voices

CrowdStrike Customer Case Study

Führender Technologie-Distributor setzt auf umfassende IT-Security für die Bedrohungslandschaft von heute und morgen

Als einer der führenden Technologie-Distributoren weltweit unterstützt Tech Data zahlreiche Konzerne und Unternehmen dabei, ihre Produkte auf den Markt zu bringen. Zudem bietet Tech Data ein breites Spektrum an technischen und geschäftlichen Unterstützungsleistungen an. Dazu zählen Zertifizierungen, Schulungen, Instruktion und Unterstützung der Vertriebspartner. Auch hilft Tech Data bei der Konfiguration, Installation und Finanzierung.

Exponierte Position bedingt hohe Ansprüche an die IT-Security

In einer derartig großen und breit aufgestellten Organisation spielt die Cybersicherheit seit jeher eine tragende Rolle für Tech Data, um sich selbst, aber auch Partner- und Kundendaten zu schützen. Daher ist es für Tech Data unerlässlich, das Thema IT-Sicherheit ernst zu nehmen und über die neuesten Entwicklungen in diesem Bereich informiert zu sein. Deshalb behielt das Unternehmen auch den Markt für Next Gen AV-Lösungen im Blick, da über kurz oder lang die bis dato eingesetzte, signaturbasierte Endpoint Security-Lösung aufgrund der sich immer stärker verändernden Bedrohungslandschaft ersetzt werden sollte. Ein ambitioniertes Vorhaben in einer über den gesamten Globus verteilten Firma mit sehr heterogenen Systemen.

Veraltete Systeme bieten keinen Schutz gegen moderne Attacken

Die Entscheidung für den Austausch des bisher eingesetzten Produkts fiel, nachdem dieses zunehmend Probleme aufwies, die Tech Data nicht weiter ignorieren konnte. Der Support wurde schwächer, es wurde keine Innovation mehr gezeigt, der Schutzeffekt des Produkts ließ zunehmend nach und die Kernfunktion Detection and Response fehlte vollständig. Eine neue Lösung war gefordert: Auf dem Prüfstand standen verschiedene Anbieter, unter denen sich am Ende CrowdStrike mit seiner umfassenden Endgeräte- und Workload-Schutz-Lösung erfolgreich durchsetzte. Überzeugt waren Jürgen Streit, Global Director of Information Security bei Tech Data, und sein Team vor allem von der robusten End-to-End-Lösung, der Kompetenz von CrowdStrike im Bereich Incident Response, das Angebot des 24/7 CrowdStrike Falcon Overwatch™ Managed Hunting-Services sowie dem einfachen Handling der Lösung auch über unterschiedliche Betriebssysteme hinweg.

„Gerade in der heutigen Zeit ist es uns in der IT-Sicherheit extrem wichtig, dass man betriebssystemunabhängig eine vollständige Sichtbarkeit über alle Workloads der Firma hat und schnell auf potenzielle Gefahren reagieren kann, um trotz stetig wachsender Angriffsfläche optimal geschützt zu sein. Die Lösung von CrowdStrike bietet uns diese so wichtige Sichtbarkeit und gibt uns zugleich weitere Tools an die Hand, die problemlos remote funktionieren, wie beispielsweise die Endpoint-Isolation und auch forensische Untersuchungen“, erläutert Jürgen Streit.

BRANCHE

IT

STANDORT/ KONZERNZENTRALE

Clearwater, Florida, USA

HERAUSFORDERUNGEN

- Ablösung des eines alten Antivirenprogramms durch eine Lösung der neuesten Generation
- Weltweit verteilte Corporation mit sehr heterogenen Systemen
- Stark vergrößerte Angriffsfläche durch massives Wachstum

LÖSUNG

Die CrowdStrike Falcon® Plattform bietet Tech Data zusammen mit dem CrowdStrike Falcon Overwatch™-Team eine umfassende IT-Sicherheits-lösung, die weniger Verwaltungs-aufwand für die IT bedeutet und auf die Herausforderungen einer modernen Bedrohungslandschaft hin optimiert ist.

“Wir haben Angriffsversuche erkennen können, die wir vorher nicht mitbekommen hätten”

Jürgen Streit,
Global Director of Information Security , Tech Data

voices

CrowdStrike Customer Case Study

Ohne Datenschutz geht nichts

Ein weiterer entscheidender Punkt für Tech Data war das Thema Datenschutz. Gerade in Europa und Ländern mit hohen Datenschutzvorgaben machte man sich Gedanken wegen der tiefgreifenden Analysefähigkeiten des CrowdStrike Falcon®-Agenten. CrowdStrike konnte hier jedoch nicht nur fundiert alle Bedenken mühelos zerstreuen, sondern lieferte Tech Data auch alle erforderlichen Sicherheitsunterlagen und Anleitungen wie beispielsweise Datenverarbeitungsauswirkungs-analysen, Vorlagen für Datenverarbeitungsvereinbarungen sowie das SOC 2-Zertifikat, die alle für die internen Genehmigung und für die Betriebsvereinbarung benötigt wurden.

Reibungslose Implementierung trotz komplexer Strukturen

Zuerst musste die CrowdStrike®-Lösung im Proof of Value überzeugen. Dabei wurde sie innerhalb einer Pilotgruppe ausgerollt und anschließend vom Engineering-Team über mehrere Wochen hinweg auf Herz und Nieren geprüft. Dabei wurden verschiedenste Testfälle ebenso durchgespielt wie der Migrationsprozess. Nachdem all diese Tests positiv ausgefallen waren, war die Entscheidung für CrowdStrike gefallen und der Rollout konnte beginnen.

Da Tech Data weltweit über gut ein Dutzend interne Rechenzentren und unterschiedliche Cloud-Umgebungen verfügt, gab es auch verschiedene Teams, die ohne einen global einheitlichen Verteilungsprozess an diesem Rollout beteiligt waren. Trotz dieser komplexen Situation konnte die CrowdStrike-Lösung innerhalb von acht Wochen auf die ca. 22.000 Endgeräte des Unternehmens ausgerollt werden.

„Dadurch, dass wir unabhängig von der vorhandenen AV-Lösung den Agenten von CrowdStrike ohne Reboot und ohne jeden Endpoint manuell konfigurieren zu müssen, ausrollen konnten, verlief dieser Rollout sehr schnell und problemlos," so Jürgen Streit.

ERGEBNISSE

Geschätzte 30% Zeitersparnis bei der Verwaltung der IT-Sicherheit

Verbesserte Optionen für Threat Hunting und Risikomanagement

Betriebssystem-unabhängige Transparenz und standortunabhängige Reaktions-möglichkeiten

ENDPUNKTE

CROWDSTRIKE-PRODUKTE

- Falcon Prevent™ Virenschutz der neuesten Generation
- Falcon Insight™ Endgeräteerkennung und Abwehr
- Falcon OverWatch™ Managed Threat Hunting
- Falcon X™
- Falcon Spotlight™

voices

CrowdStrike Customer Case Study

Falcon im Einsatz

Die neue Lösung bietet Möglichkeiten, die Tech Data in diesem Umfang vorher nicht zur Verfügung standen. So konnte das Unternehmen bereits von verschiedenen Benachrichtigungen des Managed-Hunting-Services Falcon OverWatch profitieren, indem es beispielsweise schon sehr früh vor bestimmten Angriffswellen gewarnt wurde, die CrowdStrike im Netz beobachten konnte. Tech Data ist damit in der Lage, schnell auf aufkommende, verdeckte Angriffe zu reagieren und mit den entscheidenden Informationen und Indikatoren ausgestattet, die sie benötigen, um entschlossen zu handeln und ihre Verteidigung gegen den nächsten potenziellen Angriff proaktiv zu verbessern.

Darüber hinaus konnte durch die Integration der CrowdStrike Falcon Plattform in die bestehende SOAR-Lösung von Tech Data auch das interne Cyber Defense Center massiv entlastet werden. „Wir haben zahlreiche teilautomatisierte und vollautomatisierte Response Use Cases implementiert. So konnten wir unsere Spezialisten entlasten“, so Streit weiter.

Basierend auf dem Know-how und der Erfahrung von CrowdStrike im Incident Response-Bereich, gibt es bei Tech Data hier bereits Pläne, die bereits implementierte Lösung um CrowdStrike® Incident Response (IR) als Service zu erweitern.

„Da wir CrowdStrike bereits auf all unseren Endgeräten im Einsatz haben, würden wir uns bei einem Incident Response-Vorfall das Ausrollen des Agenten sparen und könnten so wertvolle Zeit gewinnen“, ergänzt Streit.

Tech Data blickt mit CrowdStrike gut gerüstet in die Zukunft

Heute verfügt Tech Data über eine umfassende IT-Sicherheitslösung, die nicht nur weniger Verwaltungsaufwand von Seiten der Security-Spezialisten erfordert, sondern auch auf die Bedürfnisse und Herausforderungen hin optimiert ist, die in einer modernen Bedrohungslandschaft bestehen. Streits Resümee: „Wir haben mit dieser Lösung einen großen Schritt in Richtung Maturity gemacht.“

CROWDSTRIKE

Erfahren Sie mehr unter **www.crowdstrike.de**

we stop breaches