r tec
cyber security

MCAFEE, TRELLIX & SKYHIGH

Trellix und Skyhigh übernehmen das McAfee-Enterprise-Portfolio: Was Kunden jetzt wissen sollten

Trellix und Skyhigh übernehmen das McAfee-Enterprise-Portfolio: Was Kunden jetzt wissen sollten

Das Portfolio des IT-Security-Lösungsanbieters McAfee Enterprise wird aufgeteilt und zukünftig von den Softwareherstellern Trellix und Skyhigh in veränderter Form weitergeführt. Zahlreiche McAfee-Kunden stehen nun vor der Frage, welche Folgen die Sortimentsaufteilung für ihre IT-Sicherheit hat. Um betroffenen Unternehmen und Organisationen eine Antwort zu liefern, haben die Experten der r-tec IT Security GmbH das vorliegende Informationsdokument erstellt. Die folgenden Ausführungen zeigen auf, ob und in welchen Bereichen Handlungsbedarf entsteht, welche Chancen und Möglichkeiten sich ergeben und welche Vorteile ehemalige McAfee-Kunden bereits heute nutzen sollten.

Wie wird das bestehende Portfolio aufgeteilt?

Um darzulegen, welche Veränderungen sich in Zukunft für Nutzer der bisherigen McAfee-Lösungen ergeben, müssen wir uns zunächst vergegenwärtigen, wie das bestehende Portfolio aufgeteilt wird.

Dafür werfen wir zuerst einen Blick auf Skyhigh Security: Der Hersteller übernimmt schwerpunktmäßig McAfee-Technologien, die in den Bereichen Web- und Cloud-Nutzung eingesetzt werden. Dazu gehören unter anderem die Lösungen Web Gateway, Web Gateway Cloud Service, MVISION Unified Cloud Edge, Cloud Access Security Broker (CASB) und Remote Browser Isolation (RBI).

Skyhigh kombiniert diese Lösungen mit Technologien, die in der Vergangenheit von Skyhigh Networks, NanoSec, Light Point Security und Secure Computing erworben wurden. Ziel ist es, den wachsenden Anforderungen an die Cloud-Sicherheit gerecht zu werden. Entstanden ist ein Portfolio, das auf den Schutz aller Daten, Geräte, Benutzer, Anwendungen und Cloud-Dienste, die sich außerhalb der traditionellen Netzwerkgrenzen befinden, ausgelegt ist.

Es umfasst folgende Produkte:

- Skyhigh Cloud Access Security Broker
- Skyhigh Secure Web Gateway
- Skyhigh Private Access
- Skyhigh Cloud-Native Application Protection Platform

Alle Lösungen können in der Skyhigh-Cloud betrieben werden. Dies gilt sowohl für Komponenten, die auf den Schutz von Cloud-Umgebungen abzielen, als auch für Komponenten die On-Premise- oder mobile Systeme schützen.

McAfee, Trellix & Skyhigh

Der andere Teil des McAfee-Portfolios, der hauptsächlich Lösungen für den Bereich Extended Detection and Response (XDR) enthält, wird von Trellix übernommen. Der Softwarehersteller vereint die Technologien der Unternehmen McAfee und FireEye, um ein umfassendes XDR-Ökosystem zu schaffen. Es enthält alle wichtigen Sicherheitskomponenten, die benötigt werden, um Unternehmen vor Cyberbedrohungen zu schützen.

Das Portfolio beinhaltet die folgenden Komponenten:

- Trellix XDR Platform
- Endpoint Protection
- SecOps and Analytics
- Data Protection
- Network Security
- Email Security
- Cloud Security

Was bedeutet die Aufteilung für Bestandskunden?

Beide Hersteller führen die McAfee-Lösungen, die derzeit noch von Kunden genutzt werden, weiter. Dies gilt für folgende Produktlinien:

- Endpoint Protection
- Web Gateway
- Security Information and Event Management (SIEM)

Die r-tec IT Security GmbH wird diese Lösungen auch weiterhin im Rahmen ihrer Managed-Service-Modelle fortführen.

Bei der Trellix Endpoint Protection wird eine schrittweise Verschmelzung mit dem FireEye-Agenten und den Helix-Funktionen angestrebt. Die bekannten Endpoint-Security-Funktionen sowie die Verwaltung per ePO bleiben erhalten und werden weiterentwickelt. Es ist anzunehmen, dass die bisherige McAfee-EDR-Plattform jedoch mittelfristig der auf Helix basierenden XDR weichen muss. Ob die Advanced Threat Detection von McAfee – eine On-Premise-Sandboxing-Lösung – langfristig fortgeführt wird, ist derzeit noch nicht bekannt. Trellix hat den Support und die Weiterentwicklung aber bis auf Weiteres zugesichert.

Wie es mit dem bisherigen McAfee-SIEM weitergeht, ist ebenfalls noch nicht sicher. Es gibt jedoch klare Anzeichen, dass der Bestand erhalten bleibt und Support gewährleistet ist. Allerdings wird Trellix aus strategischen Gründen sicherlich auf die innovative Helix-basierte Plattform setzen und keine Innovationsleistungen mehr in die Weiterentwicklung der alten SIEM-Plattform investieren.

Skyhigh führt das Secure Web Gateway als Cloud- sowie als On-Premise-Lösung fort und ergänzt es um Funktionen aus seinem weiteren Portfolio. So profitieren Secure-Web-Gateway-Anwender heute schon von der Integration der Remote Browser Isolation.

Wie sieht die Roadmap der beiden Hersteller aus?

Beide Hersteller haben sich mit langfristig ausgerichteten Roadmaps neu aufgestellt, um für zukünftige Herausforderungen gerüstet zu sein. Trellix plant beispielsweise, sich auf die Weiterentwicklung einer leistungsstarken XDR-Plattform zu fokussieren. Um dieses Ziel zu erreichen, wurden folgende Fokusthemen definiert:

- **Open XDR Extendibility**
  Die Anbindung bestehender IT-Security-Komponenten soll vereinfacht werden, damit auch Produkte anderer Hersteller Informationen in die XDR-Plattform einliefern oder für die Reaktion auf Bedrohungen genutzt werden können.
- **One Console Experience**
  Alle relevanten Informationen und Werkzeuge, die für die Reaktion auf Cyber-Security-Bedrohungen erforderlich sind, sollen in einer einzigen, für die Arbeit von Security Operations Teams optimierten Oberfläche verfügbar sein.
- **Data Lake**
  Über einen Data Lake werden alle Daten datenschutzgerecht gespeichert.
- **Trellix Labs**
  Mit Trellix Labs wird die Forschung rund um die Bedrohungserkennung wiederbelebt. Ziel ist es, aktuellste Bedrohungsinformationen und Expertisen in die XDR-Plattform einfließen zu lassen.

Skyhigh hat angekündigt, dass die On-Premise-Variante des ursprünglichen Web Gateway von McAfee unter dem neuen Namen Skyhigh Web Gateway bestehen bleibt. Der bislang für das Produkt zur Verfügung stehende Support wird ebenfalls fortgeführt.

Insgesamt stellt sich Skyhigh als Provider einer Secure Service Edge auf, deren bestehende und in Zukunft integrierte Features sowohl Daten als auch Nutzer in Cloud- und Remote-Work-Umgebungen schützen sollen. Um dieses Ziel zu erreichen, werden Unternehmen mit dem Skyhigh-Portfolio in die Lage versetzt, Maßnahmen gegen Datenabfluss umzusetzen, durch die Verwendung von Cloud-Diensten entstehende Risiken zu erkennen und Richtlinien durchzusetzen.

Des Weiteren bietet Skyhigh umfassende Funktionen für die Nutzer an, die nicht mehr über typische Unternehmensressourcen geschützt sind, sondern aus der Ferne auf Dienste oder Unternehmensnetzwerke in der Cloud zugreifen. Dazu zählt zum Beispiel der Benutzer-Echtzeitschutz. Hierfür werden URLs, IPs und Dateien in Echtzeit mithilfe von Machine Learning und Sandboxing überprüft.

Ein weiterer Baustein zum Schutz von Nutzern ist die Remote Browser Isolation. Webseiten werden dabei nicht auf dem Endpoint selbst aufgerufen und ausgeführt, sondern auf einem sicheren System in der Cloud. So wird sichergestellt, dass Website-Bedrohungen nicht auf das Endgerät des Benutzers gelangen.

Skyhigh stellt sich somit als Provider einer zentralen Lösung für Unternehmen auf, die schon heute oder in Zukunft auf Cloud-Dienste und dezentral arbeitende Mitarbeiter setzen wollen.

McAfee, Trellix & Skyhigh

Was empfiehlt das r-tec-Expertenteam?

Nach unserer Einschätzung besteht für keinen Anwender der bisherigen McAfee-Lösungen akuter Handlungsbedarf. Allerdings ist es ratsam, eine strategische Planung hinsichtlich Fortführung, Ausbau, Ergänzung oder Ablösung durchzuführen. Dabei muss berücksichtigt werden, welche Skyhigh- bzw. Trellix-Lösungen im Einsatz sind und wie die IT-Strategie des betroffenen Endkunden aussieht. Letztlich raten wir allen Kunden, unsere Beratung für eine zukunftsorientierte SIEM-, SOC- und MDR-Strategie in Anspruch zu nehmen, um die für sie bestmögliche Lösung zu finden.

Unsere Empfehlung für Secure-Web-Gateway-Nutzer:

Kunden, die das bisherige McAfee Secure Web Gateway nutzen, können es wie gewohnt weiterbetreiben. Das deutlich erweiterte Portfolio von Skyhigh bietet aber auch die Möglichkeit, die klassischen On-Premise-Security-Architekturen schrittweise an die modernen Cloud- und Hybrid-IT-Architekturen anzugleichen, um eine zukunftsorientierte Cyber-Security-Architektur zu schaffen.

Ein Migrationspfad könnte zum Beispiel wie folgt aussehen:

01. Skyhigh verlagert Content-Security-Funktionen in die Cloud und bietet damit die Chance zur Modernisierung der Endpunkt-Security. Somit werden mobile Systeme immer wirksam geschützt, ganz gleich, wo sie sich befinden.
02. Mit der Zero-Trust-Lösung kann jegliche Form von Zugriffen – insbesondere in hybriden Umgebungen – abgesichert werden. Klassische Netzwerksegmentierungslösungen waren dazu bislang nicht in der Lage.
03. Mittels Cloud Access Security Broker (CASB) werden die Cloud-Zugriffe abgesichert. Da die darin integrierte Data Loss Prevention (DLP) das gesamte Modell überwacht, kann abschließend ein Datensicherheitssystem etabliert werden, das auf allen Ebenen wirkt.

Unsere Empfehlung für Endpoint-Protection-Nutzer:

Für Kunden, die hauptsächlich die McAfee-Endpoint-Protection-Lösungen nutzen, zeigt sich hingegen ein anderes Bild: Es ist absehbar, dass die von Trellix angestrebte XDR-Plattform frühestens Mitte 2023 eine ausreichende Marktreife erlangt haben wird. Kunden, die bereits jetzt dringend EDR- und XDR-Funktionen benötigen oder aus anderen Gründen mit den Funktionen der bisherigen McAfee Endpoint Protection unzufrieden sind, unterstützen wir bei der Evaluation von Alternativen. Unser Serviceportfolio umfasst unter anderem Lösungen des Herstellers Sophos, die wir interessierten Unternehmen gerne vorstellen.

Besteht jedoch keine Dringlichkeit, ist es aus unserer Sicht sehr sinnvoll, auf die neue XDR-Plattform von Trellix zu warten, da für Endpoint-Bestandskunden sehr wahrscheinlich keine umfangreichen Rollout-Projekte durchgeführt werden, sondern eine schrittweise funktionale Integration erfolgen wird. Eine Anbindung an den Managed-Detection-Service und somit an unser Cyber Defense Center versuchen wir in jedem Fall zu gewährleisten.

Unsere Empfehlung für SIEM-Nutzer:

Kunden, die das SIEM von McAfee nutzen, sollten mittelfristig eine Migration in Erwägung ziehen. Je nach Zeithorizont kann hier die neue auf Helix basierende Plattform von Trellix

interessant werden. Diese wird jedoch vermutlich keinen Bezug zur bisherigen McAfee-SIEM-Plattform haben. Außerdem ist eine Bewertung der Eignung zum jetzigen Zeitpunkt nicht möglich. Sicher ist hingegen, dass Trellix das von McAfee zur Verfügung gestellte SIEM nicht innovativ weiterentwickeln wird.

Im r-tec-Portfolio finden Sie allerdings schon jetzt einen Managed Detection and Response Service, der auf einem Next-Generation-Cloud-SIEM (Exabeam) beruht und nicht nur den SIEM-Betrieb, sondern das gesamte Event- und Incident-Management beinhaltet. Weitere EDR-, XDR- und OT-Features werden laufend in das Serviceportfolio aufgenommen.

Beratungsservice für McAfee-Nutzer

Sie sind unsicher, ob im Hinblick auf Ihre McAfee-Lösungen Handlungsbedarf besteht? Als Vertriebspartner der drei Herstellerfirmen McAfee, Trellix und Skyhigh bietet Ihnen r-tec eine umfassende Beratung. Auf Wunsch analysieren wir Ihre Cyber-Security-Architektur und empfehlen die für Sie individuell beste Lösung. Rufen Sie uns an unter der Telefonnummer +49 (0) 202 31767–100 oder senden Sie uns eine E-Mail an info@r-tec.net.

Die r-tec IT Security GmbH, mit Sitz in Wuppertal, wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, Konzerne, kommunale Rechenzentren und Bundes- oder Landesbehörden vertrauen seit über 20 Jahren auf unsere hoch spezialisierten Experten.

Als Strategic Supplier für Cyber Security Services schützen wir die Werte unserer Kunden vor Bedrohungen und begleiten ihr Security Management von der Initiierung über die Einführung bis zum Betrieb auf allen Ebenen.

Wir leben Regeltreue, höchste Qualitätsstandards und Servicementalität. Unser Unternehmen haben wir nach den Strukturen und Richtlinien der DIN ISO 9001:2015 und der ITIL aufgebaut. Wir sind nach ISO 27001 zertifiziert.

r-tec IT Security GmbH | Hatzfelder Str. 165-167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100