

# Schutz für die Grenzen des Unternehmensnetzwerks mit direkter Cloud-Konnektivität und -Sicherheit

## Lösung

- › Forcepoint Edge Protection schützt Standorte, Benutzer und Daten an jedem Ort.
- › Forcepoint NGFW mit SD-WAN integriert direkte Cloud-Konnektivität und umfassende Netzwerksicherheit unternehmensweit.
- › Forcepoint Web Security schützt Benutzer überall vor komplexen Bedrohungen und risikobehafteten Web-Anwendungen.
- › Forcepoint CASB schützt Anwendungen und Daten in der Cloud vor Angriffen und Missbrauch.

## Ergebnis

- › **Produktivitätssteigerungen:** schnellere interne und Cloud-Anwendungen sowie weniger Ausfallzeiten
- › **Geringere Kosten:** weniger Einzelprodukte, die implementiert und verwaltet werden müssen, effizientere Breitbandnutzung und einfachere Bedienung
- › **Geringeres Risiko:** höhere lückenlose Sicherheit ohne Redundanzen sowohl lokal als auch in der Cloud
- › **Optimierte Compliance:** Kontrolle aus einer Hand und mehr Transparenz für eine schnellere Reaktion auf Vorfälle

**Initiativen zur digitalen Transformation ersetzen häufig zunächst intern gehostete Anwendungen durch Cloud-basierte Software-as-a-Service- (SaaS-) Anwendungen, die einen ortsunabhängigen Zugriff ermöglichen. Allerdings können viele herkömmliche Backhaul-Netzwerke die erforderliche Leistung nicht erbringen. Die Übertragung großer Datenmengen von Remote-Standorten über den Hauptsitz kann die Benutzerproduktivität einschränken und eine ältere Netzwerk- bzw. Sicherheitsinfrastruktur überlasten. Die Aktualisierung von Netzwerken ist möglicherweise unerschwinglich oder erfordert die Implementierung unterschiedlicher Technologien, die das System komplexer machen und die Transparenz reduzieren. Glücklicherweise gibt es eine Alternative.**

### Transformation der Konnektivität mit SD-WAN

Software-Defined Wide-Area Networking (SD-WAN) hat einen Paradigmenwechsel für Unternehmen eingeleitet. Durch die Nutzung von schnelleren und kostengünstigeren lokalen Internetverbindungen an Remote-Standorten bietet SD-WAN die folgenden Vorteile:

- **Geringere Netzwerkkosten:** Teure MPLS-Leitungen können durch herkömmliche Internetverbindungen (DSL, Kabel, Glasfaser) in Verbindung mit VPN-Software ergänzt oder ersetzt werden.
- **Produktivitätssteigerungen:** Durch direkte Cloud-Konnektivität können Benutzer an Remote-Standorten leichter auf die nötigen Ressourcen zugreifen, um die neuen Cloud-basierten Anwendungen optimal nutzen zu können.
- **Geringere Betriebskosten:** Zentral verwaltete SD-WAN-Lösungen bieten den Netzwerkbetriebsteams eine bessere Transparenz und Kontrolle, ohne dafür vor Ort sein oder ein Flickwerk verschiedener Konsolen verwenden zu müssen.

### Schutz für die neuen Grenzen von Unternehmensnetzwerken

Wenn man von Remote-Standorten direkt auf die Cloud zugreift, verlagern sich auch die Grenzen des Unternehmensnetzwerks in die Cloud. Bei den meisten SD-WAN-Lösungen werden Daten durch Verschlüsselung geschützt. Das ist jedoch nur die halbe Miete. Wurde die Sicherheit bislang über zentralisierte Gateways vor Ort geregelt, muss es nun für jeden Standort bzw. die Cloud eine Lösung geben:

- **Netzwerksicherheit:** Zugriffskontrolle und Intrusion Prevention bieten Schutz vor Angriffen – meist in Form von Next Generation Firewalls (NGFW).
- **Web-Sicherheit:** Echtzeitschutz vor komplexen Bedrohungen, die auf Webseiten oder in Downloads lauern, ist unbedingt erforderlich. Dieser ist in der Regel als Cloud-Service verfügbar und kann, falls nötig, durch eine hybride Anwendung für lokale und Roaming-Benutzer ergänzt werden.
- **Datensicherheit für Cloud-Anwendungen:** Anwendungen und Daten in der Cloud müssen überwacht werden, um Angriffe und Missbrauch zu vermeiden.

Moderne Schutzlösungen für die Netzwerkgrenzen vereinen all diese Aspekte. So können Unternehmen ihre Netzwerke, Benutzer und Daten nahtlos und sicher miteinander verbinden und so ihre digitale Transformation beschleunigen.

### Einheitliche Konnektivität und Sicherheit auf globaler Ebene

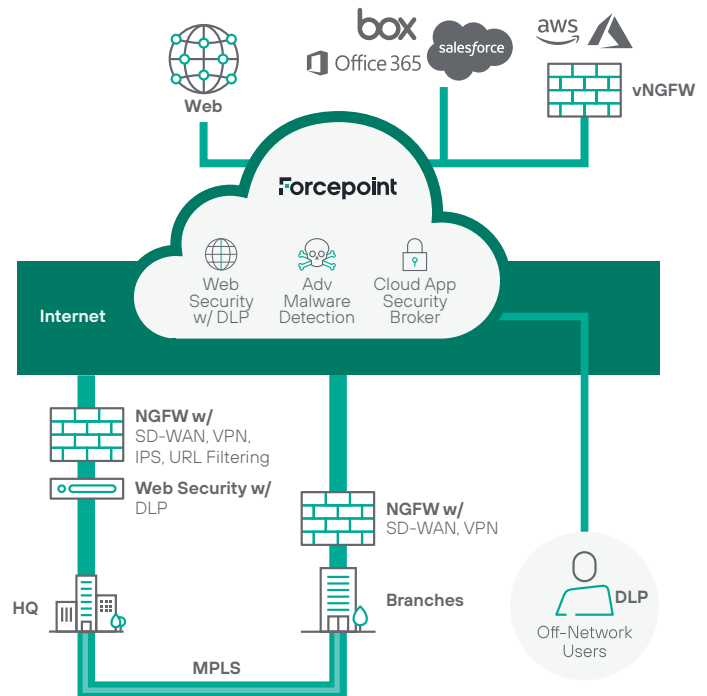
Weltweit vertrauen zahlreiche Unternehmen und Behörden auf die Lösungen von Forcepoint, um ihre weit verzweigten Standorte, Filialen und Niederlassungen zu verbinden und zu schützen. Wir haben Pionierarbeit für hochsicheres Multi-Link-Networking geleistet.

Zudem waren wir branchenweit die ersten, die ausgeklügelte Verschleierungstechniken (Advanced Evasion Techniques) erkannt und bekämpft haben, mit denen Angreifer schädlichen Code wie Ransomware durch die meisten Abwehrsysteme ins Netzwerk schleusen. Daher hat die Forcepoint NGFW mehrfach Spitzenwertungen im Bereich Sicherheit erzielt, u. a. im NGFW-Gruppentest, im NGIPS-Test und in den SD-WAN-Tests von NSS Labs.

Und das ist nur der Anfang. Unsere Sicherheitslösungen schützen auch bei der allgemeinen Internetnutzung, also beim Aufrufen von Web-Inhalten und der Bearbeitung von Daten in Cloud-Anwendungen. Forcepoint Web Security bietet soliden Schutz vor komplexen Bedrohungen und geht dabei über das einfache Blockieren von URLs hinaus: Websites und deren Inhalte werden dynamisch auf versteckte Malware und Zero-Day-Angriffe gescannt. Das Motto lautet: „Cloud-first und bereit für hybride Umgebungen.“ So erkennt Forcepoint Web Security auch potenzielle Gefahren, die mehr als 6000 Anwendungen betreffen könnten, und bietet die Möglichkeit, Risiken von Schatten-IT mit sofortiger Wirkung zu priorisieren. Damit Daten auf dem Weg in Cloud-Anwendungen geschützt

sind, überwacht Forcepoint CASB sensible (auch selbst entwickelte, benutzerdefinierte) Anwendungen automatisch, indem es Anzeichen einer betrügerischen Nutzung erkennt und die in diesen Anwendungen hinterlegten Richtlinien für Unternehmensdaten durchsetzt.

Die Grenzen des Unternehmensnetzwerks weltweit verbinden und schützen – das macht Forcepoint einzigartig.



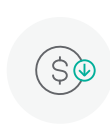
### Die Grenzen des Unternehmensnetzwerks mit Forcepoint schützen

Weltweit vertrauen Unternehmen und Behörden auf Forcepoint, weil sie mit uns bessere operative Ergebnisse erzielen:



**Höhere Produktivität**  
(Steigerung der Vertriebs-/ Serviceleistung)

- › Umfassende Konnektivität (Cloud und Site-to-Site über mehrere Verbindungen)
- › Schnellere Anwendungen
- › Hochverfügbarkeit



**Geringere Kosten**  
(Infrastruktur/Betrieb)

- › Weniger Einzelprodukte und Konsolen
- › Geringere Betriebskosten
- › Effizienz durch Lösungen von einem Anbieter



**Geringeres Risiko**  
(weniger Sicherheitsverletzungen)

- › Ein Plus an Sicherheit
- › Weniger Sicherheitslücken/ Redundanzen
- › Flexiblere Installation (Cloud & hybride Umgebungen)



**Optimierte Compliance**  
(zufriedenere Auditoren)

- › Kontrolle aus einer Hand
- › Mehr Transparenz
- › Schnellere Reaktion auf Vorfälle

Möchten Sie erfahren, wie Sie Forcepoint Edge Protection in Ihrem Unternehmen sinnvoll einsetzen können? Sprechen Sie mit unseren Experten:

[forcepoint.com/contact](https://forcepoint.com/contact)