutz mehr bieten. Benutzer fordern Zugriff auf immer mehr Anwendungen von unterschiedlichsten Gerätetypen aus und machen sich dabei oft kaum Gedanken bezüglich der damit für das Unternehmen einhergehenden Sicherheitsrisiken. Erweiterungen Ihres Rechenzentrums, Netzwerksegmentierungen, Virtualisierungsmaßnahmen und Mobilitätsinitiativen zwingen Sie dazu, Zugriffsberechtigungen für Anwendungen und Daten zu überdenken. Gleichzeitig müssen Sie Ihr Netzwerk vor neuartigen, raffinierteren Bedrohungen schützen, die herkömmliche Sicherheitsmechanismen umgehen.

Sie hatten bisher die Wahl, entweder jeglichen Zugriff bzw. Datenverkehr zum Schutz des Netzwerks zu blockieren oder im Interesse Ihres Geschäfts alle Aktionen zuzulassen. Dies bot wenig Raum für Kompromisse. Mit der Next-Generation-Sicherheitsplattform von Palo Alto Networks® können Sie Ihren Benutzern den sicheren Zugriff auf erforderliche Anwendungen gewähren und gleichzeitig Cyberbedrohungen abwehren.

Den Kern der Next-Generation-Sicherheitsplattform bildet unsere innovative Firewall, die von Grund auf zum Schutz vor raffiniertesten Bedrohungen entwickelt wurde. Die innovative Firewall untersucht den gesamten Datenverkehr einschließlich Anwendungen, Bedrohungen und Inhalten und ordnet ihn dem jeweiligen Benutzer zu, egal, wo sich dieser gerade befindet oder welchen Gerätetyp er verwendet. Die Anwendung, der Inhalt und der Benutzer – d. h. die für Ihre Betriebsabläufe wesentlichen Ressourcen – werden zu integralen Bestandteilen der Sicherheitsleitlinie Ihres Unternehmens. Folglich können Sie Ihre Sicherheitsmaßnahmen auf Ihre primären Geschäftsinitiativen ausrichten. Unsere Next-Generation-Sicherheitsplattform ermöglicht es Ihnen, die Reaktionszeiten bei Zwischenfällen zu reduzieren, unbekannte Bedrohungen zu erkennen und die Sicherheit Ihres Netzwerks zu optimieren.

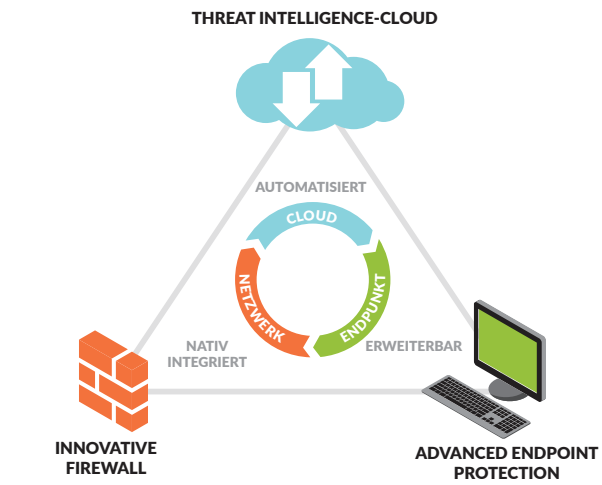

Abbildung 1: Next-Generation-Sicherheitsplattform von Palo Alto Networks

- Lassen Sie Anwendungen, Benutzer und Inhalte sicher zu, indem Sie den gesamten Datenverkehr klassifizieren und Anwendungsfälle festlegen. Weisen Sie außerdem Richtlinien zu, um den Zugriff auf relevante Anwendungen einschließlich SaaS-Anwendungen (Software-as-a-Service) zuzulassen und zu schützen.
- Wehren Sie Bedrohungen ab, indem Sie unerwünschte Anwendungen eliminieren und dadurch Ihre Angriffsoberfläche reduzieren. Sie können durch gezielte Sicherheitsleitlinien bekannte Exploits von Sicherheitslücken, Viren, Spyware, Botnets sowie unbekannte Malware (APTs) blockieren.
- Schützen Sie Ihre Rechenzentren, indem Sie Anwendungen validieren, Daten isolieren, schädliche Anwendungen kontrollieren und Bedrohungen im Handumdrehen abwehren.
- Sichern Sie öffentliche und private Cloud-Computing-Umgebungen durch erhöhte Transparenz und Kontrolle. Stellen Sie parallel zu Ihren virtuellen Maschinen Sicherheitsleitlinien bereit und sorgen Sie dafür, dass diese durchgesetzt und aufrechterhalten werden.
- Erweitern Sie die Next-Generation-Sicherheitsplattform auf Benutzer und Geräte außerhalb der Netzwerkparameter, um eine sichere Mobile Computing-Umgebung zu erhalten.

- Optimieren Sie das Geräte-, Netzwerk- und Richtlinienmanagement entsprechend Ihrer Organisationsstruktur durch intuitive Verwaltungsfunktionen.

Die Next-Generation-Sicherheitsplattform erleichtert es Ihrem Unternehmen, auf einheitliche Weise ein breites Spektrum an Sicherheitsanforderungen zu erfüllen. Dank der ausgewogenen Kombination von Netzwerksicherheit, globaler Threat Intelligence und Endpunktschutz kann Ihr Unternehmen Geschäftsinitiativen fördern und gleichzeitig den allgemeinen Sicherheitsstatus erhöhen, während Sie die Reaktionszeiten bei Sicherheitsvorfällen reduzieren.

Schutz zur Förderung Ihres Unternehmens

Schützen Sie Ihr Unternehmen mit unserer Next-Generation-Sicherheitsplattform, indem Sie Richtlinien zu Anwendungen, Benutzern und Inhalten bereitstellen und durchsetzen. Dank des einzigartigen positiven Kontrollmodells unserer Plattform können Sie gezielt bestimmte Anwendungen und Funktionen zulassen, während Sie alles andere blockieren (implizit oder explizit). Die innovative Firewall untersucht in einem Durchgang (Single-Pass-Architektur) den gesamten Datenverkehr an allen Ports. Anwendungen, zugehörige Inhalte und Benutzeridentitäten erhalten dadurch einen vollständigen Kontext, sodass Sie hinsichtlich der Sicherheitsleitlinien fundierte Entscheidungen treffen können.

- Klassifizieren Sie den gesamten Datenverkehr permanent an allen Ports. Angreifer können portbasierte Firewalls mittlerweile durch entsprechende Anwendungen und die damit verbundenen Inhalte mit unterschiedlichen Methoden umgehen. Unsere Next-Generation-Sicherheitsplattform klassifiziert den Datenverkehrsstrom mit mehreren nativen Mechanismen, um zwischen Anwendungen, Bedrohungen und Malware zu unterscheiden. Dabei wird unabhängig vom Port, von der Verschlüsselung (SSL oder SSH) oder den genutzten Umgehungsmethoden der gesamte Datenverkehr klassifiziert. Nicht identifizierte Anwendungen, die in der Regel nur einen kleinen Prozentsatz des Datenverkehrs ausmachen, jedoch ein hohes Gefahrenpotenzial bergen, werden automatisch einer systematischen Untersuchung unterzogen.

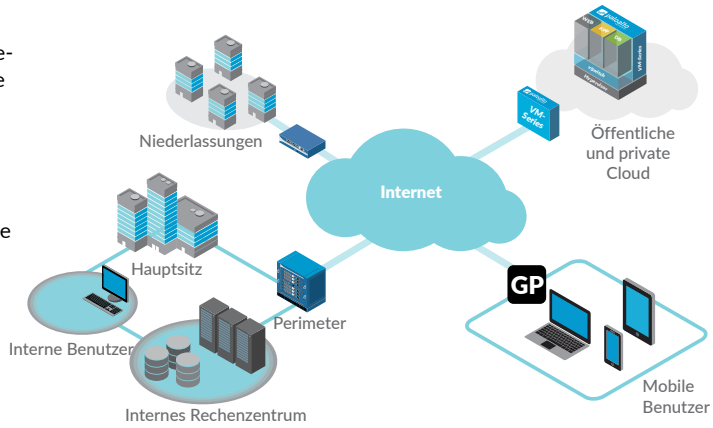

Abbildung 1: Sichere Aktivierungsrichtlinien im gesamten Unternehmen implementieren

- Reduzieren Sie die Angriffsoberfläche und verhindern Sie Cyberattacken. Nachdem der Datenverkehr vollständig klassifiziert wurde, können Sie die Angriffsoberfläche Ihres Netzwerks reduzieren, indem Sie nur bestimmte Anwendungen zulassen und alle anderen ablehnen. Blockieren Sie durch koordinierte Schutzmaßnahmen gegen Cyberattacken bekannte Malware-Sites und wehren Sie Exploits von Sicherheitslücken, Viren, Spyware und schädliche DNS-Anfragen ab. Jegliche gezielte oder unbekannte Malware wird durch Ausführen der unbekannten Dateien analysiert und identifiziert. Schädliche Funktionsweisen werden zudem in einer virtualisierten Sandbox-Umgebung direkt überwacht. Bei neu erkannter Malware wird automatisch eine Signatur für die infizierte Datei und den zugehörigen Malware-Datenverkehr erstellt und an Sie übermittelt.
- Ordnen Sie Benutzern und Geräten Anwendungsdatenverkehr und damit verbundene Bedrohungen zu. Um Ihren Sicherheitsstatus zu erhöhen und die Reaktionszeit bei Zwischenfällen zu reduzieren, ist es wichtig, die genutzten Anwendungen dem jeweiligen Benutzer und Gerätetyp

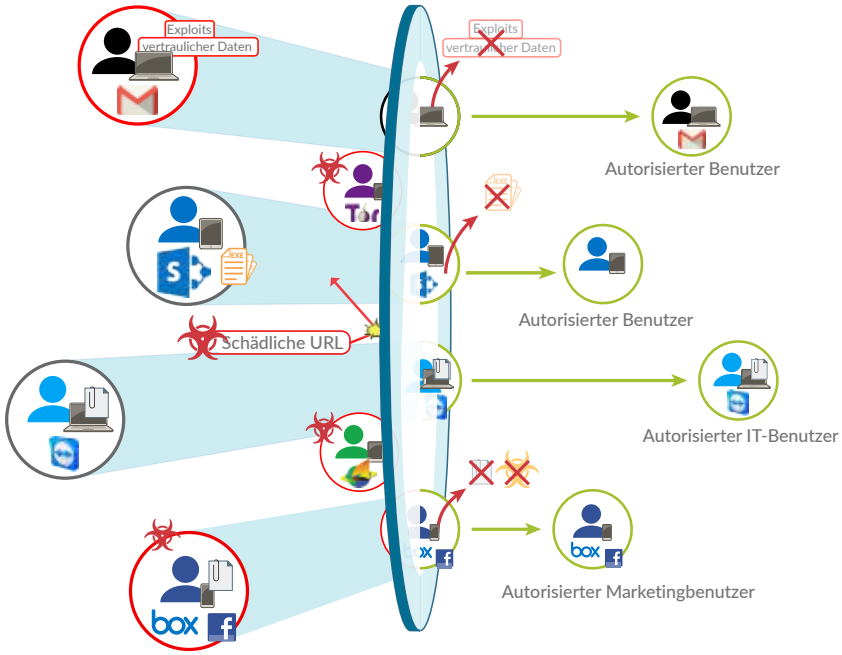

Abbildung 2: Anwendungen, Inhalte, Benutzer und Geräte – alles unter Ihrer Kontrolle

Abbildung 3: Die Firewall zeigt die Aktivitäten im Zusammenhang mit Anwendungen in einem klaren und leicht zu interpretierenden Format an. Sie können Filter hinzufügen und entfernen, um weitere Informationen über die Anwendung, ihre Funktionen und ihre Benutzer zu erhalten.

zuzuordnen. Dieser Kontext ist erforderlich, damit Ihre Sicherheitsleitlinien greifen. Durch die Integration von verschiedenen internen Benutzer-Repositorys lässt sich die Identität der Benutzer und Geräte ermitteln, die über Microsoft Windows®, Mac® OS X, Linux®, Android® oder iOS auf eine Anwendung zugreifen. Durch die Kombination aus Transparenz und Kontrolle über Benutzer und Geräte können Sie die Nutzung jeglicher Anwendungen, die Ihr Netzwerk durchlaufen, ungeachtet des Benutzerstandorts oder des Gerätetyps sicher zulassen.

Indem Sie den Kontext einer genutzten Anwendung sowie die möglicherweise darin enthaltenen Inhalte oder Bedrohungen und den ausführenden Benutzer oder das Gerät ermitteln, können Sie das Richtlinienmanagement optimieren, Ihren Sicherheitsstatus verbessern und Untersuchungen infolge von Zwischenfällen beschleunigen.

Strengere Sicherheitsrichtlinien durch umfassenden Kontext

Bei den Sicherheitsverfahren hat es sich gezeigt, dass Ihre Entscheidungen bezüglich Richtlinien, Ihre Fähigkeiten zur Berichterstattung von Netzwerkaktivitäten und Ihre forensischen Möglichkeiten vom Kontext abhängen. Der Kontext der genutzten Anwendung, die besuchte Website, die damit verbundene Nutzlast sowie der Benutzer sind allesamt wertvolle Informationen für den Schutz Ihres Netzwerks. Wenn Sie genau wissen, welche Anwendungen Ihre Internetgateways passieren, innerhalb Ihres Rechenzentrums oder Ihrer Cloud-Umgebung ausgeführt oder von Remote-Benutzern verwendet werden, können Sie auf diese Anwendungen spezielle Richtlinien sowie damit koordinierte Abwehrmaßnahmen gegen Bedrohungen anwenden. Indem Sie nicht nur die IP-Adresse, sondern auch den Benutzer kennen, erweitern Sie den Kontext und können Richtlinien noch genauer zuweisen.

Eine umfassende Reihe hoch interaktiver Visualisierungs- und Protokollfilterungstools liefern den Kontext zur Anwendungsaktivität, dem damit verbundenen Inhalt oder der Bedrohung, dem Benutzer sowie dem Gerätetyp. Jeder dieser Datenpunkte stellt einen Ausschnitt Ihres Netzwerks dar. Im Gesamtkontext betrachtet erhalten Sie jedoch einen vollständigen Überblick über das potenzielle Sicherheitsrisiko und können besser informierte Richtlinienentscheidungen treffen. Der gesamte Datenverkehr wird permanent klassifiziert. Jegliche Zustandsänderungen werden zur Analyse protokolliert. Die Aktualisierung der grafischen Zusammenfassungen der Informationen, die Sie auf einer benutzerfreundlichen, webbasierten Oberfläche anzeigen können, erfolgt automatisch.

- Sie können am Internetgateway neue und unbekannte Anwendungen untersuchen, um schnell eine Beschreibung der Anwendung, ihrer Verhaltensmerkmale und des Benutzers zu erhalten. Durch die zusätzliche Transparenz hinsichtlich der URL-Kategorien, Bedrohungen und Datenmuster erhalten Sie ein besser abgerundetes Bild des Netzwerkdatenverkehrs, der das Gateway passiert.
- Alle Dateien, die WildFire™ auf unbekannte Malware analysiert, werden intern mit vollständigen Zugriffsdetails wie etwa der genutzten Anwendung, dem Benutzer, Dateityp, Zielbetriebssystem sowie schädlichen Funktionsweisen protokolliert.
- Prüfen Sie alle innerhalb des Rechenzentrums genutzten Anwendungen, und stellen Sie sicher, dass diese nur von autorisierten Benutzern verwendet werden. Durch die erhöhte Transparenz der Aktivitäten im Rechenzentrum können Sie gewährleisten, dass keine falsch konfigurierten Anwendungen ausgeführt oder SSH bzw. RDP auf schädliche Weise genutzt werden.
- Die Bedrohungsanalyse, forensische Untersuchungen und die Erkennung werden durch den Threat Intelligence-Service AutoFocus™ beschleunigt. Sie erhalten dadurch eindeutige kontextbezogene Bedrohungsdaten vom Gerät direkt in PAN-OS®.
- Setzen Sie in öffentlichen und privaten Cloud-Umgebungen mit der Next-Generation-Sicherheitsplattform Richtlinien durch, und schützen Sie Ihre Anwendungen. Gleichzeitig können Sie virtuelle Server nach Bedarf erstellen und zuordnen.
- Unbekannte Anwendungen, die in der Regel einen kleinen Prozentsatz in jedem Netzwerk ausmachen, können in allen Bereitstellungsszenarien zu Analysezwecken und zur systematischen Verwaltung kategorisiert werden.

Häufig ist gar nicht vollständig bekannt, wer welche Anwendungen in welchem Umfang nutzt. Die vollständige Transparenz der geschäftsrelevanten Aspekte Ihres Netzwerkdatenverkehrs – der Anwendung, des Inhalts und des Benutzers – ist der erste Schritt hin zu einer verstärkt informierten Richtliniensteuerung.

Abbildung 4: Der einheitliche Richtlinien-Editor ermöglicht die schnelle Entwicklung und Implementierung von Richtlinien zur Steuerung von Anwendungen, Benutzern und Inhalten.

Reduzierung des Risikos durch gezieltes Zulassen von Anwendungen

Die herkömmliche Risikoreduzierung bestand bislang darin, den Zugriff auf Netzwerkdienste einzuschränken, was jedoch mitunter zur Behinderung von Betriebsabläufen führt. Heute werden Anwendungen zur Risikoreduzierung sicher zugelassen. Hierfür dient ein geschäftsorientierter Ansatz, der ein ausgewogenes Verhältnis zwischen den beiden bisherigen Strategien schafft, entweder nichts oder alles zuzulassen.

- Begrenzen Sie Webmail und Instant Messaging durch Anwendungsgruppen und SSL-Entschlüsselung auf bestimmte Anwendungsvarianten. Untersuchen Sie diese auf jegliche Bedrohungen, und laden Sie unbekannte verdächtige Dateien (EXE-, DLL- und ZIP-Dateien, PDF-Dokumente, Office-Dokumente, Java® und Android® APK) zur Analyse und Signaturentwicklung in WildFire hoch.
- Steuern Sie die Internetnutzung aller Benutzer, indem Sie Datenverkehr zu geschäftlich genutzte Websites zulassen und überprüfen. Blockieren Sie gleichzeitig den Zugriff auf offensichtlich für private Zwecke genutzte Websites und „coachen" Sie den Zugriff auf fragwürdige Websites über benutzerdefinierte Sperrseiten.
- Blockieren Sie mit dynamischen Anwendungsfiltern explizit jegliche Peer-zu-Peer-Dateiübertragungsanwendungen für alle Benutzer.
- Gewinnen Sie einen ausführlichen Überblick über die Nutzung von SaaS-Anwendungen innerhalb Ihres Unternehmens. Richten Sie für jede Anwendung detaillierte Zugriffs- und Nutzungssteuerungen ein und verhindern Sie die Bereitstellung von Malware durch diese Anwendungen.
- Beziehen Sie mobile Geräte ein, indem Sie die Richtlinien für Ihre Internetgateways sowie Ihre Abwehrfunktionen gegen Bedrohungen mit dem mobilen Sicherheitsservice GlobalProtect™ auf Remote-Benutzer ausdehnen.

Stellen Sie innerhalb des Rechenzentrums anhand des Kontexts sicher, dass die darin ausgeführten Anwendungen über ihre Standardports genutzt werden. Sie haben die Möglichkeit, schädliche Anwendungen zu ermitteln, Benutzer zu validieren, Daten zu isolieren und geschäftskritische Daten vor Bedrohungen zu schützen. Sie haben unter anderem folgende Möglichkeiten:

- Isolieren Sie mithilfe von Sicherheitszonen das auf Oracle® basierende Repository für Kreditkartennummern. Erzwingen Sie, dass der Oracle-Datenverkehr seine Standardports durchläuft, während Sie den Datenverkehr auf eingehende Bedrohungen untersuchen und nur der Finanzgruppe Zugriff erteilen.
- Erstellen Sie nur für die IT-Abteilung eine Remote-Management-Anwendungsgruppe (z. B. SSH, RDP oder Telnet) zur Nutzung innerhalb des Rechenzentrums.
- Automatisieren Sie innerhalb Ihres virtuellen Rechenzentrums mithilfe von dynamischen Objekten die Erstellung von Sicherheitsleitlinien für virtuelle SharePoint®-Rechner, die eingerichtet oder außer Betrieb genommen werden oder Ihre virtuelle Umgebung passieren.

Schutz von zugelassenen Anwendungen und Inhalten

Wenn Sie Richtlinien zur Abwehr von Bedrohungen sowie zur Inhaltsanalyse anwenden, werden der Kontext der Anwendung und des Benutzers zu integralen Bestandteilen Ihrer Sicherheitsleitlinie. Durch den vollständigen Kontext innerhalb Ihrer Richtlinien zur Abwehr von Bedrohungen werden Umgehungstaktiken wie Port-Hopping und Tunneling-Techniken neutralisiert. Reduzieren Sie die Angriffsoberfläche für Bedrohungen, indem Sie eine ausgewählte Reihe von Anwendungen zulassen und auf den damit verbundenen Datenverkehr Richtlinien zur Abwehr von Bedrohungen sowie zur Inhaltsanalyse anwenden.

Zur Abwehr von Bedrohungen sowie zur Inhaltsanalyse stehen Ihnen in Ihren Richtlinien die folgenden Elemente zur Verfügung:

- **Wehren Sie bekannte Bedrohungen im Netzwerk durch IPS und Antivirensoftware/Anti-Spyware ab.** Der Schutz vor einer Reihe von bekannten Bedrohungen wird durch die Untersuchung in einem Durchgang (Single Pass) mit einem einheitlichen Signaturformat und einer Stream-basierten Scanning-Engine erzielt. Intrusion Prevention System (IPS)-Funktionen erkennen Sicherheitslücken in der Netzwerk- und Anwendungsschicht, vermeiden Pufferüberläufe und Denial-of-Service-Attacken und hindern Port-Scans daran, die Datenressourcen des Unternehmens zu gefährden und zu beschädigen. Antivirensoftware/Anti-Spyware-Schutz blockiert Millionen von Malware-Varianten einschließlich derer, die in komprimierten Dateien oder Webdatenverkehr (komprimiertem HTTP/HTTPS) verborgen sind, sowie bekannte PDF-Viren. Für den mit SSL verschlüsselten Datenverkehr können Sie selektiv eine richtlinienbasierte Entschlüsselung anwenden und den Datenverkehr anschließend ungeachtet des Ports auf Bedrohungen untersuchen.
- **Blockieren Sie unbekannte oder gezielte Malware-Angriffe mit WildFire.** WildFire kann in Dateien verborgene unbekannte oder gezielte Malware, wie etwa Advanced Persistent Threats (fortgeschrittene, andauernde Bedrohungen, APTs)

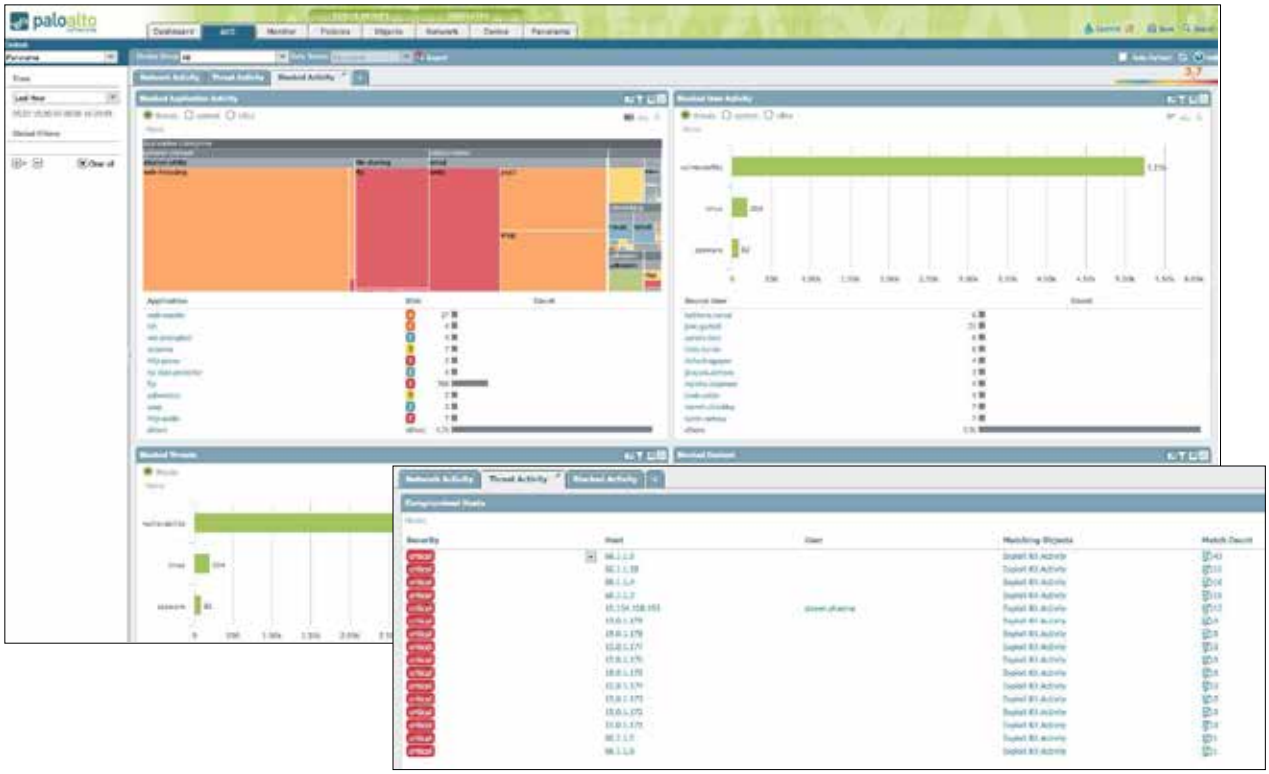

Abbildung 5: Transparente Inhalte und Bedrohungen – Zeigen Sie URL-, Bedrohungs- und Datei-/Datenübertragungsaktivitäten sowie beschädigte Hosts in einem einfachen, übersichtlichen und umfangreich anpassbaren Format an. Sie können Filter hinzu oder entfernen, um weitere Informationen zu einzelnen Elementen zu erhalten.

in unterschiedlichen Betriebssystemen und Anwendungsversionen erkennen. Unbekannte Dateien werden dabei direkt beobachtet und in einer virtuellen Sandbox-Umgebung in der Cloud oder der WF-500-Anwendung ausgeführt. WildFire überwacht mehr als 420 schädliche Funktionsweisen und entwickelt für erkannte Malware automatische eine Signatur. Von der Erkennung bis zur Bereitstellung der Signatur vergehen dabei gerade einmal 5 Minuten. WildFire unterstützt alle gängigen Dateitypen wie: PE-Dateien, Microsoft Office-Dateien (DOC, XLS und PPT), PDFs, Java Applet-Dateien (JAR und CLASS) sowie Android Application Package-Dateien (APK). Zudem analysiert WildFire Links in E-Mails, um Spear Phishing-Angriffe zu unterbinden.

- **Identifizieren Sie Bot-infizierte Hosts und durch Malware ausgelöste Netzwerkaktivitäten.** Indem Sie sämtliche Anwendungen sowie unbekannten Datenverkehr auf allen Ports vollständig und kontextbezogen klassifizieren, können Sie Anomalien in Ihrem Netzwerk bzw. potenzielle Bedrohungen aufdecken. Command-and-Control-App-ID™, verhaltensabhängige Botnet-Berichte, DNS-Sinkholing und die passive DNS-Überwachung ermöglichen es Ihnen, unbekannten Datenverkehr sowie verdächtige DNS- und URL-Anfragen schnell zu korrelieren. DNS-Anfragen an schädliche Domains können Sie durch die Anwendung globaler Threat Intelligence abfangen und umleiten (Sinkholing).
- **Beschränken Sie unzulässige Datei- und Datenübertragungen.** Die Datenfilterung gestattet Administratoren, Richtlinien zu implementieren, die die Risiken bei unerlaubten Datei- und Datenübertragungen minimieren. Dateiübertragungen lassen sich steuern, indem die einzelnen Dateien (und nicht nur die Dateinamenerweiterungen) überprüft werden, um festzustellen, ob der Transfer zugelassen werden sollte. Sie können ausführbare Dateien, die typischerweise in Drive-by-Downloads vorkommen, blockieren, um Ihr Netzwerk vor der Ausbreitung von nicht erkannter Malware zu schützen. Datenfilterfunktionen können die Übertragung vertraulicher Daten (Kreditkarten- und Sozialversicherungsnummern sowie benutzerdefinierte Muster) erkennen und steuern.
- **Steuern Sie die Internetnutzung.** Eine vollständig integrierte, anpassbare Engine für die URL-Filterung ermöglicht es Ihren Administratoren, detaillierte Richtlinien für das Surfen im Internet zu erstellen, die Anwendungstransparenz zu erhöhen, Richtlinien durchzusetzen und das Unternehmen vor einer ganzen Palette an rechtlich kritischen und der Produktivität abträglichen Risiken zu schützen.
- **Führen Sie eine gerätebasierte Richtlinie für den Anwendungszugriff ein.** GlobalProtect bietet Ihnen die Möglichkeit, spezielle Richtlinien festzulegen um zu steuern, welche Geräte auf bestimmte Anwendungen und Netzwerkressourcen Zugriff haben. Stellen Sie beispielsweise sicher, dass Notebooks den Unternehmensanforderungen entsprechen, bevor Sie diesen den Zugriff auf das Rechenzentrum gewähren. Prüfen Sie bei mobilen Geräten, ob sich diese auf dem aktuellen Stand befinden, zum Unternehmensinventar gehören und vollständig gepatcht sind, bevor damit auf vertrauliche Daten zugegriffen wird.
- **Ermitteln Sie beschädigte Hosts automatisch.** Eine automatisierte Korrelations-Engine überprüft das gesamte Netzwerk auf vorgegebene Gefährdungsindikatoren, korreliert Übereinstimmungen und hebt beschädigte Hosts automatisch hervor, wodurch das manuelle Daten-Mining reduziert werden kann.

Netzwerksicherheitsmanagement

Die Next-Generation-Sicherheitsplattform kann individuell über eine Command Line Interface (Kommandozeilenschnittstelle, CLI) oder eine voll funktionsfähige browserbasierte Schnittstelle verwaltet werden. Bei umfangreichen Bereitstellungen bietet

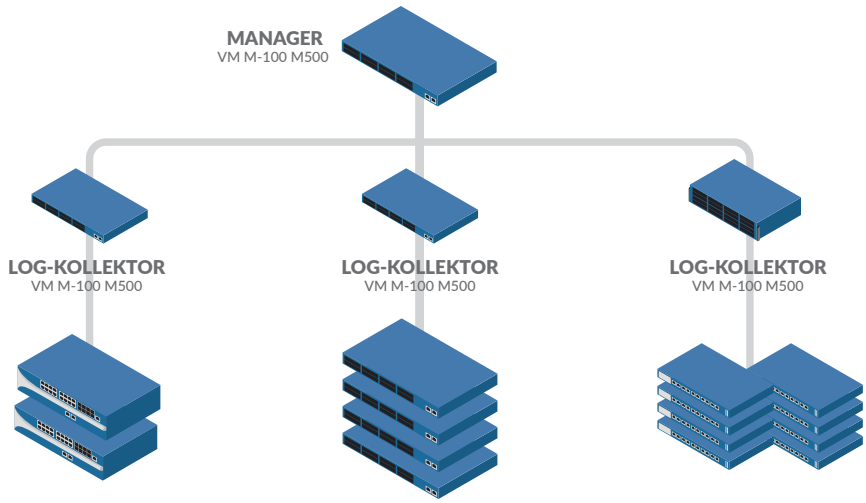

Abbildung 6: Panorama kann auf einer dedizierten Appliance oder auf mehrere verteilt bereitgestellt werden, um die Skalierbarkeit zu maximieren.

Panorama™ globale Transparenz-, Richtlinienbearbeitungs-, Reporting- und Protokollierungsfunktionen für Ihre gesamte Hardware und alle Firewalls Ihrer virtuellen Appliances. Mit Panorama erhalten Sie dasselbe Maß an kontextbezogener Kontrolle über Ihre globalen Bereitstellungen wie über eine einzelne Appliance.

Schaffen Sie dank der rollenbasierten Verwaltung in Verbindung mit Pre- und Post-Rules ein ausgewogenes Verhältnis zwischen zentralisierter Steuerung, lokaler Richtlinienbearbeitung und flexibler Gerätekonfiguration. Es macht keinen Unterschied, ob Sie die Weboberfläche des Geräts oder von Panorama verwenden. Das Aussehen und Verhalten der Oberfläche ist identisch, damit beim Wechsel keine Lernkurve entsteht. Ihre Administratoren können jederzeit über jede der Oberflächen Änderungen vornehmen, ohne sich über die Synchronisierung Gedanken machen zu müssen. Durch die zusätzliche Unterstützung für normenbasierte Tools wie SNMP und REST-basierte APIs ist eine Integration in Verwaltungs-Tools von Drittanbietern möglich.

Reporting und Protokollierung

Laut den Best Practices bezüglich Sicherheitsverfahren sollte ein ausgewogenes Verhältnis zwischen laufenden Verwaltungsmaßnahmen und Reaktivität herrschen. Dies kann die Untersuchung und Analyse von Sicherheitsvorfällen oder das Generieren der täglichen Berichte beinhalten.

- **Reporting:** Vordefinierte Berichte können im Ist-Zustand verwendet, angepasst oder miteinander zu einem Report gruppiert werden, um den spezifischen Anforderungen zu entsprechen. Alle Berichte können ins CSV- oder PDF-Format exportiert und nach Zeitplan ausgeführt und per E-Mail versendet werden.
- **Protokollierung:** Protokollfilterung in Echtzeit ermöglicht eine schnelle forensische Untersuchung jeder Sitzung im Netzwerk. Als Filterkriterien können der vollständige Kontext der Anwendung, der Inhalt (einschließlich von WildFire erkannte Malware) und der Benutzer verwendet werden. Die Ergebnisse lassen sich zur Offline-Archivierung oder weiteren Analyse in eine CSV-Datei exportieren oder an einen Syslog-Server senden. Von Panorama zusammengefasste Protokolle können Sie ebenfalls zur weiteren Analyse oder zu Archivierungszwecken an einen Syslog-Server senden.
- **Bedrohungserkennung:** Die Threat Intelligence des AutoFocus-Service ist direkt in PAN-OS zugänglich. Dies beschleunigt die Bedrohungsanalyse und die Erkennung, ohne dass spezielle zusätzliche Ressourcen erforderlich sind. Werden weitere Analysen benötigt, haben Benutzer die Möglichkeit, mit vorab ausgefüllten Suchanfragen zwischen AutoFocus und PAN-OS zu wechseln.

Neben den Reporting- und Protokollierungsfunktionen der Next-Generation-Sicherheitsplattform von Palo Alto Networks können Sie auch SIEM-Tools von Drittanbietern wie etwa Splunk® für Palo Alto Networks integrieren. Diese Tools bieten weitere Reporting- und Datenvisualisierungsfunktionen und ermöglichen die Korrelation von Sicherheitsvorfällen in unterschiedlichen Systemen Ihres Unternehmens.

Spezielle Hardware- oder virtualisierte Plattformen

Unsere innovative Firewall ist als speziell entwickelte Hardwareplattform erhältlich, die von einer Zweigniederlassung des Unternehmens bis hin zu einem Hochgeschwindigkeits-Rechenzentrum oder als virtualisierter Formfaktor skaliert werden kann. Dies ermöglicht die Umsetzung Ihrer cloudbasierten Computing-Initiativen. Wir unterstützen die umfangreichste Reihe an virtuellen Plattformen, um die unterschiedlichen Anforderungen Ihres virtualisierten Rechenzentrums und Ihrer öffentlichen und privaten Cloud zu erfüllen. Die VM-Series-Firewallplattform ist für VMware® ESXi™, NSX™, Citrix® SDX™, Microsoft Hyper-V®, Amazon® Web Services (AWS), Microsoft Azure™ und KVM-Hypervisoren verfügbar. Wenn Sie unsere Plattform auf Hardware oder als virtuellen Formfaktoren bereitstellen, können Sie für das zentrale Management Panorama nutzen.

4401 Great America Parkway
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/320/4788
Support: +1/866/89 89 087

www.paloaltonetworks.com

pan-next-generation-firewall-overview-ds-050616