DATENBLATT

Zero Trust Bundle

Sicherheit ohne Grenzen

Dauerhafter Rund-um-die-Uhr-Schutz, der die Anwender überallhin begleitet

Die Mitarbeitenden von heute können sich von überall aus verbinden – zu Hause, im Büro, an Flughäfen oder im öffentlichen WLAN. Jede neue Verbindung bietet Angreifern die Möglichkeit, schwache Anmeldeinformationen, kompromittierte Geräte oder exponierte Anwendungen auszunutzen. Das WatchGuard Zero Trust Bundle erweitert den Schutz auf jeden Benutzer und jedes Gerät, wo auch immer Sie arbeiten.

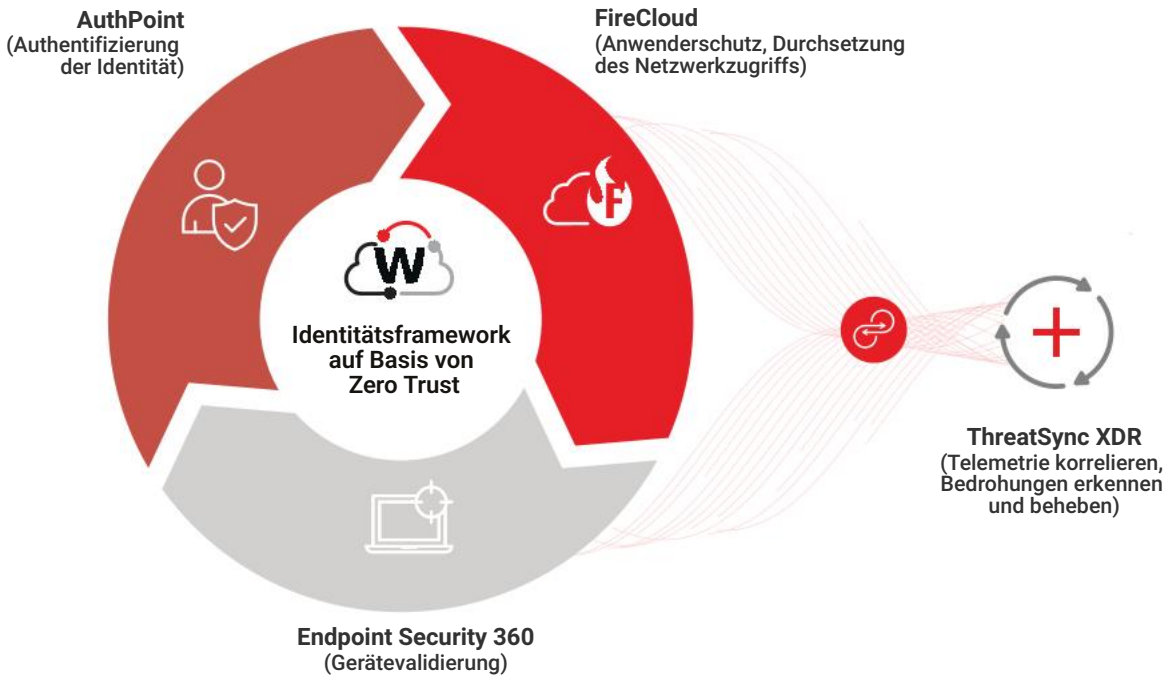
Mit WatchGuard Zero Trust können Sie:

1. **Vertrauen schaffen,** indem Sie jeden Benutzer und jedes Gerät überprüfen, bevor Sie bei einer neuen Sitzung Zugriff gewähren
2. **Sich vor internetbasierten Bedrohungen schützen,** wenn Benutzer eine Verbindung herstellen, und erhalten Sie Einblicke in Benutzeraktivitäten und -risiken
3. **Angriffe und laterale Bewegungen verhindern** – über lokale Anwendungen und Daten hinweg mit Zero-Trust-Netzwerkzugriff

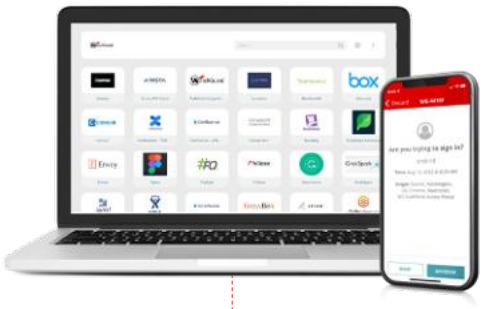
Management und Bereitstellung aus der Cloud

Das Zero Trust Bundle wird zu 100 % cloudverwaltet, sodass keine Software gewartet oder Hardware bereitgestellt werden muss. Administratoren definieren Zero-Trust-Richtlinien, stellen Endpoint-Agenten bereit und verwalten Authentifizierungstoken über eine einheitliche Konsole in der WatchGuard Cloud. Durch die standardmäßige Integration für führende Bereitstellungstools und mandantenfähiges Management profitieren Unternehmen sowie Managed Service Provider von schneller Einsatzfähigkeit und einfacher Skalierung.

> Kontinuierliche Verifizierung von Anwenderidentität, Gerät und Netzwerk

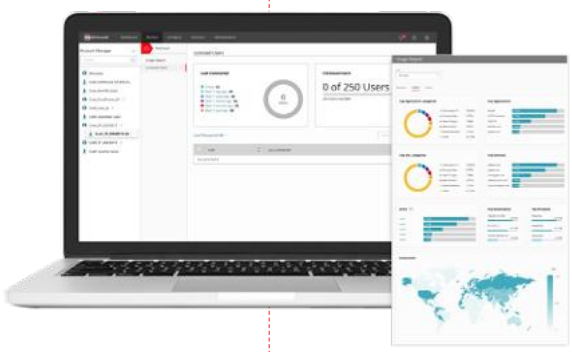


Umfang des Zero Trust Bundle



> Multifaktor-Authentifizierung mit Überwachung von Anmeldedaten im Dark Web

Da der Diebstahl von Anmeldeinformationen und das Kompromittieren von Benutzerkonten auf dem Vormarsch sind, ist die Überprüfung der Identität der Grundpfeiler von Zero Trust. AuthPoint bietet Multifaktor-Authentifizierung, Single Sign-On und risikobasierte Richtlinien, die jeden Benutzer kontextbasiert überprüfen. Die integrierte Überwachung von Anmeldeinformationen im Dark Web erkennt proaktiv exponierte Anmeldeinformationen, bevor Angreifer diese ausnutzen können. AuthPoint stellt sicher, dass die richtige Person zum richtigen Zeitpunkt mit den richtigen Faktoren Zugriff erhält.



> Hybride Netzwerksicherheit und Zero-Trust-Netzwerkzugriff

Fire Cloud Total Access vereint sicheren Internetzugriff und Zero-Trust-Netzwerkzugriff in einem Cloud-Dienst. Es ersetzt VPNs durch identitätsbasierte Konnektivität pro Sitzung für SaaS und private Apps. Firewall as a Service und Secure Web Gateway blockieren Phishing und Malware in jedem Netzwerk. Zero-Trust-Richtlinien überprüfen Benutzer und Geräte vor der Gewährung von Zugriff. Globale PoPs sorgen dafür, dass Sitzungen schnell, verschlüsselt und für Angreifer unsichtbar bleiben.

> Erweiterte Endpoint-Sicherheit

Die KI-Engine der WatchGuard Endpoint-Security überwacht und klassifiziert jeden Prozess, um unbekannte oder bösartige Aktivitäten automatisch zu blockieren. Der Zero-Trust Application Service verhindert Zero-Day-Exploits und In-Memory-Angriffe. Kontinuierliche Überprüfungen der Sicherheitslage bestätigen, dass jedes Gerät die Sicherheitsrichtlinien vor dem Zugriff erfüllt. Nur vertrauenswürdige, konforme Endpoints sind für Zero-Trust-Verbindungen zugelassen.

WatchGuard Cloud

Mobile AuthPoint-App

AUTHENTIFIZIERUNGSFUNKTIONEN

- Push-basierte Authentifizierung (online)
- QR-Code-basierte Authentifizierung (online und offline)
- Zeitbasiertes Einmalkennwort (online und offline)

SICHERHEITSFUNKTIONEN

- DNA-Signatur des Geräts
- Onlineaktivierung mit Erstellung von dynamischen Schlüsseln
- Schutz pro Authentifikator
  - PIN
  - Fingerabdruck (Samsung/Apple)
  - Gesichtserkennung (Apple)
- Self-Service: Sichere Migration des Authentifikators von einem Smartphone zum Nächsten
- Jailbreak und Root-Detection

PRAKTISCHE FUNKTIONEN

- Unterstützung mehrerer Tokens
- Unterstützung für Social-Media-Token von Drittanbietern
- Anpassbare Token-Namen und -Bilder

STANDARDS

- OATH Time-Based One-Time Password Algorithm (TOTP) – RFC 6238
- OATH Challenge-Response Algorithms (OCRA) – RFC 6287
- OATH Dynamic Symmetric Key Provisioning Protocol (DSKPP) – RFC 6063

Endpoint Detection and Response

UNTERSTÜTZTE BETRIEBSSYSTEME

- **Windows:** Workstations – XP, Vista, 7, 8, 8.1, 10. Server – 2003 SP2 und höher, 2008, 2008 R2, SBS 2011, 2012, 2012 R2, 2016, 2019, Server Core 2008, 2008 R2, 2016, 2019
- **Linux:** Red Hat Enterprise 6.0 und höher, Debian Squeeze, Ubuntu 12 oder höher, OpenSuse 12 oder höher, Suse Enterprise Server 11SP2 oder höher, CentOS 6.x und höher
- **macOS:** 106 Snow Leopard, 10.7 Lion, 10.8 Mountain Lion, 10.9 Mavericks, 10.10 Yosemite, 10.11 El Capitan, Sierra

ERKENNUNGSMETHODEN

- Generalistische Signaturen und -Heuristiken
- Cloudbasierter Abgleich mit der Schwarmintelligenz
- IoAs-Erkennung
- Firewall, IDS/IPS
- Manipulationsabwehr
- Gerätesteuerung
- Endpoint-Aktivitätsüberwachung und EDR-Funktionen wie:
- Kontextuelle Verhaltenserkennung
- Anti-Exploit-Technologie für den Arbeitsspeicher

Überwachung von Anmeldedaten im Dark Web

ERKENNUNGSMETHODEN

- Kontinuierliche Überwachung der Anmeldedaten
- Korrelation kompromittierter Anmeldedaten nach Benutzerkonto
- Registrierung jeder erkannten Sicherheitsverletzung mit dem Kontext

FireCloud

UNTERSTÜTZTE BETRIEBSSYSTEME

- Windows 7, 8 und 10
- Gateway: Hyber-V (Windows Server 2022/2025, VMware ESXi 7.0/8.0, Proxmox 8.4/9.0

ERKENNUNGSMETHODEN

- Blockieren von Phishing-Angriffen
- Verhindern von C2-Verbindungen
- Inhaltsfilterung
- Sofortige Schulung zum Sicherheitsbewusstsein

UNTERSTÜTZTE AUTHENTIFIZIERUNGEN

- AuthPoint
  SAML: Drittanbietern-IDP, Entra ID, Okta, FIDO
- WatchGuard Cloud Directory: Active Directory, Entra ID, Cloud Directory
- Identitätsprüfung auf Sitzungsebene: Unified Zero Trust

MANAGEMENT UND BEREITSTELLUNG

- Management: Zentrale Konsole der WatchGuard Cloud für Konfiguration, Richtlinienvorlagen und Funktionen für mandantenfähige Service Provider
- Points-of-Presence: Globales Netzwerk auf fünf Kontinenten

> Funktionsweise

Authentifizieren > Validieren > Durchsetzen

- **AuthPoint** überprüft die Benutzeridentität und bewertet das Risiko bei jeder neuen Sitzung.
- **Endpoint-Sicherheit** überprüft den Gerätezustand und die Konformität in Echtzeit.
- **FireCloud** wendet Zero-Trust-Richtlinien an, um den Zugriff auf Web, SaaS und private Apps zu regeln.
- **Das Zero Trust Identity Framework** vereint Identitäts-, Geräte- und Zugriffsverifizierung in einem kontinuierlichen Prozess.
- **ThreatSync XDR** korreliert alle Aktivitäten für ununterbrochene Transparenz, Erkennung und automatisierte Reaktion.
- **WatchGuard Cloud** bietet ein einheitliches Management für alle Dienste und vereinfacht die Erstellung und Bereitstellung von Richtlinien sowie Berichterstellung über eine einzige, mandantenfähige Konsole.

Möchten Sie mehr über das Zero Trust Bundle erfahren?

Weitere Informationen erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter www.watchguard.com/de

Informationen zu WatchGuard

WatchGuard® Technologies gehört zu den weltweit führenden Anbietern im Bereich Cybersicherheit für Managed Service Provider. Im Gegensatz zu anderen Anbietern bietet WatchGuard über seine Unified Security Platform® *echte Sicherheit für reale Umgebungen*. Auf der Grundlage von künstlicher Intelligenz und Zero-Trust-Ansätzen bietet das Unternehmen starken und skalierbaren Schutz für Netzwerke, Endpoints und Identitäten. WatchGuard genießt das Vertrauen von mehr als 17.000 Vertriebspartnern und Managed Service Providern, die über 250.000 Unternehmen schützen. Das Unternehmen hilft Partnern, schnell zu wachsen, betriebliche Belastungen zu beseitigen und starke Ergebnisse zu erzielen – ohne zusätzliche Anbieter, Konsolen oder Komplexität. WatchGuard hat seinen Hauptsitz in Seattle, Washington, und unterhält Niederlassungen weltweit. Weitere Informationen finden Sie unter WatchGuard.com/de.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.com/de WatchGuard Technologies, Inc.