KURZVORSTELLUNG

Ein vereinfachter Ansatz für Endgerätesicherheit

Entwicklung einer zentralen Bedrohungsabwehr für alle Endgeräte – vom Gerät bis zur Cloud

Cyber-Sicherheit befindet sich in der Zwickmühle: Während die schiere Masse, die Raffinesse und die finanziellen Auswirkungen von Kompromittierungen immer weiter zunehmen, ist der Pool verfügbarer Analystenexperten so klein wie noch nie.

Jetzt gibt es jedoch eine Möglichkeit, komplexe Sicherheitsprobleme in Ihrem Unternehmen mit weniger Zeit- und Ressourcenaufwand zu beheben: Die McAfee®-Produkte zum Schutz von Endgeräten nutzen Analysen und Machine Learning, um branchenführende Effektivität zu erreichen. Gleichzeitig können unsere Lösungen flexibel mit Produkten von mehr als 150 Drittanbietern verbunden werden. Unser Ziel ist die Zentralisierung von Datensicherheit und Bedrohungsabwehr vom Gerät bis zur Cloud. Hierfür setzen wir auf ein integriertes System, das einfacher, intelligenter und breiter aufgestellt ist alles, was bisher zur Verfügung steht.

Hauptvorteile

- Schutz Ihrer Endgeräte durch Exploit-Schutz, Firewall, Web-Kontrolle und Machine Learning
- Schutz von iOS- und Android-Geräten vor Phishing, Zero-Day-Angriffen und Datenverlust in Echtzeit (auch im Offline-Zustand)
- Leistungsfähige Erkennung, Untersuchung und Abwehr von Bedrohungen – durch KI-geführte Untersuchungen vereinfacht
- Ergänzung der grundlegenden Sicherheitsfunktionen des Betriebssystems um Machine Learning, Schutz vor Anmeldedaten-Diebstahl und Behebung durch Rollback
- Vereinfachte und schnellere Sicherheitsverwaltung dank zentraler Übersicht
- Wahlweise mit SaaS-basierter Verwaltung über MVISION ePO oder lokaler Verwaltung über McAfee® ePO™

Folgen Sie uns

Da die Zahl, Vielfalt und Komplexität der Unternehmensendgeräte weiterhin steigt, stehen Unternehmen vor einer wichtigen Entscheidung. Verlassen sie sich weiterhin ausschließlich auf herkömmliche Virenschutzlösungen – in dem Wissen, dass sie damit keinen Schutz vor modernen Bedrohungen, wie Ransomware und Botnets, erhalten? Oder sollen sie eine „Lösung" aus Produkten mehrerer Anbieter zusammenstückeln, die zwar größeren Bedrohungsschutz bietet, aber Prozesse und Systeme ausbremst und erhebliche Ausfallzeiten verursacht? Die Antwort sind McAfee-Produkte zum Schutz von Endgeräten: Jetzt müssen Unternehmen keine Kompromisse mehr eingehen und zwischen zuverlässiger Bedrohungsabwehr und operativer Flexibilität wählen.

McAfee Endpoint Security

Zentrale Verwaltung, gemeinsame Analysen

Diese integrierte und zentral verwaltete Plattform für Endgeräteschutz benötigt nur einen Agenten für mehrere Technologien, einschließlich Bedrohungsschutz, Firewall, Web-Kontrolle, adaptive Bedrohungsabwehr usw., die darauf ausgelegt sind, den Schutz in komplexen Umgebungen zu vereinfachen.

Im Gegensatz zu herkömmlicher Virenschutz-Software nutzt McAfee Endpoint Security Verbindungen zwischen lokalen Endgeräten und dem Cloud-basierten Service McAfee® Global Threat Intelligence, um Zero-Day-Bedrohungen fast in Echtzeit zu erkennen. Sobald eine Bedrohung irgendwo entdeckt wurde, kann sie überall aufgespürt werden. Durch die Kombination aus gemeinsam genutzten Analysen und Informationen sowie hochentwickelten Exploit-Schutzfunktionen erzielt McAfee Endpoint Security eine um 25 % höhere Schutzrate vor Zero-Day-Bedrohungen als McAfee® VirusScan® Enterprise. In unabhängigen Tests wurde die Sicherheitseffizienz von McAfee Endpoint Security mit 99,98 % bewertet, wobei keine False-Positives generiert wurden.

Automatische Wartung, effiziente Behebung

Mit McAfee Endpoint Security können Sie erweiterte Funktionen für Automatisierung und Machine Learning nutzen. Die Machine Learning-Verhaltensklassifizierung der Plattform erkennt Zero-Day-Bedrohungen nahezu in Echtzeit und liefert umsetzbare Bedrohungsdaten. Zudem wird die Verhaltensklassifizierung automatisch weiterentwickelt, um Verhaltensweisen aufzudecken sowie Regeln hinzuzufügen, mit denen zukünftige Angriffe aufgedeckt werden können.

Während eines Angriffs lässt sich für Administratoren schnell erkennen, wo sich Infektionen befinden und wie lange sie bereits bestehen. Dadurch können sie Bedrohungen besser einschätzen und schneller reagieren. Die Real Protect-Funktion setzt das Endgerät in den letzten als sicher bekannten Zustand zurück, um Infektionen sofort zu verhindern und den Aufwand für Administratoren zu reduzieren. Die Funktion zur dynamischen Eindämmung von Anwendungsprozessen wehrt durch den Schutz von „Patient Null" zudem Ransomware und Greyware ab.

Die Kombination aus der McAfee ePO-Plattform und McAfee Endpoint Security ermöglicht einen besseren Überblick, höhere Produktivität für das IT-Team, vereinfachte Abläufe, einheitliche Sicherheit und reduzierte Kosten. Dank dieser und weiterer Effizienzvorteile können Cyber-Sicherheitsteams durch den

Wichtige Vorteile von McAfee Endpoint Security

- Erkennt Zero-Day-Bedrohungen fast in Echtzeit
- Aktualisiert kontinuierlich das Malware-Schutz-Modul
- Ermöglicht Kommunikation zwischen Virenschutz, Exploit-Schutz, Firewall und Web-Kontrollen
- Repariert das Endgerät durch Zurücksetzen in den letzten bekannt guten Zustand
- Dämmt schädliche Anwendungen und Prozesse auf Geräten ein – auch wenn sie offline sind
- Priorisiert Warnmeldungen mit „Playback" von Angriffsereignissen
- Bietet integrierte, benutzerfreundliche Funktionen für Zwischenfallsuche und Reaktion
- Ermöglicht Reaktionen auf Zwischenfälle mit einem einzigen Mausklick

Wechsel zu McAfee Endpoint Security pro Woche 40 Stunden Verwaltungsaufwand einsparen. Auch die Produktivität der Mitarbeiter wird verbessert: Scans nehmen nur wenige Sekunden in Anspruch, werden nur durchgeführt, wenn das Gerät im Leerlauf ist und werden nach einem Geräteneustart nahtlos fortgesetzt. Das beste dabei: Die ressourcenschonende Lösung McAfee Endpoint Security benötigt keine Cloud-Verbindung, sodass Benutzer auch offline geschützt sind.

McAfee MVISION EDR

Eine durchschnittliche IT-Abteilung verwaltet tausende Endgeräte – von Desktops und Servern bis zu Mobiltelefonen, Smartwatches und IoT-Geräten. Aktuelle EDR-Lösungen setzen bereits überlastete Sicherheitsteams einer Informationsflut aus und überlassen die Untersuchung der Bedrohungen erfahrenen Analysten. Dieser Ansatz ist weder effektiv noch skalierbar – ganz besonders in Anbetracht aktueller Bandbreitenbeschränkungen und des Fachkräftemangels.

MVISION EDR setzt dort an, wo Virenschutz-Technologien und herkömmliche EDR-Lösungen aufhören. Die integrierte Endgerätesicherheitslösung vereinfacht die Verwaltung großer Mengen an Warnmeldungen, die Überwachung und Erfassung von Aktivitätsdaten von Endgeräten, die auf Bedrohungen hinweisen können, und liefert den erforderlichen Überblick und Kontext. Durch die Analyse der Daten auf Bedrohungsmuster können die automatisierten, KI-basierten Reaktions- und Analysefunktionen automatisch Bedrohungen entfernen oder eindämmen sowie das Sicherheitspersonal informieren.

Die Forensik- und Analyse-Tools untersuchen zudem die identifizierten Bedrohungen und suchen nach verdächtigen Aktivitäten.

Vorteile KI-geführter Untersuchungen

EDR-Lösungen „unterstützen“ üblicherweise Untersuchungen, indem sie Rohdaten, Kontext und Suchfunktionen zur Verfügung stellen. Allerdings sind zur Durchführung der eigentlichen Untersuchungen und Analysen weiterhin erfahrene Analysten erforderlich. MVISION EDR führt die Analysten jedoch durch die Untersuchung, sodass weniger Kompetenzen und Aufwand erforderlich sind. Zudem können die Analysten schneller den Risikoschweregrad und die Ursache des Zwischenfalls bestimmen.

Die KI-geführte Untersuchung erfasst und verarbeitet automatisch erhebliche Datenmengen aus verschiedenen Quellen und liefert dadurch Informationen zum Ursprung und Ziel des Angriffs sowie zum Angriffsmuster. Anschließend imitiert die Lösung das Verhalten eines erfahrenen Analysten: Sie führt unerfahrene Analysten durch die Untersuchungsschritte, indem sie automatisch verschiedene Hypothesen zu Warnmeldungen aufstellt und während der Untersuchung Fakten aus mehreren Quellen erfasst, zusammenfasst und visualisiert. Mithilfe der gefundenen Fakten und der Hypothesen formuliert MVISION EDR relevante Fragen und hilft bei deren Beantwortung, während die Analysten entscheiden, ob sie mit weiteren Fragen und der Datenerfassung fortfahren oder das Problem ad acta legen oder eskalieren wollen.

Wichtige Vorteile von McAfee MVISION EDR

- Qualitativ hochwertige, umsetzbare Bedrohungserkennungen ohne False-Positives
- Schnellere Analyse für eine zuverlässigere Abwehr
- KI-geführte Untersuchungen für Erkenntnisse zum Angriff, die von der Maschine generiert werden
- Optimale Nutzung der Stärken des vorhandenen Personals
- Wartungsarme Cloud-Lösung
- Branchenweit anerkannte zentrale Sicherheitsverwaltung über eine Konsole, MVISION ePO (SaaS-basiert) oder McAfee ePO (lokal oder IaaS-basiert)
- Konzentration der Analysten auf strategische Zwischenfallreaktion ohne zusätzlichen Verwaltungsaufwand

Das stärkt die Kompetenz der Analysten, erleichtert ihnen den Umgang mit größeren Zahlen von Warnmeldungen, verringert den Zeitaufwand für die Untersuchung und verbessert deren Qualität. Selbst unerfahrene Analysten können zuverlässige Analysen durchführen, während sich Ihre Analyseexperten darauf konzentrieren, verborgene Bedrohungen aufzudecken und die Reaktion zu beschleunigen.

Schnellere Identifizierung ermöglicht schnellere Reaktionen

Mithilfe der leistungsstarken Suchmöglichkeiten und der jederzeit aktiven Datenerfassungsfunktionen können Analysten auch umfassendere Abfragen durchführen und Ereignisse genauer sowie systemübergreifend analysieren. MVISION EDR kann einen Snapshot aktiver Prozesse, Netzwerkverbindungen, Dienste und Autostart-Einträge erstellen, um sofortige Untersuchungen, Echtzeitsuchen und Suchen in Verlaufsdaten zu ermöglichen. Diese Daten werden zur schnellen Anpassung neuer Analyse-Module und -Techniken zusätzlich in die Cloud gestreamt. Gleichzeitig werden die Ergebnisse der verhaltens-basierten Erkennung mit dem MITRE ATTACK-Framework abgeglichen, damit sie konsistent einer Angriffsphase sowie den entsprechenden Risiken und angemessenen Reaktionen zugeordnet werden können.

Die Untersuchungsfunktionen und Erkenntnisse von MVISION EDR werden durch die Integration mit SIEM-Lösungen (Sicherheitsinformations- und Ereignis-Management), wie McAfee® Enterprise Security Manager oder Drittanbieterprodukten, zusätzlich erweitert. Das ermöglicht die Korrelation von Endgeräteartefakten mit Netzwerkinformationen sowie anderen vom SIEM erfassten Daten.

McAfee MVISION Endpoint

Für Kunden, die ihren Endgeräteschutz verstärken möchten, bietet MVISION Endpoint erweiterte Erkennungs- und Korrekturfunktionen. Die Lösung wurde speziell als Verstärkung für die systemeigenen Betriebssystem-Schutzfunktionen konzipiert, zum Beispiel für die in Windows 10, Windows Server 2016 und Windows Server 2019 standardmäßig enthaltenen Virenschutz-Firewall- und Exploit-Schutz-Technologien. Dazu erkennt die Lösung hochentwickelte Bedrohungen, die von Microsoft Defender übersehen werden.

Eine intelligentere Endgerätestrategie

Im Gegensatz zu den Alternativen, die lediglich eine Form der Machine Learning-Analyse anbieten, kann MVISION Endpoint statische, verhaltensbezogene sowie auf dateilose Malware ausgerichtete Analysen durchführen und dadurch stärkeren Bedrohungsschutz und geringere False-Positives bieten. Die Lösung verwendet verhaltensorientiertes Machine Learning, um Bedrohungen anhand von tatsächlichem Verhalten zu erkennen, und überführt eine Datei, wenn sie die gleichen Eigenschaften besitzt wie andere Malware. Sie ermöglicht auch erweiterte Behebung durch Rollback, sodass ein System nach einem Ransomware-Angriff in den letzten als sicher bekannten Zustand zurückversetzt werden kann.

Wichtige Vorteile von McAfee MVISION Endpoint

- Zentrale Verwaltung für Windows 10 sowie Windows Server 2016 und Windows Server 2019
- Hochentwickelte dateibasierte, dateilose und verhaltens-basierte Machine Learning-Schutzmaßnahmen
- Niedrigere Gesamtbetriebs-kosten und optimierte Workflows
- Schutz vor Diebstahl von Anmeldedaten und Behebung durch Rollback
- Verwaltung der McAfee- und Microsoft-Schutztechnologien mit einer Richtlinie über eine Konsole

Wichtige Vorteile von McAfee MVISION Mobile

- Bietet Echtzeit-Schutz auf dem Gerät
- Erkennt mobile Bedrohungen und schützt vor Zero-Day-Angriffen

Zentrale Konsole und Cloud-basierter Schutz

Der größte Vorteil von MVISION Endpoint ist die zentrale Verwaltung, d. h. Sie können die Richtlinien für Windows Defender Antivirus, Exploit Guard, Windows Firewall-Einstellungen und McAfee zentral verwalten. Wenn Sie McAfee MVISION Endpoint zusammen mit McAfee ePO oder MVISION ePO bereitstellen, erhalten Sie ein tatsächlich integriertes Schutzsystem mit einer zentralen Übersicht. McAfee ePO und MVISION ePO ermöglichen zudem die Integration von Drittanbieter-Produkten, sodass über die Konsole noch weitere Gegenmaßnahmen verfügbar sind und Ihre Sicherheit gestärkt wird.

Der äußerst ressourcenschonende Agent ist schneller, einfacher und zuverlässiger als herkömmliche Sicherheits-Tools. Aktualisierungen werden automatisch auf den Client übertragen, und da der Agent nur wenig Ressourcen und Rechenleistung auf dem Gerät benötigt, bleiben die Auswirkungen auf die Produktivität der Benutzer minimal.

McAfee MVISION Mobile

McAfee MVISION Mobile erkennt Bedrohungen und Schwachstellen auf Apple iOS- oder Google Android-Geräten, in den Netzwerken, mit denen die Geräte verbunden sind, sowie in den von Benutzern heruntergeladenen Anwendungen. Durch die Integration in unsere wichtigste zentrale Verwaltungsplattform für Unternehmen, McAfee ePO, können Sie Mobilgeräte genauso wie alle anderen Endgeräte verwalten. Als integrierte Komponente von McAfee® Device Security erweitert MVISION Mobile die Übersicht und Kontrolle Ihrer mobilen Ressourcen mit der gleichen zentralen Konsole auf alle Ihre von McAfee verwalteten Geräte.

Intelligenter und wachsamer

Im Gegensatz zu Cloud-basierten Sicherheitslösungen für Mobilgeräte, die auf App Sandboxing oder Datenverkehr-Tunneling setzen, wird MVISION Mobile direkt auf dem Mobilgerät installiert. Dadurch bietet die Lösung permanent aktiven Schutz, ganz gleich, wie das Gerät gerade verbunden ist – mit dem Unternehmensnetzwerk, über einen öffentlichen Zugriffspunkt, einen Netzanbieter und sogar offline.

MVISION Mobile nutzt Machine Learning-Algorithmen, in die Milliarden Datenpunkte von Millionen Geräten einfließen, um aktuelle oder neue Bedrohungen zu identifizieren. Diese Algorithmen analysieren abweichendes Geräteverhalten und treffen Entscheidungen zu Kompromittierungsindikatoren, um hochentwickelte geräte-, anwendungs- und netzwerkbasierte Angriffe zu identifizieren – einschließlich bislang völlig unbekannter Angriffe. Umfassende Daten zu Anwendungen mindern Sicherheits- sowie Datenschutzrisiken und reduzieren damit die Wahrscheinlichkeit von Datenverlusten. Die Benachrichtigungen der Netzwerkschutzfunktion informieren Sie und Ihre Mitarbeiter, wenn Mobilgeräte Verbindungen mit unsicheren oder kompromittierten Netzwerken herstellen. So können Angriffe gestoppt werden, bevor sie Schaden anrichten.

McAfee MVISION ePO

Die branchenweit anerkannte Lösung McAfee MVISION ePO ist für die Verwaltung von McAfee-Lösungen und die Verbesserung der Betriebssystemen-eigenen Sicherheitskontrollen ausgelegt. Diese globale, mandantenfähige und unternehmensgerechte SaaS-Version der bewährten

- Stellt Datenschutzrisiken heraus, damit sich die Benutzer über die Gefahren mit einer bestimmten Anwendung bewusst werden
- Beschleunigt die Reaktion durch unternehmensgerechte umsetzbare Erkenntnisse zu Mobilgeräten
- Ermöglicht Mitarbeitern dank Compliance-Kontrollen, jederzeit, überall und an allen Geräten zu arbeiten
- Erkennt schädliche Links in Textnachrichten, Social-Media-Apps und E-Mails durch Phishing-Schutz
- Integriert sich mit EMM-Lösungen (Enterprise Mobility Management), lässt sich aber auch in BYOD-Szenarien (Bring-Your-Own-Device) anwenden
- Ermöglicht Vorfallreaktionsteams die Nutzung umfassender forensischer Bedrohungsdaten zu Analysezwecken, um zu verhindern, dass ein kompromittiertes Gerät zu einem Ausbruch führt

und einzigartigen Software McAfee ePO erlaubt das Verwalten Ihrer Sicherheitsfunktionen, das Festlegen und automatische Durchsetzen von Richtlinien sowie das Optimieren und Automatisieren der Compliance-Abläufe. Außerdem profitieren Sie von mehr Transparenz. Die Lösung kann für hunderttausende Geräte – einschließlich solcher mit systemeigenen Kontrollen – skaliert werden. Dabei wird die gesamte Bandbreite vom Gerät bis zur Cloud abgedeckt, ohne dass eine lokale Architektur gepflegt werden muss.

Sicherheit UND Einfachheit

Die erweiterbare Plattform MVISION ePO stellt gemeinsame Verwaltungsfunktionen mit gemeinsamen Richtlinien für alle Geräte (einschließlich Microsoft Windows 10-Geräte) in heterogenen Unternehmensumgebungen bereit und gewährleistet dadurch Konsistenz und Einfachheit. Durch die zentrale Übersicht von MVISION ePO wird die komplexe Koordinierung mehrerer Produkte vereinfacht. Dank flexibler, automatisierter Verwaltungsfunktionen können Benutzer Schwachstellen, Änderungen der Sicherheitslage sowie bekannte Bedrohungen schnell erkennen, verwalten und darauf reagieren. Dies alles ist über den Browser möglich. Von hier können auch in nur wenigen Schritten Sicherheitsrichtlinien bereitgestellt und im gesamten Unternehmen erzwungen werden.

Die Benutzeroberfläche liefert eine Zusammenfassung all Ihrer Umgebungen in einer grafischen Übersicht, sodass Administratoren den Risiken Prioritäten zuweisen und für zusätzliche Erkenntnisse Details zu einzelnen Ereignissen aufrufen können. Diese Übersicht reduziert den Zeitaufwand für Berichterstellung sowie Datenoptimierung und vermeidet potenzielle Fehler bei manuellen Eingriffen. Durch die Kombination von Risikoverwaltung und Zwischenfallanalysen liefern Ihre Geräte wichtige Erkenntnisse für Ihr SIEM-System sowie wichtige Informationen, die Ihren Analysten sofort für verbesserte Bedrohungssuchen und Behebungsmaßnahmen zur Verfügung stehen.

Größere Effizienz

Laut dem Gartner Magic Quadrant für Endgeräteschutz ist McAfee ePO ein Grund dafür, dass viele Unternehmen zu McAfee wechseln und bei McAfee bleiben. Da diese bewährte Technologie nun auch im SaaS-Format verfügbar ist, profitieren Unternehmen jetzt zusätzlich dadurch, dass sich ihre Sicherheitsexperten ganz auf die Überwachung und Kontrolle aller Geräte konzentrieren können. MVISION ePO entlastet Unternehmen von den Support- und Wartungsaufgaben für die lokale Sicherheitsinfrastruktur, automatisiert die Bereitstellung der Gerätesicherheit im gesamten Unternehmen und bietet kontinuierliche, transparente Aktualisierungen. Das gewährleistet Stabilität und spart Zeit. Dank der hochentwickelten Funktionen kann das Sicherheitsteam Bedrohungen effizienter beseitigen oder Änderungen zur Wiederherstellung der Compliance vornehmen – wodurch noch größte Zeitersparnisse möglich sind.

Um festzustellen, ob MVISION ePO für Ihr Unternehmen die optimale Lösung ist, klicken Sie hier, um eine kostenlose Testversion zu erhalten.

Wichtige Vorteile von McAfee MVISION ePO

- Branchenweit anerkannte zentrale Verwaltung
- Einfache zentrale Konsole für Übersicht und Kontrolle von überall
- Keine Komplexität durch Wartung einer lokalen Sicherheitsplattform
- Einheitlicher Überblick für Risikoverwaltung und Analyse von Vorfällen
- Umfassende Plattform, die McAfee-Produkte und systemeigene Kontrollen in Betriebssystemen verwaltet
- Effiziente administrative Aufgaben durch automatisierte Workflows
- Optimierte Untersuchung und Behebung von Vorfällen
- Gemeinsame Sicherheitsverwaltung für die meisten auf dem Markt erhältlichen Geräte
- Skalierbarkeit auf hunderttausende Geräte
- Abdeckung vom Gerät bis zur Cloud

ANWENDERBERICHTE

MGM Resorts International
20.000 Knoten in 20 Resorts weltweit

- **Herausforderungen:** Minimierung von Risiken und Blockierung von Zero-Day-Angriffen; Verständnis komplexer Angriffsmuster und Rund-um-die-Uhr-Betrieb kritischer Anwendungen; Möglichkeit zur Reduzierung der SecOps-Kosten bei aktueller Umgebung
- **Lösungen:** McAfee® Enterprise Security Manager, McAfee® Investigator, MVISION EDR, McAfee® Web Gateway, McAfee Endpoint Security, McAfee Data Loss Prevention, DXL, McAfee® Professional Services
- **Ergebnisse:** Verkürzung der Zeit zur Eindämmung; Untersuchung und Reaktion auf Bedrohungen und verbesserte Kompetenzen des SecOps-Teams

Atrius Health
Mehr als 65.000 Benutzer an 9.000 Endgeräten an mehr als 29 Standorten

- **Herausforderungen:** Schutz vor Ransomware und Phishing; Beschleunigung von Erkennung und Reaktion; Absicherung des Unternehmens und Unterstützung des Geschäftswachstums
- **Lösungen:** McAfee Enterprise Security Manager, McAfee Endpoint Security
- **Ergebnisse:** Betriebskosteneinsparungen; kein Bedarf an zusätzlichen Vollzeitmitarbeitern; schnellere Erkennung und Reaktion; verbesserte Sicherheit für die virtuelle Umgebung

Florida International University
55.000 Studenten und 15.000 Mitarbeiter an zwei Hauptcampus-Standorten und weiteren Satelliten-Campussen außerhalb der USA

- **Herausforderungen:** Unterstützung von BYOD und dennoch Schutz der Umgebung vor Bedrohungen; Schutz der Studenten vor versehentlicher Malware-Infizierung der Umgebung; Gewährleistung vollständiger Transparenz
- **Lösungen:** McAfee Enterprise Security Manager, McAfee Endpoint Security
- **Ergebnisse:** Schnellere Eindämmung verdächtiger Dateien oder Angriffe; stärkere allgemeine Sicherheitsaufstellung ohne zusätzlichen Mitarbeiterbedarf; zuverlässiger Endgeräteschutz mit minimalen Auswirkungen auf Benutzer; einfache Verwaltung und unternehmensweiter Überblick

Banco Delta
400 Endgeräte

- **Herausforderungen:** Reduzierung der Belastung des Sicherheitsverwaltungsteams; starker Schutz vor hochentwickelten Angriffen; zukunftsfähige Sicherheitsstrategie, einschließlich Cloud-Migration
- **Lösungen:** McAfee ePO-Plattform, McAfee Enterprise Security Manager, McAfee Endpoint Security
- **Ergebnisse:** Spürbare Verringerung der Infektionen und des potenziell kompromittierenden Benutzerverhaltens

US-Versicherungsunternehmen
6.000 Desktop-PCs und 2.000 Server an 12 Standorten

- **Herausforderungen:** Schutz der vertraulichen personenbezogenen Kundendaten; Bereitstellung hervorragender Sicherheit ohne Beeinträchtigung der Kundenerfahrung
- **Lösungen:** McAfee Endpoint Security, McAfee Data Loss Prevention, McAfee Web Gateway
- **Ergebnisse:** Reduzierung der CPU-Spitzenauslastung von 95 % auf 30–35 % und Verkürzung der Scan-Dauer von mehreren Tagen auf Stunden; Einsparung zahlreicher Stunden pro Woche aufseiten der Cyber-Sicherheitstechniker; höhere Produktivität der Endbenutzer und SecOps; verbesserte Sicherheitsaufstellung

Große internationale Bank (EMEA)
45.000 Endgeräte in mehr als 40 Ländern und zwei Rechenzentren

- **Herausforderungen:** Schutz des Unternehmens vor Ransomware und Zero-Day-Bedrohungen bzw. Blockierung von Bedrohungen, die durch Benutzerverhalten entstehen; Verbesserung der Effizienz der Sicherheitsmaßnahmen
- **Lösungen:** McAfee Endpoint Security, McAfee ePO-Plattform, McAfee Web Gateway
- **Ergebnisse:** Verbesserter Endgeräteschutz, der mehr Malware erkennt und besser vor Zero-Day-Bedrohungen schützt; schnellerer Schutz dank integrierter Sicherheitslösungen, die Bedrohungsinformationen praktisch in Echtzeit austauschen; weniger Zeitaufwand für operative Aufgaben dank vereinfachter Sicherheitsverwaltung und weniger Zwischenfälle

Hervorragende Testergebnisse

McAfee Endpoint Security

- Silber bei den Cybersecurity Excellence Awards 2019 in der Kategorie „Endgerätesicherheit“
- AV-Comparatives: Auszeichnung als bewährtes Produkt für Unternehmen
- AV-TEST: McAfee erhält perfekte Punktzahl für Benutzerfreundlichkeit

MVISION Endpoint

- Silber bei den Cybersecurity Excellence Awards 2019 in der Kategorie „Endgerätesicherheit“
- Auszeichnung als Tech Innovator 2018 für Endgerätesicherheit

MVISION Mobile

- Silber bei den Cybersecurity Excellence Awards 2019 in der Kategorie „Mobilgerätesicherheit“

Einsatz der McAfee-Endgeräteprodukte

- 622 Millionen Endgeräte insgesamt
- 97 Millionen Endgeräte in Unternehmen
- 525 Millionen Endgeräte von Privatanwendern
- 69.000 Unternehmenskunden
- 7.000 Mitarbeiter
- 189 Länder
- 80 % der Fortune 100-Unternehmen
- 75 % der Fortune 500-Unternehmen
- 64 % der Global 2000-Unternehmen
- 87 % der weltweit größten Banken
- 54 % der Top 50-Einzelhändler
- Mehr als 1.550 Sicherheitspatente weltweit

„McAfee ePO gehört zu den Vorreitern bei der integrierten Automatisierung und Koordinierung von Sicherheitsmaßnahmen… Sicherheitsexperten benötigen heute die Leistung herkömmlicher [McAfee] ePO-Funktionen, allerdings als vereinfachte Lösung, damit sie effizient UND effektiv arbeiten können… Als SaaS-Lösung kombiniert MVISION Analyse, Richtlinienverwaltung und Ereignisse so, dass große und mittlere Unternehmen davon profitieren.“

– Frank Dickinson, Research Vice President, Security Products, IDC

McAfee
Together is power.

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