Forcepoint

Datenblatt

Next Generation Firewall

Unternehmensnetzwerksicherheit mit nativen SD-WAN-Funktionen

Die wichtigsten Vorteile

Ständige SD-WAN-Konnektivität für Unternehmen

Unternehmen von heute verlangen nach vollständig ausfallsicheren Netzwerksicherheitslösungen. Forcepoint Next-Gen Firewall (NGFW) bietet eine hohe Skalierbarkeit und Verfügbarkeit auf allen Ebenen.

- **Aktiv-aktives, gemischtes Clustering.** Bis zu 16 Knoten verschiedener Modelle mit verschiedenen Versionen können zusammen geclustert werden. Dies bietet eine überragende Netzwerkleistung und -ausfallsicherheit und ermöglicht Sicherheit wie tiefe Paketprüfung und VPNs.
- **Nahtlose Richtlinienupdates und Software-Upgrades.** Die branchenführende Verfügbarkeit von Forcepoint ermöglicht es Richtlinienaktualisierungen (und sogar Software-Upgrades) nahtlos an ein Cluster zu üb ertragen, ohne den Dienst zu un terbrechen.
- **SD-WAN-Netzwerk-Clustering.** Erweitert die hohe Verfügbarkeit auf Ne tzwerk- und VPN-Verbindungen. Kombiniert die ununterbrochene Sicherheit mit der Möglichkeit, lokale Breitbandverbindungen zu nutzen, um teure Mietleitungen wie MPLS zu ergänzen oder zu ersetzen.

Forcepoint Next-Gen Firewall bietet ein branchenführendes Netzwerk Sicherheit mit schneller, flexibler SD-WAN-Konnektivität zur Verbindung und den Schutz der Menschen und der von ihnen genutzten Daten in den verschiedensten, sich entwickelnde Unternehmensnetze. Forcepoint NGFW bietet konsistente Sicherheit, Leistung und Betrieb in physischen, virtuellen und Cloud-Systemen. Es wurde von Grund auf für eine hohe Verfügbarkeit und Skalierbarkeit entwickelt, zusammen mit einer zentralen Verwaltung und einer vollständigen 360°-Sichtbarkeit.

Kunden, die zu Forcepoint NGFW wechseln kunden, die zu Forcepoint NGFW wechseln melden einen Rückgang der Cyberangriffe um 86 %, 53 % weniger Belastung der IT-Abteilung und 70 % weniger Wartungszeit.*

Mit sich ändernden Sicherheitsanforderungen Schritt halten

Ein einheitlicher Softwarekern ermöglicht es Forcepoint, mehrere Sicherheitsrollen zu verwalten,ified software core enables Forcepoint to handle multiple security roles, von Firewall/VPN und ZTNA Application Connector bis Intrusion Prevention System (IPS) und Layer-2-Firewall, in dynamischen Unternehmensumgebungen. Forcepoint kann auf verschiedene Arten eingesetzt werden (z. B. physisch, virtuell), Cloud-Appliances), die alle über eine einzige Konsole verwaltet werden.

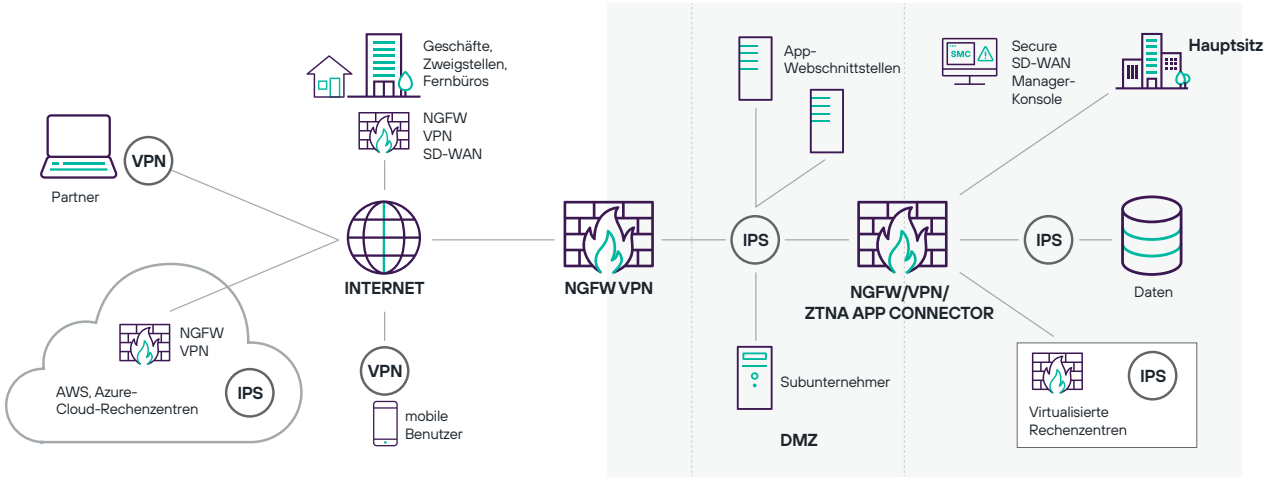
Forcepoint passt die Zugangskontrolle und die Tiefeninspektion für jede Verbindung an, um eine hohe Leistung und Sicherheit zu bieten. Es kombiniert granulare Anwendungskontrolle, IPS-Schutz, integrierte Kontrolle über virtuelle private Netzwerke (VPN), und geschäftskritische Anwendungsproxys in eine effiziente, erweiterbare und hoch skalierbares Design. Unsere leistungsstarken Anti-Evasion-Technologien dekodieren und normalisieren den Netzwerkverkehr vor der Inspektion und über alle Protokollschichten hinweg, um die fortschrittlichsten Angriffsme thoden aufzudecken und zu blockieren.

Blockieren sie fortschrittliche kompromittierungsangriffe auf ihre daten

Große Datenschutzverletzungen plagen Unternehmen und Organisationen in jeder Branche nach wie vor. Bekämpfen Sie diese Bedrohung mit einem Exfiltrationsschutz auf Anwendungsebene. Forcepoint erlaubt oder blockiert selektiv und automatisch den Netzwerkverkehr von bestimmten Anwendungen auf PCs, Laptops, Servern, Dateifreigaben und anderen Endpunktgeräten auf der Grundlage hochgranularer kontextbezogener Endpunktdaten. Es geht über typische Firewalls hinaus, um den Versuch der Exfiltration sensibler Daten von Endpunkten über nicht autorisierte Programme, Webanwendungen, Benutzer und Kommunikationskanäle zu verhindern.

* „Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, Mai 2017.

Eine Plattform mit vielen Bereitstellungsoptionen – verwaltet von einer einzigen Konsole



Unübertroffener Schutz

Angreifer sind zu Experten für das Eindringen in Unternehmensnetzwerke, Anwendungen, Rechenzentren und Endpunkte geworden. Sobald sie dort sind, stehlen sie geistiges Eigentum, Kundeninformationen und andere sensible Daten, was Unternehmen und ihrem jeweiligen Ruf irreparablen Schaden zufügt.

Neue Angriffstechniken können die Erkennung durch herkömmliche Sicherheitsnetzwerkgeräte, einschließlich vieler namhafter Firewalls, umgehen, und gehen über die einfache Übertragung von Schwachstellenausnutzungen hinaus.

Umgehungstechniken funktionieren auf mehreren Ebenen, um Exploits und Malware z u tarnen und sie für die herk ömmliche signaturbasierte Paketprüfung unsichtbar zu machen. Selbst Angriffe, die seit Jahren blockiert werden, können mit Umgehungen umgepackt werden, um interne Systeme zu kompromittieren.

Forcepoint verfolgt einen anderen Ansatz. Unsere branchenführende Sicherheits-Engine wurde für alle drei Phasen der Netzwerkverteidigung entwickelt: zur Bekämpfung von Umgehungen, zur Erkennung von Exploits von Schwachstellen und zur Verhinderung von Malware. Es kann transparent hinter bestehenden Firewalls bereitgestellt werden, um einen unterbrechungsfreien Schutz zu bieten, oder als voll funktionsfähige Enterprise Firewall für All-in-One-Sicherheit.

Darüber hinaus bietet Forcepoint eine schnelle Entschlüsselung des verschlüsselten Datenverkehrs, einschließlich HTTPS-Webverbindungen, in Kombination mit granularen Datenschutzkontrollen, die Ihr Unternehmen und Ihre Benutzer in einer sich schnell verändernden Welt schützen. Es kann sogar den Zugriff von bestimmten Endpunkten aus beschränken Anwendungen zum Sperren von Geräten oder zum Verhindern des Verwendung von anfälliger Software.

Vorteile für Ihr Unternehmen

- → Schnellere Einführung von Zweigstellen, Clouds oder Rechenzentren
- → Weniger Ausfallzeiten
- → Größere Sicherheit ohne Unterbrechung
- → Weniger Verletzungen
- → Weniger Gefährdung durch neue Schwachstellen, während sich IT-Teams auf die Bereitstellung neuer Patches vorbereiten
- → Geringere Gesamtkosten für Netzwerkinfrastruktur und -sicherheit

Wichtigste Merkmale

- → SD-WAN-Konnektivität im Unternehmensmaßstab
- → SASE/SSE-Integration für Web, Cloud, Sicherheit privater Anwendungen
- → Integriertes IPS mit Anti-Evasion-Abwehr
- → Hochverfügbarkeits-Clustering von Geräten und Netzwerken
- → Automatisierte, ausfallfreie Updates
- → Richtliniengesteuerte zentrale Verwaltung
- → Umsetzbare, interaktive 360°-Sichtbarkeit
- → Sidewinder Security Proxies für missionskritische Anwendungen
- → Benutzer- und Endpunktkontext
- → Leistungsstarke Entschlüsselung mit granularen Datenschutzkontrollen
- → Erlauben/Sperren nach Client-Anwendung und Version
- → Überwachung des Anwendungszustands
- → CASB- und Web-Sicherheitsintegration
- → Anti-Malware-Sandboxing
- → Einheitliche Software für physische, AWS, Azure, VMware-Bereitstellungen
- → Weniger Gefährdung durch neue Schwachstellen, während sich IT-Teams auf die Bereitstellung neuer Patches vorbereiten
- → Geringere Gesamtkosten für Netzwerkinfrastruktur und -sicherheit

Forcepoint NGFW-Spezifikationen

PLATTFORMEN	
Physische Appliance	Mehrere Hardware-Appliance-Optionen, von Zweigniederlassungs- bis hin zu Rechenzentrumsinstallationen
Cloud-Infrastruktur	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Virtuelle Appliance	x86-64-Bit-basierte Systeme; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM und Nutanix AHV
Endpunkt	EEndpoint Context Agent (ECA), VPN-Client
Virtuelle Kontexte	Bis zu 250
Zentrale Verwaltung	Zentralisiertes Managementsystem auf Unternehmensebene mit Protokollanalyse, Überwachung und Reporting-Funktionen. Weitere Informationen finden Sie im Datenblatt zum Forcepoint Security Management Center.

FIREWALL-FUNKTIONEN	
Deep Packet Inspection	Mehrschichtige Verkehrsnormalisierung/Vollstrom-Tiefeninspektion, Anti-Evasions-Verteidigung, dynamisch Kontexterkennung, protokollspezifische Verkehrsabwicklung/Inspektion, granulare Entschlüsselung von SSL/TLS-Verkehr (sowohl TLS 1.2 als auch 1.3), Erkennung von Sicherheitslücken und benutzerdefinierten Fingerabdrücken, Aufklärung, Anti-Botnet, Korrelation, Verkehrsaufzeichnung, DoS/DDoS-Schutz, Blockieren Methoden, Automatische Updates
Benutzeridentifikation	Interne Benutzerdatenbank, natives LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Client-Zertifikate
Hochverfügbarkeit	› Active-active/active-standby Firewall-Clustering bis zu 16 Knoten › SD-WAN › Zustandsbehaftetes Failover (einschließlich VPN-Verbindungen) › Server-Lastverteilung › Link-Aggregation (802.3ad) › Link-Fehlererkennung
IP-Adresszuordnung	› IPv4 statisch, DHCP, PPPoA, PPPoE, IPv6 statisch, SLAAC, DHCPv6 › Dienste: DHCP-Server für IPv4 und DHCP-Relay für IPv4 und IPv6
Routing	› Statisches IPv4- und IPv6-Routen, richtlinienbasiertes Routing, statisches Multicast-Routing › Dynamisches Routing: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP proxy › Anwendungsabhängiges Routing
IPv6	Dual-Stack-IPv4/IPv6, NAT64, ICMPv6, DNSv6, NAT, vollständige NGFW-Funktionen
Proxy-Umleitung	HTTP-, HTTPS-, FTP-, SMTP-Protokolle-Umleitung an Forcepoint oder einen Drittanbiet er-Content-Inspection-Service (CIS) vor Ort und in der Cloud
Geo-Schutz	Dynamisch aktualisiertes Quell-/Zielland oder Kontinent
IP-Adressliste	Vordefinierte IP-Kategorien oder Verwendung von benutzerdefinierten oder importierten IP-Adresslisten
URL-Filterung (separates Abonnement)	Benutzerdefinierte oder importierte URL-Listen; unterstützt QUIC und HTTP/3
Endpunkt-Anwendungen:	Anwendungsname und -version
Netzwerkanwendungen	Über 7400 Netzwerk- und Cloud-Anwendungen
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

SASE-INTEGRATION	
Web-Traffic-Weiterleitung	GRE und IPsec Tunneln zu Security Service Edge (SSE) Plattformen wie Forcepoint ONE
ZTNA Application Connector	Ermöglicht privaten Anwendungen in internen Rechenzentren, sich mit Forcepoint ONEs Zero Trust zu verbinden

SD-WAN	
Protokolle	IPsec and TLS
Site-to-Site VPN	› Site-to-Site-VPN › Richtlinien- und routenbasiertes VPN › Nabe und Speiche, volles Mesh, teilweises Mesh, Hybrid-Topologien › Dynamische Auswahl mehrerer ISP-Links › Lastverteilung, Aktiv/Standby, Link-Aggregation › Live-Überwachung und Berichterstattung über die ISPs Linkqualität (Verzögerung, Jitter, Paketverlust)
Remote-Zugriff	› Forcepoint VPN-Client für Microsoft Windows, Android und Mac OS › Jeder Standard-IPsec-Client › Hohe Verfügbarkeit mit automatischem Failover › Client-Sicherheitsüberprüfungen › Zugriff auf das TLS VPN-Portall

ERWEITERTE MALWARE-ERKENNUNG UND DATEIKONTROLLE	
Protokolle	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Dateifilterung	Richtlinienbasierte Dateifilterung mit effizientem Auswahlverfahren. Über 200 unterstützte Dateitypen in 19 Dateikategorien
Datei-Reputation	Hochgeschwindigkeits-Cloud-basierte Malware-Reputationsprüfung und -blockierung
Anti-Virus	Lokale Antivirus-Scan-Engine*
Zero-Day Sandboxing	Forcepoint Advanced Malware Detection and Protection ist sowohl als Cloud- als auch als lokaler Dienst verfügbar

* Lokaler Anti-Malware-Scan ist nicht mit 110/115-Appliances verfügbar.