



WIE INTEGRIERT IST IHRE NETZWERKSICHERHEIT?

Die Trennung zwischen Networking und Sicherheit verschwindet, und das ist gut so. Da KI neue Chancen und Risiken birgt, gehört Sicherheit von Beginn an in das Netzwerk. Wenn Ihre Netzwerk- und Sicherheitsstrategien Hand in Hand gehen, erreichen Sie eine bessere Transparenz, eine schnellere Reaktion auf Sicherheitsbedrohungen und insgesamt eine höhere Ausfallsicherheit.

Wo steht Ihre Organisation auf dem Weg zu einer von Grund auf sichereren Architektur? Überprüfen Sie die drei unten aufgeführten verschiedenen Betriebsprofile, um Ihr aktuelles Setup zu bewerten, Legacy-Annahmen zu hinterfragen und einen besseren Weg zum Schutz Ihres Unternehmens zu entdecken.

Profil 1: Fragmentierte Verteidigung

Gilt für Ihre Netzwerk- und Sicherheitsteams ...	Die Kompromisse
Dass sie mehrere, unterschiedliche Konsolen verwenden?	Durch die unterschiedlichen Konsolen fehlen gemeinsame Daten, was die Ermittlungen verlangsamt und operative Schwachstellen entstehen lässt.
Dass sie Domänen in verschiedenen Umgebungen manuell konfigurieren?	Hohes Risiko menschlicher Fehler und uneinheitlicher Durchsetzung von Richtlinien in Campus-, Zweigstellen-, Remote- und IoT-Umgebungen.
Dass sie Schwierigkeiten bei der Identifizierung und Profilierung von nicht standardisierten IoT Geräten haben?	Geräte verbinden sich ohne verifizierte Identität außerhalb des IT-Bereichs, wodurch die Angriffsfläche vergrößert und Schwachstellen geschaffen werden.
Dass sie mehrere fragmentierte Geräte von verschiedenen Anbietern verwalten?	Ein komplexes architektonisches Rätsel, das die Aufrechterhaltung einheitlicher Sicherheit erschwert.
Dass sie Daten nach einem Vorfall manuell aus fragmentierten Protokollen zusammensetzen?	Die Rekonstruktion einer vollständigen Ansicht über unverbundene Quellen hinweg kann die Eindämmung von Vorfällen verzögern und die Zeiträume der Bedrohungslage verlängern.
Dass sie stark von manuellen Arbeitsabläufen abhängig sind?	Hohe operative Komplexität, langsamere Reaktionszeiten und die Unfähigkeit, den Schutz mit wachsenden Geschäftsanforderungen zu skalieren.



Profil 2: Vernetzte Infrastruktur

Gilt für Ihre Netzwerk- und Sicherheitsteams ...	Die Kompromisse
Dass sie hohe Transparenz vor allem für Kernsysteme aufrechterhalten?	Am Netzwerk-Edge bestehen weiterhin erhebliche Schwachstellen, die Ihre Fähigkeit einschränken, Bedrohungen im Frühstadium zu erkennen.
Dass sie Kernvorlagen anwenden und gleichzeitig Randpositionen manuell verwalten?	Manuelle Ausnahmen am Rand führen zu Inkonsistenzen und schwächen die Durchsetzung von Richtlinien.
Dass sie automatisiertes Scannen mit manueller Validierung verwenden?	Die Automatisierung beschleunigt die Erkennung, aber die Abhängigkeit von der menschlichen Validierung verlangsamt die Behebung von Anomalien.
Dass sie die Cloud Edges separat von Ihren primären Rechenzentren aktualisieren?	Aufgeteilte Management-Workflows führen zu einem uneinheitlichen Sicherheitsniveau in den verschiedenen Umgebungen.
Dass sie auf manuelle Eingriffe zur Analyse von Verhaltensanomalien zurückgreifen?	Warnmeldungen weisen auf bekannte Merkmale hin, die Analyse von Verhaltensanomalien ist jedoch stark von menschlichem Eingreifen abhängig.
Dass sie Kernstabilität neben getrennten Edge Tools verwalten?	Auch wenn die Kernumgebungen standardisiert und stabil sind, bleiben durch die fehlende Integration in die Netzwerkumgebung kritische Zweigstellen und IoT-Standorte ungeschützt.

Profil 3: Autonomer Schutz

Gilt für Ihre Netzwerk- und Sicherheitsteams ...	Die Vorteile
Gibt es eine gemeinsame Quelle der Wahrheit?	Beseitigt Datensilos, korreliert Daten in Echtzeit und ermöglicht eine nahtlose teamübergreifende Zusammenarbeit.
Zentralisierte, identitätsbasierte Richtlinien einsetzen?	Gewährleistet, dass Richtlinien Benutzern und Geräten in allen Umgebungen automatisch folgen und so einen einheitlichen Schutz gewährleisten.
Kontinuierliche KI-Profilierung für neue Geräte nutzen?	Erkennt und klassifiziert neue Geräte sofort und automatisch ohne manuellen Aufwand.
Eine einheitliche Managementebene für Firewalls nutzen?	Orchestriert Cloud-native und lokale Firewall-Richtlinien global von einem einzigen Punkt aus.
KI für automatisierte Sicherheitsoperationen einsetzen?	Kann das Vertrauen in Echtzeit anpassen und durch automatisches Erkennen und Blockieren von Bedrohungen sofortige Gegenmaßnahmen auslösen.
Auf einer einheitlichen Architektur aufbauen?	Skaliert die Infrastruktur nahtlos und passt sich sofort an neue Bedrohungen an, ohne den Betriebsaufwand zu erhöhen.

Der Weg zum modernen Schutz

Das Hinzufügen unzusammenhängender Sicherheitstools zu einer Legacy-Infrastruktur erhöht die Komplexität und schafft gefährliche Schwachpunkte. Echte Cyber-Ausfallsicherheit erfordert einen grundlegenden Wandel: die Betrachtung des eigenen Netzwerks als Quelle für Bedrohungsinformationen und die Durchsetzung von Richtlinien in Echtzeit. Durch die Zusammenführung von Routing, Switching und Zero Trust-Sicherheit in einem einzigen intelligenten System verwandeln Sie Ihre Infrastruktur in eine aktive Verteidigungsebene.

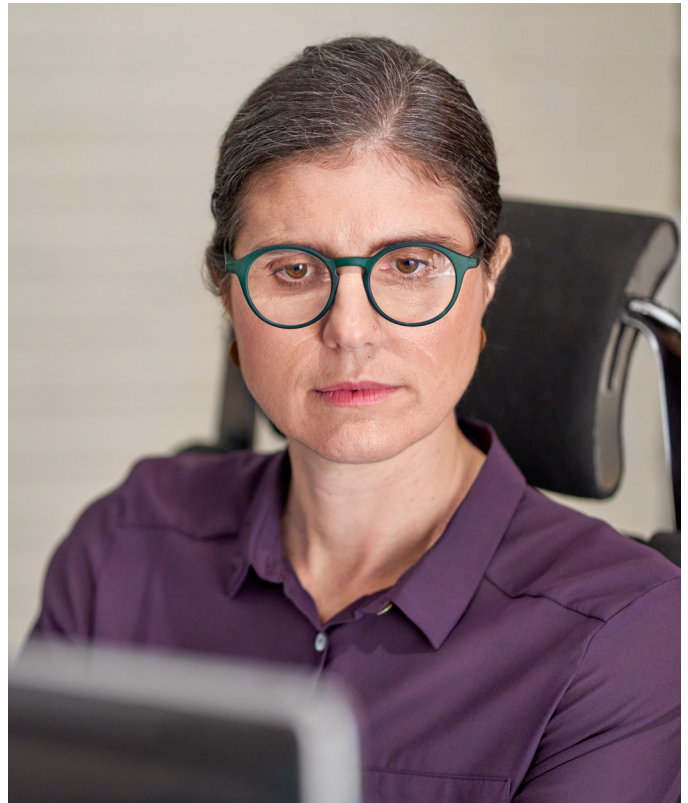
Bereit für echte, integrierte Sicherheit? Erfahren Sie, wie ein einheitlicher Ansatz betriebliche Abläufe vereinfacht und die Cyber-Ausfallsicherheit durch KI-gestützte Transparenz, globale Richtliniendurchsetzung und die Reaktion auf Sicherheitsbedrohungen in Echtzeit in Ihrer gesamten Edge-to-Cloud-Umgebung stärkt.

Weitere Informationen finden

Sie unter:

[HPE.com/networking](https://hpe.com/networking)

HPE.com besuchen



[Jetzt chatten](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Die Informationen in diesem Dokument können jederzeit ohne vorherige Ankündigung geändert werden. Neben der gesetzlichen Gewährleistung gilt für Produkte und Dienstleistungen von Hewlett Packard Enterprise ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Dienstleistungen explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

a00161060DEE

HEWLETT PACKARD ENTERPRISE

hpe.com

