APPGUARD

Die Malware-Defensive

Internationale Fluggesellschaft senkt die Cyber-Kosten und verstärkt die Sicherheitslage mit AppGuard

FALLSTUDIE: WELTWEIT TÄTIGE FLUGGESELLSCHAFT

HERAUSFORDERUNGEN:

- Management der Kosten für Cyber-Abwehr bei gleichzeitiger Verbesserung der Sicherheitslage
- Komplexe Tools zur Endpunkt-Absicherung erfordern Cyber-Spezialisten

ERGEBNISSE:

- Um 76% verringerte Kosten für die Störfallreaktion
- Mehr Sicherheit mit weniger Ressourcen und Aufwand
- Geringere Belastung beim Patch-Management

Über die Fluggesellschaft

Führende, weltweit tätige Fluggesellschaft mit etwa 50.000 Mitarbeitern, die jährlich ungefähr 7.000.000 Passagiere rund um die Welt befördert. Die kritische Infrastruktur muss 24x7 betriebsbereit sein, um größere finanzielle Verluste zu vermeiden. Ein Cyber-Einbruch könnte das Leben der Passagiere gefährden, den Ruf schädigen und die Einnahmen erheblich verringern.

Situation: Komplexe Cyber-Betriebsabläufe und jahrelange lückenhafte Endpunkt-Absicherung

Beinahe 100.000 Endpunkte greifen aus der ganzen Welt jederzeit auf missionskritische IT-Infrastruktur zu. Die wachsenden Angriffsflächen des Unternehmens haben den Anstieg der Cyber-Aktivitäten über mehr als 10 Jahre angetrieben.

Es wurden mehrere Ebenen von Tools eingesetzt, um Endpunkt-Attacken zu erkennen und darauf zu reagieren. Mehrere Teams mit Spezialisten waren erforderlich, um technische Ebenen zu unterstützen und die Arbeitsabläufe untereinander zu koordinieren, einschließlich einer 24x7 Personalbesetzung zum Sichten der Alarme und für die Störfallreaktion. Die sich daraus ergebenden Arbeitsabläufe waren komplex und erhöhten die Gefahr von menschlichen Irrtümern und negativen Auswirkungen auf die Cyber-Bereitschaft. Je mehr Tools zur Sicherheitssuite hinzugefügt wurden, desto mehr Daten mussten analysiert werden.
Qualifizierte Cybersecurity-Analysten und das Personal zur Pflege der verschiedenen Tools zu finden und zu halten führte zu jährlich steigenden Cyber-Kosten. Jedoch stieg das Aufkommen von Cyber-Vorkommnissen trotz der hohen Investitionen in Technologie und Personal.

Unzureichende Endpunkt-Absicherung trotz erheblicher Investitionen in die Cyber-Sicherheit

Vor Jahren wurde eine Suite zur Endpunkt-Absicherung von einer der am meisten anerkannte Marken eingesetzt. Sie enthielt verschiedene Schutzfunktionen: Anti-Virus, Maschinenlernen-Binäranalyse, Verhaltens-

> *Wir benötigen keine Bataillone mit Spezialisten mehr, um auf Malware-Angriffe zu reagieren, denn AppGuard blockiert sie im Moment des Zuschlagens am Endpunkt.*

analyse, EDR, Anwendungskontrolle, HIPS, Anti-Exploit, URL-/Domain-Blacklisting und mehr. Obwohl ein einzelner Agent die Suite von einem einzigen Bildschirm aus steuerte, erforderte jedes Tool trotzdem erheblichen Arbeitsaufwand für Konfiguration, Wartung und Support. Die Komplexität und ungewollten Konsequenzen der unterschiedlichen Fähigkeiten schränkten die Möglichkeiten zur Nutzung der Cyber-Kontrollen ein. Darüber hinaus wurde viel Personal benötigt, um die Suite zu verwalten und weitere Mitarbeiter mussten Bedrohungen bearbeiten, die es geschafft hatten, die Suite zu umgehen.

AppGuard: Mehr Sicherheit, weniger Aufwand.

Als sie realisierte, dass der Status quo ineffizient und riskant war, wählte die Fluggesellschaft AppGuard aufgrund seiner einzigartigen Fähigkeit, Malware in Echtzeit zu blockieren, und aufgrund der einfachen Bereitstellung und Wartung aus. Im Gegensatz zu anderen Tools, die von geschultem Sicherheitspersonal gemanagt werden müssen, kann AppGuard von einem Windows-Administrator gemanagt werden. Das war angesichts der Kosten und des Mangels an geschulten Sicherheitsanalysten wichtig.

Bei der Auswertung bewies ein Penetrationstest die Effektivität von AppGuard beim Blockieren von Malware. Durch das Bereitstellen von Schutz vor Kompromittierung eliminiert AppGuard die Notwendigkeit von Überwachung, Untersuchung und Behebung - und verringert so die allgemeinen Anforderungen an Cybersecurity-Mitarbeiter und Budget bei gleichzeitiger Verbesserung der Sicherheitslage der Fluggesellschaft.

Geringere Belastung beim Patch-Management

Die einzigartige, patentierte Isolationstechnologie von AppGuard schützt Endpunkte vor den Anwendungen und Dienstprogrammen, die häufig über Software-Sicherheitslücken gekapert werden. Dadurch konnte die Fluggesellschaft den Aufwand für das Patch-Management verringern und das Sicherheitspersonal konnte sich verstärkt auf die strategischen Angelegenheiten konzentrieren. Dadurch fiel auch die Notwenigkeit weg, dem Personal Überstunden zum Implementieren von Patches zu bezahlen.

Da AppGuard die Risiken minimierte, wurde die Anzahl der Exploit-Angriffe auf Anwendungen auf null verringert.

Weniger Alarme und falsch Positive

AppGuard ist kein Erkennungstool. Es beurteilt nicht, ob eine Datei gut oder schlecht ist oder Endpunkt-Aktivitäten normal oder nicht normal sind. Es blockiert nicht-konforme Aktivitäten und meldet sie. Zum Analysieren der Alarme werden keine Spezialisten benötigt. AppGuard ist einfach zu konfigurieren und es lassen sich leicht Ausnahmen von den Regeln einrichten, die aus der Ferne an Agenten verteilt werden, um sicherzustellen, dass rechtmäßige Anwendungen nie blockiert werden.

Verringerte Kosten für die Störfallreaktion (Incident Response/IR)

Der vor der Kompromittierung einsetzende Schutz von AppGuard bietet eine Vielzahl von Vorteilen - einschließlich der Möglichkeit, die Kosten für die Störfallreaktion zu verringern.

Durch die Verwendung von AppGuard war die Fluggesellschaft in der Lage, die Belegschaft vom 24x7-Betrieb auf 24x5-Betrieb zu reduzieren. Durch den anhaltenden Erfolg von AppGuard konnte der Arbeitsaufwand für Störfallreaktionen weiter auf 8x5 reduziert werden. Durch die interne Verwendung von AppGuard schraubt die Fluggesellschaft ihre Kosten für die Störfallreaktion weiter nach unten.

Durch die Verringerung auf 12x5-Betrieb konnte die Fluggesellschaft die Arbeitskosten um 64% reduzieren. Das spiegelt nicht nur ehebliche Kosteneinsparungen wider, es setzt auch Sicherheitsmitarbeiter frei für Initiativen zur Verbesserung der Effektivität der Cybersecurity der Organisation und für die Optimierung der allgemeinen Sicherheitslage des Unternehmens.

Endpunkte ohne Kompromisse

Durch den Einsatz von AppGuard hat die Fluggesellschaft einen höheren Grad an Sicherheit erreicht und gleichzeitig die Kosten für die Cybersicherheit reduziert. AppGuard ermöglicht der Fluggesellschaft, ihren Aufgaben nachzugehen, während die Malware an ihrem Vorhaben gehindert wird. AppGuard ermöglicht der Fluggesellschaft mehr Sicherheit trotz weniger Auffand und sie kann sicher sein, dass ihre Endpunkte nicht kompromittiert werden.

Über AppGuard

AppGuard ist ein Cybersecurity-Unternehmen, das es sich zur Aufgabe gemacht hat, einen neuen Standard zu setzen: echter Cyber-Schutz für alle.
Die patentierte Technologie von AppGuard verhindert Kompromittierungen, bevor sie geschehen, indem sie Malware-Aktivitäten daran hindert, Schaden anzurichten, ohne sie wiederkennen zu müssen.

Im Gegensatz zu erkennungsbasierten Lösungen überlistet AppGuard böswillige Akteure, damit Unternehmen ihren Aufgaben nachgehen können und die Schadsoftware nicht machen kann, was sie will.

APPGUARD
Die Malware-Defensive

www.appguard.us | software@ingrammicro.ch