DTS
Next-Generation Firewall

Next-Generation Firewall

Wie, wann und wo werden Anwendungen genutzt? Wie verändert sich das Benutzerverhalten im Zuge der Digitalisierung? Wie komplex und unübersichtlich sind Netzwerkinfrastrukturen? Diese Fragen sind immens wichtig bei der Ausgestaltung Ihrer Cyber Security. Die Antworten offenbaren häufig wesentliche Schwächen. Angreifer können diese Schwächen sowie die traditionelle, portbasierte Netzwerksicherheit problemlos ausnutzen bzw. umgehen. Es gilt den Zugriff auf sensible Anwendungen und Daten über Ihr Netzwerk so zu gestalten, dass die Antworten auf diese Fragen immer einen Schutz gegen die neueste Generation hochentwickelter Gefahren beinhaltet. Der effektivste Schutz beginnt mit einer modernen Firewall, welche eine auf Prävention ausgerichtete, intelligente Architektur unterstützt. Die führende Palo Alto Networks Next-Generation Firewall ist seit 15 Jahren Leader auf diesem Gebiet und setzt konstant neue Maßstäbe.

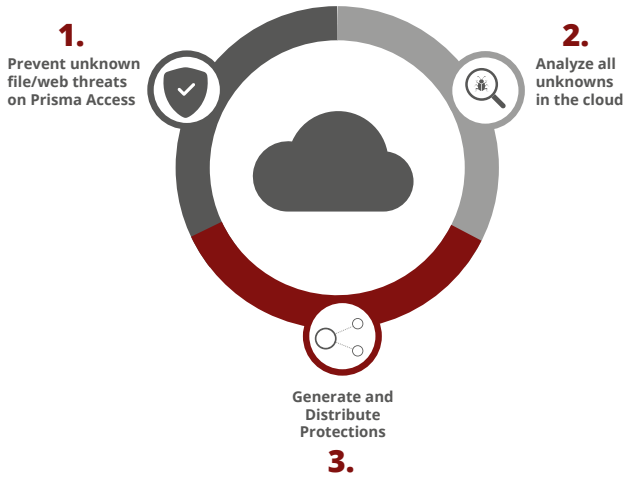
- Permanente Überwachung des gesamten Datenverkehrs, inkl. richtlinienbasierte Datenverkehrsformung & Kontextklassifizierung
- Granulare Sicherheitskontrolle & richtlinienbasierte Sicherheitssteuerung
- Datei- & Datenfilterung, Netzwerksegmentierung & Zonensicherheit
- Prävention von u. a. Malware, Zero-Day-Malware, Exploits, Phishing-Links & -Websites, bösartigen Domains, Command-and-Control, Datendiebstahl durch DNS-Tunneling usw.
- Integrierte Lösung mit der Palo Alto Networks Sicherheitsplattform, inkl. Zusammenspiel mit zahlreichen weiteren Security-Modulen
- Integration in die ganzheitliche DTS Cyber Security, inkl. Schutz vor unbekannten Gefahren durch DTS German WildFire Cloud
- DTS Managed Services

Schätzungen zur Folge wird die Anzahl der mit dem Internet verbundenen Geräte im Jahr 2025 bei 41,6 Milliarden liegen. Unternehmensdaten werden auf immer mehr Systeme und teilweise sehr komplexe Infrastrukturen verteilt. Dies erhöht die Angriffsfläche. Die einzig wirkliche Lösung ist eine integrierte Lösung. Sie muss sowohl vorbeugend agieren, als auch Angriffe aktiv verhindern sowie die Sicherheitsinfrastruktur vereinfachen, egal wo sich Benutzer, Anwendungen und Daten befinden. Die Next-Generation Firewall von Palo Alto Networks basiert auf innovativen Funktionalitäten und optimiert durch Automatisierungs- und Analyse-Tools Ihre Sicherheitsprozesse – konsistenter Schutz dank lückenloser Überwachung.

Die Next-Generation Firewall führt permanent eine vollständige Stack- und Single-Pass-Überprüfung Ihres gesamten Datenverkehrs durch. Dies geschieht unabhängig von Port, Verschlüsselung oder Ausweichmethoden. Dadurch kann für jede Anwendung, jede Aktivität, jeden Inhalt und jeden Benutzer der gesamte Kontext berücksichtigt werden. Die Kontextklassifizierung entsteht durch eine große Bandbreite an interaktiven Visualisierungs- und Logfiltertools. Die anschließende Bedrohungsanalyse, Forensik und Verfolgung erkennt Bedrohungen zuverlässig und es entsteht eine wesentliche Basis für konkrete Sicherheitsmechanismen – Machine Learning als großer Vorteil.

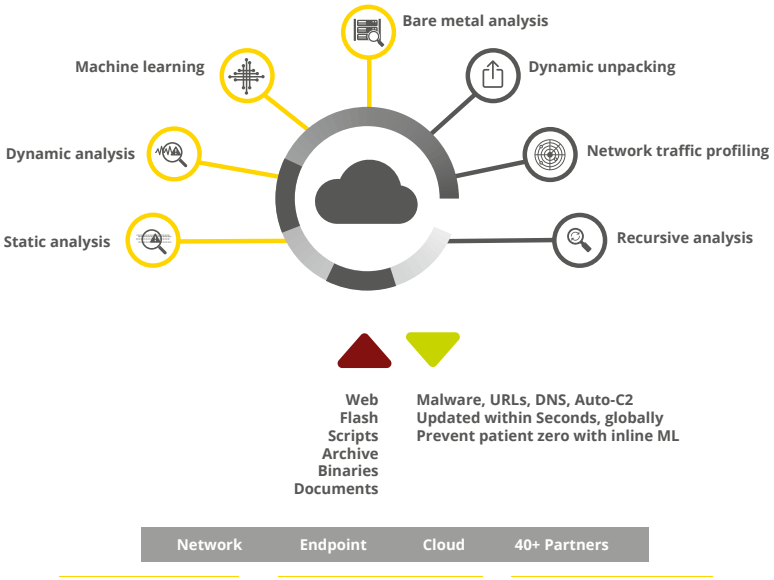
Beispielsweise können Sie Anwendungen zulassen bzw. blockieren oder die Anwendungsnutzung einzelnen Benutzern und Gerätetypen zuordnen. Nicht autorisierte Datentransfers werden beschränkt. Bekannte Malware, Exploits, Viren, Spyware und schädliche DNS-Anfragen können durch die Nutzung vom Intrusion Prevention System (IPS) und Antivirensoftware/ Antispyware abgewehrt werden. Botinfizierte Hosts und aktive Netzwerkaktivitäten von Malware werden anhand von Anomalien aufgespürt. Mit Hilfe der konfigurierbaren URL-Filterfunktion kann das Surfen im Internet kontrolliert werden.

Mit der German WildFire Cloud gehen Sie zudem einen Schritt weiter. Infizierte Dateien werden hier in einer virtuellen Sandbox ausgeführt und auf ihr schädliches Verhalten hin beobachtet. Auf diese Weise spürt WildFire unbekannte Malware, Zero-Day-Malware und Exploits auf. Wenn neuartige Bedrohungen entdeckt wurden, bekommt die infizierende Datei automatisch eine Signatur, welche in nur 5 Min. jedem der mit dem Dienst verbunden ist, bereitgestellt wird. Diese Informationen dienen dem vollständigen Schutz von Netzwerken, Endpunkten und Clouds.



Selbstverständlich ist es möglich spezifische Berichte zu erstellen und zu exportieren. Ebenso können Protokollierungen, z. B. vom Log-Filtering in Echtzeit oder dem vollständigen Kontext bestimmter Anwendungen, Inhalte (inkl. der von WildFire aufgedeckten Malware) und Benutzer gesammelt, versendet oder archiviert werden. Die globale Sichtbarkeit, Strategiebearbeitung, rollenbasierte Administration sowie Berichterstellung und Protokollierung wird über ein zentrales Netzwerksicherheitsmanagement für Ihre Hardware- oder Virtual-Appliance-Firewalls bereitgestellt.

Um beim Zusammenspiel aller Komponenten, gerade im Hinblick auf die gesamte Sicherheitsplattform von Palo Alto Networks, keine komplexe Infrastruktur zu schaffen, die möglicherweise sogar neue Schwachstellen enthält, sind die innovativen Sicherheitstechnologien nativ integriert. Die Features sind nicht nur in ihrem Zusammenspiel zur Cyber Security bahnbrechend, sondern auch in Bezug auf den reduzierten, manuellen Arbeitsaufwand. Die gesamte Plattform aktualisiert sich kontinuierlich und automatisch.



Security Subscriptions bzw. Module:

- Threat Prevention:
  - Blockieren von Exploits, Malware und Command-and-Control-Kommunikation mit nur einem Scan
  - Legitime Netzwerkverkehr wird nur minimal beeinträchtigt
  - Inhaltsbasierte Signaturen werden automatisch aktualisiert
  - Mehrschichtige Sicherheitsinfrastruktur gemäß Zero-Trust-Modell
- URL Filtering
  - Angriffe, bei denen das Internet als Angriffsvektor missbraucht wird, werden automatisch blockiert (z. B. per E-Mail verschickte URLs zu schädlichen Websites, Phishing, Malware, Exploits usw. sowie HTTP-basierte Angriffe)
  - Umsetzung von Richtlinien, um ganzes Unternehmen vor komplettem Spektrum an Geschäftsrisiken zu schützen (inakzeptable Nutzung, Sicherheits- und Compliance-Verstöße, rechtliche Schwierigkeiten)

WildFire

- Erkennen und Blockieren von noch unbekannten Bedrohungen
  - Kombination aus statischen und dynamischen Analysen mit innovativen maschinellen Lernverfahren und neuartiger Umgebung
  - Mehrgleisige Ansatz erkennt Zero-Day-Exploits und Malware
  - Grundlage für neue Schutzmaßnahmen in allen Phasen des Angriffsverlaufs
  - Aktualisierung sämtlicher Sicherheitstechnologien in der Infrastruktur
- DNS Security
  - Vorausschauende Analysen, DNS-basierte Command-and-Control-Kommunikation oder Datendiebstahl zu verhindern
- SD-WAN
  - Sicheres, zuverlässiges, „software defined“ WAN sorgt für sicheren Zugriff auf Cloud-Anwendungen von Zweig- oder Verkaufsstellen
- GlobalProtect
  - Schutz der mobilen Benutzer vor im Angriffsdatenverkehr versteckten Bedrohungen, Phishing, Diebstahl von Anmeldedaten usw.
- Zentrales Management
  - Appliance, VM/CN-Series, Prisma Access, Private, Public oder Hybrid Cloud: Das zentrale Management hilft dabei, die Security Policy einfach und übersichtlich zu verwalten
  - Eine Oberfläche für Konfiguration und Reporting sowie für ganzheitlichen Blick auf Netzwerk-Infrastruktur