Intrusion Prevention mit Forcepoint Next-Generation Firewall

Forcepoint bietet das branchenweit sicherste Intrusion Prevention System (IPS) zum Schutz von verteilten Unternehmensnetzwerken einschließlich Rechenzentren, Büros, Niederlassungen und der Cloud.

Die Netzwerksicherheitslösungen von Forcepoint bieten eines der branchenweit sichersten Intrusion Prevention Systems. Die in unabhängigen Tests mit Bestnote ausgezeichnete Forcepoint Next-Gen Firewall kann als eigenständiges Layer 2-IPS-Gerät oder als Teil einer vollständigen Layer 3-Firewall der nächsten Generation (Next Generation Firewall, NGFW) in physischen, virtuellen und Cloud-Umgebungen eingesetzt werden. Sie schützt vor Umgehungen, Exploits und Malware, mit denen Angreifer in Unternehmensnetzwerke eindringen und sich dort ausbreiten.

Effektivität und hohe Geschwindigkeit dank einzigartiger Architektur

Forcepoint Next-Generation Firewall verwendet einen dynamischen, datenstrombasierten Ansatz für die Überprüfung, der über die einfache Packet Inspection hinausgeht. Dabei werden die tatsächlichen Nutzlasten rekonstruiert und untersucht, um Umgehungstechniken abzuwehren, mit denen Exploits und Malware verschleiert werden.

Zudem werden Angriffe, die sich in SSL/TLS-Datenverkehr verbergen, mithilfe einer detaillierten Hochgeschwindigkeitsentschlüsselung entlarvt. Forcepoint analysiert jeden Datenstrom und entschlüsselt dabei die verschiedenen Protokollschichten auf der Suche nach auffälligen oder manipulierten Protokollkonfigurationen, Metadaten und Headern.

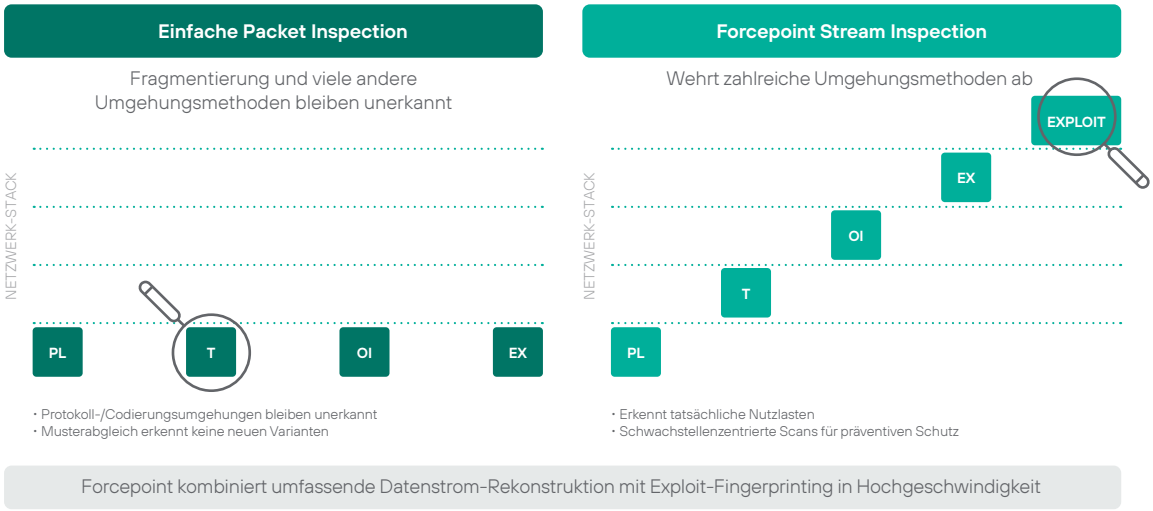
Mithilfe von innovativen Methoden werden dann die Übertragungsinhalte von Forcepoint auf Anzeichen für Exploit-Angriffe untersucht, die die Schwachstellen in vielen Systemtypen ausnutzen. Im Gegensatz zu ausführlichen, musterbasierten Signaturmechanismen ermöglicht es der ausgefeiltere Ansatz von Forcepoint, solche Angriffe mit einem einzigen, prägnanten Fingerabdruck zu identifizieren. Fingerabdrücke werden mit High-Speed Deterministic Finite Automata (DFA) abgeglichen, die auf den jeweiligen Protokollkontext zugeschnitten sind, sodass neue Fingerabdrücke fast ohne Auswirkungen auf die CPU-Ressourcen ergänzt werden können.

Dank kontinuierlicher Updates Angreifern immer einen Schritt voraus

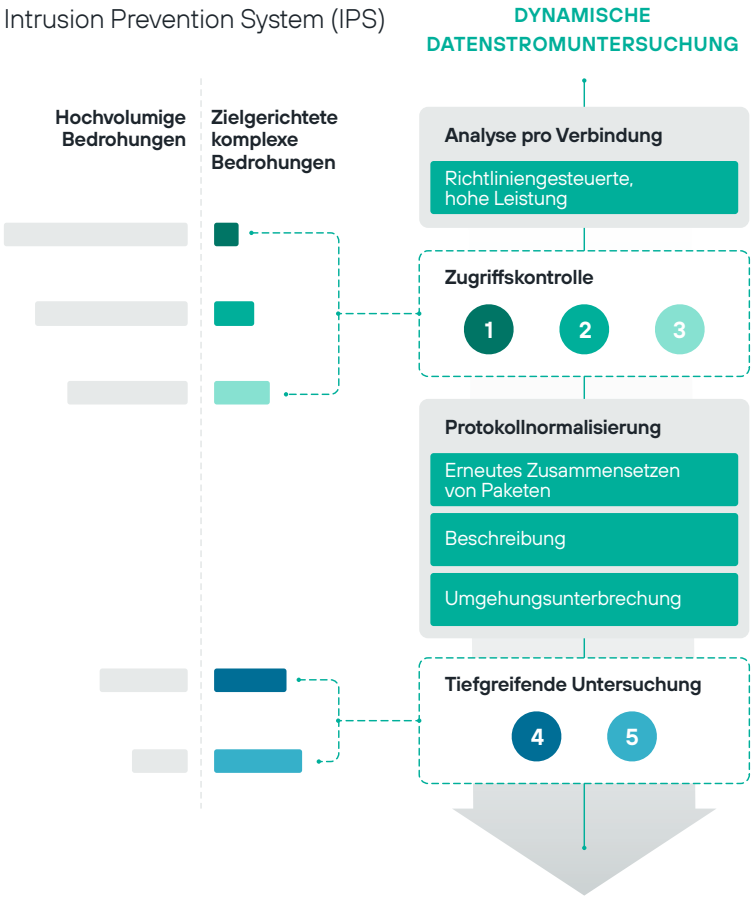
Das globale Forschungsteam von Forcepoint prüft ständig Threat-Intelligence-Feeds, Berichte zu Schwachstellen aus verschiedenen Quellen und eine Vielzahl von Testsystemen, um Exploits und Schwachstellen zu analysieren. Neue Fingerabdrücke werden nach Bedarf über unseren Cloud-Service veröffentlicht und von Forcepoint Netzwerksicherheitssystemen automatisch heruntergeladen. Durch diesen proaktiven Ansatz haben IT-Teams genug Zeit für die Analyse neu veröffentlichter Patches und die Umsetzung von Abhilfemaßnahmen, ohne dass sie eine unmittelbare Gefährdung befürchten müssten.

Schluss mit Zero-Days und unerwünschten Inhalten

Die Netzwerksicherheitsprodukte von Forcepoint bieten zudem mehrere Verteidigungsebenen vor zuvor unbekannten Angriffen und unerwünschten Inhalten. Übertragene Dateien durchlaufen ein strenges Reputations- und Malware-Scanning. Neue Bedrohungen, wie Zero-Day-Angriffe, können mit unserer fortschrittlichen Sandboxing-Technologie aufgedeckt werden. Forcepoint ist einer der Vorreiter auf dem Gebiet der Kategorisierung und Filterung von Websites und Inhalten. Unsere IPS-Geräte und Firewalls erleichtern es Unternehmen, Arbeitsplatzrichtlinien einzuhalten, die Offenlegung personenbezogener Daten zu beschränken und zu verhindern, dass Benutzer Websites mit gefährlichem Inhalt überhaupt erst besuchen.



Forcepoint kombiniert umfassende Datenstrom-Rekonstruktion mit Exploit-Fingerprinting in Hochgeschwindigkeit



1. Verbindungskontrollen
   - Anti-Spoofing
   - IP-Reputation
   - Standortbasierter Schutz
   - Ungültige Verbindungen
2. Verwendungskontrollen
   - Nach Benutzer, URL oder Anwendung (Server und Endpunkt)
3. Befehlskontrollen
   - Whitelists für App-Versionen und -Befehle
   - Proxies zum Schutz vor direkten Verbindungen
4. Schwachstellenuntersuchung
   - Exploit- und Anomalieerkennung
   - Botnet-Schutz
5. Malware-Untersuchung
   - Dateifilterung und -Reputation
   - Anti-Malware-Scans
   - Sandboxing

Fail-Open-Resilienz

Die Appliances von Forcepoint unterstützen eine Reihe von modularen Netzwerkkarten, einschließlich Fail-Open-Schnittstellen, die den Datenverkehr auch dann ermöglichen, wenn Next-Generation Firewall an Leistung verliert.

Schutz für unterbrechungsfreie Geschäftsabläufe

Angreifern fällt es immer leichter, in Unternehmensnetzwerke, Anwendungen, Rechenzentren und Endpunkte einzudringen. Ist ihnen das Eindringen gelungen, können sie geistiges Eigentum, Kundendaten und andere sensible Daten entwenden und so Ihr Unternehmen und Ihren Ruf unwiderruflich schädigen.

Bei Internetangriffen geht es nicht mehr nur darum, Systemschwachstellen auszunutzen. Zunehmend werden auch neue Methoden verwendet, um die Erkennung durch herkömmliche Netzwerksicherheitsgeräte zu umgehen, darunter auch viele Firewalls bekannter Marken.

Diese Umgehungsmethoden funktionieren auf mehreren Ebenen, um Exploit-Angriffe und Malware zu verschleiern und sie für die herkömmliche signaturbasierte Packet Inspection unsichtbar zu machen. Durch diese Umgehungen können sogar alte Angriffe, die jahrelang blockiert wurden, jetzt genutzt werden, um interne Systeme zu beschädigen.

Forcepoint verfolgt einen anderen Ansatz. Unsere branchenführende IPS-Engine wurde für alle drei Stufen der Netzwerkverteidigung konzipiert. Sie schützt vor Umgehungsmethoden, erkennt Exploit-Angriffe auf Schwachstellen und stoppt Malware. Sie kann transparent hinter bestehenden Firewalls eingesetzt werden, um ohne Unterbrechung weiteren Schutz zu bieten, oder als Teil unserer vollständigen Next-Generation Firewall als All-in-One-Sicherheitslösung.

Alle Netzwerksicherheitsprodukte von Forcepoint werden ständig aktualisiert, zentral verwaltet und können Sicherheitsrichtlinien und Dashboards in Ihrem gesamten Netzwerk nahtlos nutzen. Mit Forcepoint können Sie die zuverlässige, durchgängige und effiziente Sicherheit Ihrer Organisation in Rechenzentren, Büronetzwerken, Niederlassungen und Cloud-Umgebungen sicherstellen.

Vorteile

- Weniger Sicherheitsverletzungen
- Mehr Sicherheit ohne Betriebsbeeinträchtigungen
- Geringere Gefährdung durch neue Schwachstellen, während IT-Teams neue Patches bereitstellen
- Sicherere Bereitstellung in Niederlassungen, Cloud-Umgebungen und Rechenzentren
- Geringere Gesamtbetriebskosten (TCO) für Sicherheit und Netzwerkinfrastruktur

Die wichtigsten Merkmale

- Bereitstellung als Layer 2-IPS, Layer 2-NGFW oder als Teil einer Layer 3-NGFW
- Kombination aus Intrusion Detection System (IDS) und Intrusion Prevention System (IPS) für Schutz und Abwehr
- Datenstrom-Überprüfung, bei der die tatsächlichen Nutzlasten untersucht werden
- Vorreiter im Bereich Umgehungsschutz
- Hochgeschwindigkeitsentschlüsselung mit detaillierten Datenschutzkontrollen
- Erkennung von Protokollabweichungen und Missbrauch
- Exploit- und Malware-Erkennung über Hochgeschwindigkeits-DFA
- Denial of Service (DoS)-Erkennung
- Botnet-Schutz
- Zero-Day-Sandboxing über Cloud oder lokale Appliance
- Branchenführende URL-Filterfunktion
- Modulare Fail-Open-Netzwerkschnittstellen für Appliances

Forcepoint Next-Gen Firewall – Technische Daten

UNTERSTÜTZTE PLATTFORMEN	
Appliances	Mehrere Serien modularer Appliances zur Bereitstellung in Rechenzentren, an Netzwerkrändern und in Niederlassungen
Cloud-Infrastruktur	Amazon Web Services, Microsoft Azure
Virtuelle Appliance	Auf x86 64 Bit basierende Systeme; VMware ESXi, VMware NSX, Microsoft Hyper-V und KVM-virtualisierte Umgebung
Bereitstellungsmodi	Eigenständiges IPS (Layer 2, mit optionalen Fail-Open-Netzwerkschnittstellenmodulen), als Teil der NGFW (Layer 3)
Virtueller Kontext	Virtualisierung, um logische Kontexte mit separaten Schnittstellen und Richtlinien zu trennen

ÜBERPRÜFUNG	
Mehrstufige Datenverkehrsnormalisierung/ Umfassende Deep Inspection	› Rekonstruiert und analysiert tatsächliche Nutzlasten, um die Integrität von Datenströmen sicherzustellen › Löscht duplizierte, untergeordnete Segmente, die beim erneuten Zusammensetzen zu Unklarheiten führen könnten
Umgehungsschutz	Blockiert Fragmente außer der Reihe, überlappende Segmente, Protokollmanipulation, Verschleierung und Verschlüsselungstricks
Dynamische Kontexterkennung	Protokoll-, Anwendungs- und Dateityp
Protokollspezifische Datenverkehrsabwicklung/-prüfung	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6-Einkapselung, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, integrierte Prüfung mit Sidewinder Security Proxies
Detaillierte Entschlüsselung von SSL/ TLS-Datenverkehr	› Hochleistungsentschlüsselung von HTTPS-Client- und Serverdatenströmen › Richtliniengesteuerte Kontrollen, um die Privatsphäre der Benutzer zu schützen und die Offenlegung von personenbezogenen Daten in Unternehmen zu beschränken › Gültigkeitsprüfung von TLS-Zertifikaten und Zertifizieren von Domain-basierten Ausnahmelisten
Erkennung von Exploits für Schwachstellen	› Protokollunabhängig, funktioniert mit jedem TCP/UDP-Protokoll mit Erkennung von und Schutz vor Umgehungsmethoden › Unterstützung von Snort-Signaturintegrationen für die Anpassung und Erweiterung des Sicherheitsprofils › Intelligenter Fingerprinting-Ansatz, wodurch weniger Signaturen notwendig sind › Abgleich durch High-Speed Deterministic Finite Automata (DFA) zur schnellen Erstellung neuer Fingerabdrücke › Kontinuierliche Updates von Fingerabdrücken über Forcepoint
Benutzerdefiniertes Fingerprinting	› Protokollunabhängiger Fingerprinting-Abgleich › Ausdrucksbasierte Fingerprinting-Sprache, die benutzerdefinierte Anwendungen unterstützt
Erkundung	TCP/UDP/ICMP-Durchsuchung, Erkennung von Tarnverhalten und langsamen Scans in IPv4 und IPv6
Botnet-Schutz	› Auf Entschlüsselung basierende Erkennung und sequenzielle Analyse der Nachrichtenlänge › Automatische Aktualisierung der URL-Kategorisierung, um Botnet-Websites zu blockieren oder Benutzer vor solchen Websites zu warnen
Korrelation	Lokale Korrelation, Protokollserverkorrelation
Schutz vor DoS/DDoS	› SYN/UDP-Flood-Erkennung mit gleichzeitiger Verbindungsbeschränkung, schnittstellenbasierte Protokollkomprimierung › Schutz vor langsamen HTTP-Abfragemethoden, halboffene Verbindungsbeschränkung › Trennung von Steuerebene und Datenebene
Blockierungsmethoden	Direktes Blockieren, Zurücksetzen von Verbindungen, Blacklists (lokal und dezentral), HTML-Reaktion, HTTP-Umleitung
Aufzeichnung von Datenverkehr	Automatische Aufzeichnung von Datenverkehr / Auszüge von Missbrauchssituationen
Automatische Updates	› Kontinuierliche dynamische Updates über Forcepoint Security Management Center (SMC) › Aktualisierung von virtuellen Patches und Erkennung und Vermeidung von neuen Bedrohungen

Forcepoint Next-Generation Firewall – Technische Daten (Fortsetzung)

ADVANCED MALWARE DETECTION UND DATEIKONTROLLE	
Protokolle	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Dateifilter	Richtlinienbasierte Dateifilter mit effizientem Einschränkungsprozess; über 200 unterstützte Dateitypen in 19 Dateikategorien
Datei-Reputation	Cloudbasierte Hochgeschwindigkeitsprüfung der Malware-Reputation und Malware-Blockierung
Virenscanner für Dateien	Lokale Virenscanner-Engine*
Zero-Day-Sandboxing	Forcepoint Advanced Malware Detection ist für Forcepoint NGFW sowohl als Cloud-Service als auch als lokaler Service verfügbar, wie er auch von Forcepoint Web Security, Forcepoint Email Security und Forcepoint CASB verwendet wird

URL FILTERING	
URL-Kategorisierung	Mithilfe von Forcepoint ThreatSeeker Intelligence, wie bei Forcepoint Web Security und Forcepoint Email Security
Automatische Updates	Kontinuierliche Aktualisierung, wenn neue Websites analysiert werden
Durchsetzung kategoriebasierter Zugriffsrichtlinien	Forcepoint NGFW URL Filtering ist als Add-On-Abonnement verfügbar

VERWALTUNG & ÜBERWACHUNG	
Verwaltungsoberflächen	Zentrales Verwaltungssystem auf Unternehmensebene mit Protokollanalyse-, Überwachungs- und Reporting-Funktionen (weitere Details finden Sie im Datenblatt für Forcepoint Security Management Center)
SNMP-Überwachung	SNMPv1, SNMPv2c und SNMPv3
Erfassen von Datenverkehr	Tcpdump-Konsole, Remote-Erfassung mittels Forcepoint Security Management Center
Hochsichere Management-kommunikation	256-Bit-Sicherheitsstärke für Kommunikation zwischen Engine und Verwaltungsoberfläche
Sicherheitszertifizierungen	Common Criteria Network Devices Protection Profile mit Extended Package Stateful Traffic Filter Firewall, FIPS 140-2Krypto-Zertifikat, CSPN by ANSSI, First Level Security Certification USGv6
Endpoint Context Agent	Whitelisting und Blacklisting von Client-Anwendungen, die auf Hosts und Endbenutzergeräten ausgeführt werden Kann verhindern, dass nicht vertrauenswürdige Dateien ausgehende Verbindungen herstellen können, und ermöglicht granulare Kontrollen, die auf die Anforderungen Ihres Unternehmens angepasst werden können.

*Der lokale Malware-Scan ist bei 110/115-Appliances nicht verfügbar.