

Schweizerischer IT-Dienstleister schützt neue Rechenzentren mit Check Point und erfüllt strenge SLAs seiner Kunden

Check Point Next Generation Security Gateway ermöglicht es der Wagner AG mit fortschrittlichem Netzwerkschutz und zentralisiertem Sicherheitsmanagement, Kunden-Workloads über mehrere Standorte zu verteilen



Kundenprofil

Die Wagner AG ist ein schweizerischer IT-Dienstleister, der sich auf Outsourcing und Beratungsdienstleistungen spezialisiert hat.

Herausforderung

- Stärkung der Sicherheit in zwei verbundenen Rechenzentren
- Bessere Sichtbarkeit der Bedrohungslandschaft mit konsolidierter Überwachung und granulearem Reporting
- Einfaches Kundenmanagement und Geschäftskontinuität für die Kunden

Lösung

- Check Point Next Generation Security Gateway
- Check Point R80.10 Security Management

Vorteile

- Fortschrittlicher Schutz und Gefahrenerkennung durch Identifizieren von Cyberangriffen im Anfangsstadium
- Mögliche Skalierung für Wachstum der Managed Services an beiden Standorten
- Sichere Verteilung der Kunden-Workloads auf zwei Rechenzentren

„Am meisten schätzen wir an der R80 Lösung die klare und einfache Verwaltung unserer Richtlinien. Die gleichzeitige Richtlinienverwaltung für mehrere Benutzer macht den Arbeitsalltag wesentlich einfacher.“

— Thomas Eltschinger, Leiter für Managed Backend Services, Wagner AG

Überblick

Wagner AG

Die Wagner AG ist ein schweizerischer IT-Dienstleister mit Kunden in verschiedenen Marktsegmenten, darunter Finanzen, Lebensmittel und Gesundheitswesen. Das Unternehmen wurde 1996 gegründet und hat derzeit über 100 Mitarbeiter.

Business-Herausforderungen

Aufbau einer auf Wachstum ausgelegten Infrastruktur

Die Wagner AG bieten ihren schweizerischen Kunden Managed IT-Services an. Da immer mehr Unternehmen ihre IT an einen Spezialisten outsourcen möchten, um die Verwaltung zu vereinfachen und Kosten zu stabilisieren, hat die Wagner AG Pläne für

zwei neue Rechenzentren entworfen, die sich 120 km voneinander entfernt befinden und über zwei 40-Gbits-Verbindungen verfügen. Diese Investition sollte Raum für mehr Wachstum schaffen und mehr Redundanz bieten.



„Die Cluster-Funktion der Check Point Lösung funktioniert sehr gut mit anderen Netzwerkkomponenten. Das ist definitiv ein Vorteil.“

– Thomas Eltschinger,
Leiter für Managed Backend
Services, Wagner AG

„Das war eine beträchtliche strategische Investition in ein System, das wir von Grund auf neu aufgebaut haben“, erzählt Thomas Eltschinger, Leiter der Managed Backend Services, Wagner AG. „Wir wollten neueste Technologien verwenden. Da wir Managed Services mit sehr strengen SLAs anbieten, benötigten wir an beiden Standorten Cluster-Firewalls.“

Wir möchten unseren Kunden den bestmöglichen Schutz mit den modernen Optionen von heute bieten. Und das können wir mit den unterschiedlichen Blades und dem flexiblen Lizenzmodell von Check Point definitiv tun.“

Lösung

Maximale Betriebszeit mit fortschrittlichem Schutz

Das Check Point Next Generation Security Gateway kombiniert umfassenden Schutz mit Rechenzentrums-Hardware und liefert so maximale Betriebszeiten und den optimalen Schutz der Unternehmens- und Rechenzentrumsnetzwerke. Die Lösung bietet leistungsstarken Schutz vor hochmodernen Cyberangriffen.

Eltschinger betont, dass die Features der Check Point Lösung einfach am besten passten und es dem Unternehmen nun ermöglichen, die höchsten Industriestandards in Sachen Sicherheit und Rückverfolgbarkeit einzuhalten. Das Check Point Next Generation Security Gateway bietet eine einzigartige „Erstangriff-Abwehr“ der ausgeklügeltsten Zero-Day-Angriffe von heute. Es prüft auch SSL-verschlüsselten Datenverkehr und verbessert durch die zentralisierte Verwaltung und das Lights Out Management (LOM) die Wartbarkeit. Zudem ist es modular und kann so jederzeit erweitert werden.

Zusätzlich bietet das Check Point R80.10 Security Management vollständig integrierte Sichtbarkeit und gut verständlichen Sicherheitsinformationen. Mit der R80.10 SmartConsole kann die Wagner AG einheitliche Richtlinien für alle Netzwerke und Cloudumgebungen erstellen und zentral verwalten.

„Die Automatisierung und die API-Optionen sind nützliche Features“, bestätigt Eltschinger. „Wir standardisieren unsere Kundenumgebungen, wodurch die vorhandene API immer wichtiger für die Automatisierung wird. Das wiederum senkt die Gesamtbetriebskosten.“



„Die Dokumentation und Sicherheitsinformationen auf der Check Point Webseite sind ausgezeichnet. Es war ganz einfach, Antworten auf technische Fragen zu finden.“

– Thomas Eltschinger,
Leiter für Managed Backend
Services, Wagner AG

Vorteile

Skalieren für wenig Latenz und absolute Redundanz

„Die Implementierung verlief problemlos. Wir haben uns für die manuelle Variante entschieden, um unsere alten Regeln durchzugehen, neue zu erstellen und generell aufzuräumen. Wir wollten keine ungewünschten Sicherheitsregeln von alten Geräten übernehmen“, meint Eltschinger.

Er erzählt weiter, dass die Implementierung mit dem Check Point Partner BNC Business Network Communications AG, stattfand und alle Probleme schnell gelöst wurden: „Die Dokumentation und Sicherheitsinformationen auf der Check Point Webseite sind ausgezeichnet. Es war ganz einfach, Antworten auf technische Fragen zu finden.“

Heute beherbergen die beiden Rechenzentren etwa 50 Kunden der Wagner AG mit bis zu 3.000 Benutzern und 5.000 unterschiedlichen Firewall-Objekten. „Da diese Objekte an beiden Standorten laufen können, können wir die Last gleichmässig verteilen. Wir können die Kunden nach ihrer geografischen Lage verbinden, behalten aber eine niedrige Latenz und absolute Redundanz bei“, erklärt Eltschinger weiter. „Die Cluster- Funktion der Check Point Lösung funktioniert sehr gut mit anderen Netzwerkkomponenten. Das ist definitiv ein Vorteil. Am meisten schätzen wir an der R80 Lösung jedoch die klare und einfache Verwaltung unserer Richtlinien. Die gleichzeitige Richtlinienverwaltung für mehrere Benutzer macht den Arbeitsalltag wesentlich einfacher.“

„Das Feedback unserer Kunden“, fügt er hinzu, „war sehr positiv. Im Gegensatz zur alten Lösung läuft alles glatt.“

Eltschinger erzählt auch von Wagners Plänen, Ende 2018 SandBlast™ Threat Emulation und Threat Extraction einzuführen.

„Unser Ziel ist es, jegliche Malware im Netzwerk zu eliminieren, nichts ungehindert ins Netzwerk zu lassen und Probleme so früh wie möglich zu erkennen. Und Check Point SandBlast bietet genau das.“

Für weitere Informationen besuchen Sie:
<https://www.checkpoint.com/products/sandblast-network-security/>

