ANWENDERBERICHT

Neugestaltung des Endgeräteschutzes unterstützt Innovation und stärkt die Sicherheit

Innovatives, weltweit tätiges Unternehmen für die Transformation von Geschäftsprozessen transformiert seine eigenen Sicherheitsprozesse mit McAfee

Sutherland Global Services

Kundenprofil
Internationales Unternehmen für die Transformation von Geschäftsprozessen

Branche
Technologie und geschäftliche Dienstleistungen

IT-Umgebung
Ca. 50.000 Endgeräte in 16 Ländern auf sechs Kontinenten

Sutherland Global Services unterstützt 100 *Fortune 1000*-Unternehmen in 16 Ländern bei der Neukonzeption und Neuaufstellung von Geschäftsprozessen für das digitale Zeitalter. Dabei setzt Sutherland Global Services auf Datenanalysen und weitere Technologien, Design-Expertise branchenspezifische Kompetenzen. Das in Pittsford, New York, angesiedelte Unternehmen investierte in die Transformation seiner eigenen Endgerätesicherheit und konnte dadurch seine allgemeine Sicherheitsaufstellung erheblich verbessern. Gleichzeitig erreichte es auf diese Weise eine deutliche Senkung des Zeit- und Kostenaufwands. Durch die Nutzung von Open Data Exchange Layer (OpenDXL) baute Sutherland Global Services eine einheitliche Schutzstruktur auf, in der unterschiedliche Sicherheitssysteme interagieren und einander verstärken können.

Folgen Sie uns

Verhinderung von Geschäftsunterbrechungen und Sicherheitsverletzungen

„Jede Minute, in der das System eines geschäftlichen Benutzers nicht verfügbar ist, kostet uns viel Geld", erklärt Prashanth M. J., Global Head of Technology Infrastructure bei Sutherland Global Services. „Geschäftsunterbrechungen und Datenschutzverstöße sind eine reale Gefahr, vor der wir uns schützen möchten. Der ordnungsgemäße Betrieb der notwendigen Kontrollen steht für uns an erster Stelle, damit diese Risiken minimiert werden und wir unseren Kunden auch weiterhin innovative, maßgeschneiderte Lösungen und Services bereitstellen können."

Angesichts von 50.000 zu schützenden Nodes, darunter 1.000 Servern, mehr als 80 Rechenzentren und Bereitstellungszentren sowie einem digitalen Backbone in 16 Ländern und auf sechs Kontinenten, ist die Abwehr von Sicherheitsrisiken eine Mammutaufgabe, die den Einsatz zahlreicher Sicherheitslösungen erfordert. Für das Team, das für die Technologieinfrastruktur verantwortlich zeichnet, ist es alles andere als einfach, Kommunikation und Austausch von Sicherheitsdaten zwischen den unterschiedlichen Systemen und Kontrollen zu gewährleisten. Gleichzeitig lässt sich nur auf diese Weise das gesamte erweiterte Unternehmen schützen.

Unverzichtbar: Strategische Partner, die Innovation unterstützen

Ein so weit verzweigtes Unternehmen wie Sutherland Global Services ist auf die Unterstützung strategischer Partner wie McAfee angewiesen. „Wir haben großes Vertrauen in McAfee, da McAfee stets unsere geschäftlichen Anforderungen erfüllt hat – wozu auch ständige Innovationen gehören", betont Prashanth. „Und genau diese Innovationen sind es, die unser Unternehmen voranbringen."

„Unsere Services verbinden innovative Geschäftsabläufe sowie Technologien und transformieren Prozesse, um die Ziele unserer Kunden zu realisieren", fährt Prashanth fort. „McAfee führt kontinuierlich Lösungen ein, die unsere geschäftlichen Anforderungen direkt erfüllen. Dazu gehören beispielsweise das Schließen der Lücke zwischen Erkennung und Behebung oder die Ermittlung des Fortschritts unserer digitalen Transformation."

Implementierung einheitlicher Schutzmaßnahmen mit OpenDXL

Prashanth zeigt sich auch von OpenDXL begeistert. Mit dieser von McAfee entwickelten Technologie lassen sich Systeme aus vernetzten Lösungen erstellen, die in Echtzeit Informationen austauschen, um zuverlässige Sicherheitsentscheidungen zu ermöglichen. Mithilfe von OpenDXL integriert Sutherland Global Services gerade die McAfee-externe SIEM-Lösung (Sicherheitsinformations- und Ereignis-Management) in den McAfee-Endgeräteschutz. Auch die Integration in das unternehmenseigene Web-Gateway und die Firewall stehen auf dem OpenDXL-Fahrplan von Sutherland.

„Ich sehe enormes Potenzial bei OpenDXL", betont Prashanth. „Wir nutzen zahlreiche Sicherheitsprodukte verschiedener Hersteller, die jeweils isoliert agieren. Für einheitlichen Schutz vor Cyber-Angriffen müssen die Bedrohungsdaten eines Systems von anderen Systemen genutzt werden können."

Herausforderungen

- Permanente Verfügbarkeit für weltweite Unternehmensnutzer
- Integration von Sicherheitslösungen für einheitliche Cyber-Sicherheitsmaßnahmen
- Effiziente Einhaltung von Vorschriften insbesondere im Gesundheits- und Finanzwesen

McAfee-Lösungen

- McAfee® Advanced Threat Defense
- McAfee® DLP Endpoint
- McAfee® Endpoint Encryption
- McAfee® Endpoint Security
- McAfee® Endpoint Threat Defense and Response
- McAfee® ePolicy Orchestrator®
- McAfee® File Integrity Monitoring
- McAfee® Professional Services
- McAfee® Threat Intelligence Exchange

Konsolidierung des Endgeräteschutzes senkt Kosten und steigert Möglichkeiten zur Umsatzgenerierung

Für den Schutz seiner weltweit verteilten Endgeräte setzt Sutherland Global Services stark auf die zentrale Verwaltungskonsole McAfee ePolicy Orchestrator (McAfee ePO™). Mithilfe von McAfee ePO können Administratoren mehrere McAfee-Produkte und -Sicherheitsfunktionen – Virenschutz, Datenkompromittierungs- und Eindringungsschutz für Hosts, Endgeräte-Verschlüsselung, Dateiintegritätsüberwachung usw. – auf einer zentralen Benutzeroberfläche verwalten.

„[Die Software] McAfee ePO bietet uns einen Vorteil bei der nahtlosen Verwaltung unseres weltweiten Unternehmens“, erläutert Prashanth. „Sie ist auch so benutzerfreundlich, dass ich keine teuren Level-2- oder Level-3-Sicherheitstechniker einsetzen muss.“

In den letzten zwei Jahren konsolidierte das Unternehmen im Rahmen einer vollständigen Aktualisierung und Transformation seines Endgeräteschutzes sieben weltweit verteilte McAfee ePO-Server zu einem. Heute wird der Schutz aller ca. 50.000 Endgeräte über die zentrale McAfee ePO-Konsole im Sicherheitskontrollzentrum (SOC) des Unternehmens verwaltet.

„Als wir die anderen sechs McAfee ePO-Server stilllegten, profitierten wir sofort von den Kosteneinsparungen“, erinnert sich Prashanth. „Neben den Hardware- und Software-Kosten verringerte sich auch der Stromverbrauch im Rechenzentrum sowie der Zeitaufwand für Wartung und Verwaltung. Wir konnten auch ohne zusätzliche Mitarbeiter neue Funktionen implementieren sowie Mitarbeiter für wichtigere Aufgaben freistellen.“

„Desweiteren steigerte die Überholung des Endgeräteschutzes die unternehmensweite Systemverfügbarkeit“, fügt Prashanth hinzu. „Und durch die höhere Verfügbarkeit gewannen wir auch mehr Möglichkeiten, zusätzliche Umsätze zu generieren.“

Schnelle und einfache Compliance-Berichte steigern die Compliance-Einhaltung auf über 95 %

Die Konsolidierung auf eine zentrale Konsole ermöglichte enorme Zeitersparnisse im Compliance-Bereich, insbesondere im Gesundheitswesen und der Finanzdienstleistungsbranche. „Mit einer zentralen Konsole ist die Compliance-Berichterstellung jetzt erheblich effizienter“, bestätigt Prashanth. „Wir können schnell und einfach Dashboards bereitstellen, die für die Sicherheitsbetreiber unterschiedlicher Regionen, Kunden oder Branchen angepasst und kontextualisiert sind. Aus diesem Grund lassen sich die benötigten Berichte erheblich leichter erzeugen, und unsere Compliance-Einhaltung ist auf über 95 % gestiegen.“

Ergebnisse

- Reduzierter Verwaltungsaufwand sowie geringere Hardware- und Software-Kosten
- Verbesserte Systemverfügbarkeit
- Mehr Möglichkeiten zur Umsatzgenerierung
- Einfachere Verwaltung des Endgeräteschutzes, sodass Administratoren weltweit entlastet werden
- Stärkerer mehrschichtiger Schutz vor Malware einschließlich Zero-Day-Bedrohungen
- Erheblich effizientere Compliance-Berichterstattung weltweit
- Compliance-Einhaltung auf mehr als 95 % gesteigert
- Schnellere Erkennung und Abwehr von Bedrohungen

Mehrschichtiger Schutz mit Austausch von Bedrohungsdaten stärkt die Abwehr von Zero-Day-Bedrohungen

Die Migration von McAfee® VirusScan® Enterprise zu McAfee Endpoint Security war ein weiterer wichtiger Schritt bei der Neuaufstellung des unternehmensweiten Endgeräteschutzes. „Wir suchten nach einer zuverlässigen Malware-Schutzlösung der nächsten Generation mit zusätzlichen Schutzebenen. Zum Glück bietet McAfee alles, was wir brauchten", erklärt Prashanth. „Wir wollten insbesondere die dynamische Eindämmung von Anwendungsprozessen einsetzen, um unbekannte Dateien zu isolieren, und mit der Machine Learning-Funktion Real Protect verdächtige Dateien im laufenden Betrieb analysieren."

Das Unternehmen wechselte auch zu McAfee Endpoint Security, um McAfee Threat Intelligence Exchange nutzen zu können. Hier werden permanent aktualisierte weltweite und lokale Bedrohungsdaten erfasst und bidirektional über den Data Exchange Layer (DXL) mit allen damit verbundenen Systemen geteilt. McAfee Endpoint Security verbindet sich standardmäßig mit dem DXL. „Wenn also eines unserer Endgeräte eine böswillige Datei findet oder ein weltweites Forschungszentrum eine neue Zero-Day-Bedrohung entdeckt, müssen unsere Endgeräte nicht mehr darauf warten, dass Signaturen verfügbar und von einem Administrator ausgebracht werden – sie erhalten sie sofort und automatisch", erklärt Prashanth.

Sutherland Global Services engagierte McAfee Professional Services für eine reibungslose und stufenweise Migration zu McAfee Endpoint Security, die ohne die Beeinträchtigung der Systemverfügbarkeit geschäftlicher Benutzer weltweit vonstatten ging. Die Migration für alle Endgeräte zu McAfee Endpoint Security umfasste das Advanced Threat Protection-Modul mit der dynamischen Eindämmung von Anwendungsprozessen und Real Protect. Das Unternehmen stellte auch die DXL-Struktur sowie McAfee Threat Intelligence Exchange in seinem gesamten Netzwerk bereit.

Schnellere Reaktion auf Zwischenfälle

Im Rahmen der Endgeräteschutz-Transformation implementierte Sutherland Global Services auch eine McAfee Advanced Threat Defense-Appliance zur dynamischen und statischen Sandbox-Analyse. „Dabei hilft uns McAfee Advanced Threat Defense auf zwei Weisen", erklärt Prashanth. „Erstens, wenn unsere Endgeräte eine unbekannte Datei entdecken und sie isolieren, wird sie direkt an die McAfee-Appliance zur detaillierten Analyse gesendet. Im Anschluss wird das Ergebnis [über McAfee Threat Intelligence Exchange] an das gesamte Unternehmen weitergegeben. Auf diese Weise haben wir eine Menge böswilliger Dateien erkannt und alle unsere Endgeräte proaktiv geschützt."

„Unsere Services verbinden innovative Geschäftsabläufe sowie Technologien und transformieren Prozesse, um die Ziele unserer Kunden zu realisieren. McAfee führt kontinuierlich Lösungen ein, die unsere geschäftlichen Anforderungen direkt erfüllen. Dazu gehören beispielsweise das Schließen der Lücke zwischen Erkennung und Behebung oder die weitere Umsetzung unserer digitalen Transformation."

– Prashanth M. J., Senior Vice President, Global Head of Technology Infrastructure bei Sutherland Global Services

„Zweitens beschleunigt McAfee Advanced Threat Defense unseren Untersuchungsprozess anhand von Kompromittierungsindikatoren“, fährt Prashanth fort. „Früher mussten wir bei jedem unbekannten Kompromittierungsindikator einen Hash-Wert an den McAfee-Support senden und auf Rückmeldung warten, ob er böswillig ist. Mit McAfee Advanced Threat Defense können wir jetzt den Kompromittierungsindikator selbst analysieren und schneller feststellen, welche Maßnahmen ergriffen werden müssen.“

Außerdem ist das Unternehmen gerade dabei, McAfee Endpoint Threat Defense and Response zu integrieren, um effektiver proaktiv nach Bedrohungen zu suchen. „Wir möchten offensiver und nicht nur defensiv vorgehen“, betont Prashanth. „Ich gehe davon aus, dass McAfee Endpoint Threat Defense and Response eines der wichtigsten Tools in unserem Arsenal wird, wenn es um den Schutz vor inaktiven Bedrohungen geht, die in unserer Umgebung nur auf den richtigen Auslöser warten… Letztendlich geht es um Reaktionsgeschwindigkeit. Die richtigen Maßnahmen sind sinnlos, wenn die Reaktion nicht schnell genug erfolgt.“

Größere Zukunftssicherheit hängt nicht nur von Produkten ab

„Unsere Partnerschaft mit McAfee war bisher außerordentlich erfolgreich. Ich kann darauf vertrauen, dass unsere Systeme geschützt und zukunftssicher sind“, betont Doug Gilbert, CIO und Chief Digital Officer bei Sutherland Global Services. „Bei der Entscheidung für einen Partner geht es nicht nur um einzelne Produkte, sondern das ganze Ökosystem. Mit McAfee haben wir Menschen, die zu uns stehen – und nicht nur Produkte verkaufen, sondern uns dabei unterstützen, sie zu konzipieren, bereitzustellen, zu warten und zu optimieren."

Zukünftig will Sutherland Global Services stärker auf die Cloud setzen und die bereits begonnene digitale Transformation weiter ausbauen. McAfee wird dabei eine zentrale Rolle spielen. Prashanth erwähnt dabei die neuen McAfee® MVISION-Produkte als weiteres Beispiel für Innovationen, die sein Unternehmen dabei unterstützen werden: „Die Bedrohungslage ist so komplex, dass enge Zusammenarbeit unerlässlich ist. McAfee stellt uns die [richtige] Technologie bereit, während wir das geschäftliche Fachwissen einbringen. ‚Together is Power‘ ist der richtige Ansatz für die Zukunft.“

„Unsere Partnerschaft mit McAfee war bisher außerordentlich erfolgreich. Ich kann darauf vertrauen, dass unsere Systeme geschützt und zukunftssicher sind. Bei der Entscheidung für einen Partner geht es nicht nur um einzelne Produkte, sondern das ganze Ökosystem. Mit McAfee haben wir Menschen, die zu uns stehen – und nicht nur Produkte verkaufen, sondern uns dabei unterstützen, sie zu konzipieren, bereitzustellen, zu warten und zu optimieren."

– Doug Gilbert, CIO und Chief Digital Officer bei Sutherland Global Services

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de