APPGUARD
The Malware Disruptor

DATENBLATT

AppGuard: Endpunkt-Absicherung für kleine und mittelständische Unternehmen (KMUs)

Wenn Sie ein kleines oder mittelständisches Unternehmen sind und glauben, Sie wären zu klein, um ein Ziel für Cyber-Kriminelle zu sein, denken Sie noch einmal nach. Dem Ponemon Institute zufolge betrafen 63% aller Datenschutzverletzungen im Jahre 2019 kleine und mittelständische Unternehmen. Das liegt daran, dass Hacker Opportunisten sind. Sie erkennen, dass KMUs normalerweise geringere und weniger geschulte Ressourcen für den Kampf gegen Cyber-Widersacher zur Verfügung haben und wahrscheinlich eher die von Schadsoftware verursachten Kosten tragen, ohne die Mittel zur Behebung zu investieren. Böswilligen Akteuren einen Schritt voraus zu sein ist schwierig, insbesondere für kleine und mittelständische Unternehmen. Unglücklicherweise ist diese Herausforderung heute sogar noch größer, da die COVID-Pandemie die Art und Weise verändert hat, wie wir unsere Geschäfte führen.

Die durch COVID ausgelöste Umstellung auf Fern- und Hybrid-Arbeitsumfelder hat die Risiken für KMUs erhöht. Das Organisieren einer mobilen Belegschaft, die neue digitale Dienste und Produkte verwendet, vergrößert die Angriffsfläche erheblich, wenn sich die Mitarbeiter von Unternehmensnetzwerken und Sicherheitsmaßnahmen entfernen. Ein vormals klar abgegrenzter Perimeter ist nun verschwommen, porös und offen für Cyber-Attacken. KMUs müssen heute mehr als jemals zuvor ihre Schutzbarrieren erhöhen, um die Endpunkte vor Kompromittierung zu schützen.

AppGuard: Einfache, effektive Endpunktabsicherung

Mit AppGuard können KMUs die Herausforderungen durch begrenzte Personal- und Sicherheitsbudgets überwinden. Ob die Endpunktsicherheit intern oder mithilfe eines MSSP gemanagt wird - AppGuard bietet Ihnen den Schutz, den Sie brauchen, um Malware zu stoppen, bevor sie Schaden anrichtet.

Besserer Schutz, weniger Verbrauch von Ressourcen

Ohne Ihre bereits überarbeiteten Mitarbeiter weiter zu strapazieren, erlaubt AppGuard Ihrem Unternehmen, seinen Aufgaben nachzugehen, während die Malware an ihrem Vorhaben gehindert wird. AppGuard wurde ursprünglich entwickelt, um hochriskante U.S-Geheimdienstmitarbeiter und -daten zu schützen. Es benötigt im Betrieb nur geringe menschliche Ressourcen und Rechenleistung. Anders als andere Tools, die zur Verwaltung ein Heer von Sicherheitsprofis benötigen, ist AppGuard einfach bereitzustellen und kann von einem einzelnen Windows-Administrator gemanagt werden. Adaptive Präventionskontrollen heißt keine Alarme, keine Untersuchungen, kein Threat-Hunting und keine zu pflegenden Whitelists - nur erhöhter Schutz mit geringeren Betriebs- und Arbeitskosten.

Prävention ohne Detektion

Die meisten Endpunkt-Absicherungstools verwenden einen reaktiven Ansatz - sie erkennen, wenn ein System kompromittiert wurde und versuchen dann, den Schaden unter Kontrolle zu bringen. AppGuard geht anders vor. Statt Malware zu erkennen, unterbricht AppGuard Malware proaktiv, um Sicherheitsverstöße zu verhindern. So bietet AppGuard besseren Schutz bei weniger Aufwand und Stress.

AppGuard überlistet böswillige Akteure, indem es autonom adaptive Richtlinienkontrollen auf das Verhalten von Anwendungen anwendet. AppGuard-Richtlinienkontrollen schränken die Art der Aktionen ein, die Malware an Endpunkten ausführen muss, um Schaden anzurichten (z.B. Befehl und Kontrolle oder Ausfiltern von Daten). Durch das Blockieren von Aktivitäten basierend auf Kontext schützt AppGuard Systeme in Echtzeit vor Malware, ungeachtet des Angriffsvektors oder der Art des Angriffs - ohne die Begrenzungen oder die mit der Kompromittierung verbundenen Folgekosten von erkennungsbasierten Tools.

Prävention am Endpunkt reduziert die Arbeit an den äußeren Ebenen und erhöht die Kapitalrendite bei vorhandenen Sicherheitstools. Wenn Malware den Endpunkt nicht durchbricht, gibt es für die anderen Tools (z.B. Netzwerk-Einbruchserkennung, Deception Grid, SIEM etc.) weniger Anzeichen, Kompromittierung zu erkennen, und sie produzieren weniger falsche Positive.

Präventive Kontrollen am Endpunkt reduzieren laterale Bewegung und die Arbeitsbelastung anderer Tools, was die Effizienz von Ressourcen und die Effektivität von Sicherheitsprogrammen erhöht.

> *“AppGuard sollte auf jedem Windows-System der Welt vorhanden sein.”* — Bob Bigman, CISO, CIA (i.R.)

Zero Trust innerhalb des Endpunkts

Zero-Trust-Security ist nicht länger bloß ein hochtrabendes Konzept. Das Schlüsselprinzip des Zero-Trust-Sicherheitsmodells gewährleistet, dass nur vertrauenswürdige Aktionen ausgeführt werden. Angesichts der Tatsache, dass der Endpunkt das Ziel der meisten Hacker ist, ist das Gewährleisten von Zero Trust innerhalb des Endpunkts entscheidend für das Vereiteln von Angriffen und das Verhindern von böswilligen lateralen Bewegungen innerhalb des Netzwerks. Durch das Anwenden von Zero Trust am Endpunkt stellt AppGuard sicher, dass Anwendungen und Dienstprogramme nicht von Hackern missbraucht werden können, um in Endpunkte einzudringen und Schaden anzurichten.

AppGuard erreicht Zero Trust innerhalb des Endpunkts durch adaptive Eingrenzung und Isolation, um die von der Malware geplanten Aktivitäten zu blockieren, indem es nicht akzeptable Aktivitäten oder Prozesse vor hochriskanten Anwendungen und Dienstprogrammen abschirmt. Durch das Eingrenzen, welche Aktionen innerhalb des Endpunkts erlaubt sind und statt gutes und schlechtes oder normales und unnormales Verhalten erkennen zu müssen, erhöht AppGuard die Widerstandsfähigkeit gegenüber Angriffen und verbessert die Sicherheitsaufstellung Ihrer Organisation, ohne die internen Ressourcen zu erschöpfen. Der Zero-Trust-Ansatz von AppGuard beim Absichern von Endpunkten versetzt Sie in die Lage, Angriffe zu stoppen, bevor sie beginnen.

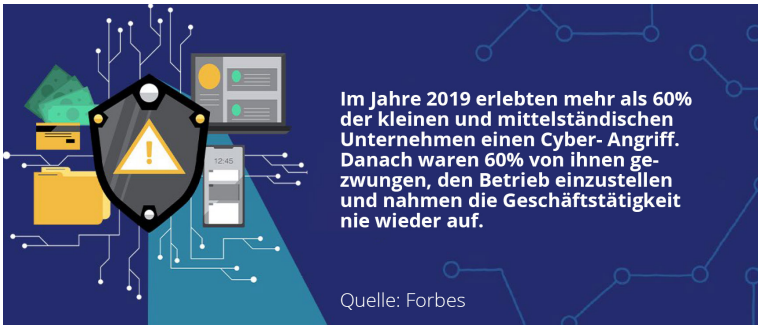
Richtliniengesteuerter Schutz

AppGuard arbeitet vom OS-Kernel aus und kann dadurch Echtzeit-Prozessdaten verwenden, um Anwendungsaktivitäten zu beurteilen und nicht vertrauenswürdige ausführbare Dateien und Skripte vom Starten abzuhalten. Vom Kernel aus kann es den Eltern-Kind-Ausführungspfad für jeden Prozess sehen (z.B. was den Prozess in Gang setzte und die Zwischenschritte, um zu der hochriskanten Aktivität zu gelangen). AppGuard passt seine Steuerung an und blockiert hochriskante Anwendungen nur, wenn sie von einer nicht vertrauenswürdigen Quelle ausgehen.

Standardmäßig sind die Agenten mit ihren Eingangs-Richtlinieneinstellungen voll funktionstüchtig und üben ihre Schutzfunktion aus, die Agenten laufen monate- oder jahrelang reibungslos ohne Richtlinienupdates. Anwendungsupdates, Patches oder Änderungen des Systems (einschließlich Malware-Evolution) verändern die Effizienz von AppGuard oder die Abläufe nicht, denn die Richtlinien sind nicht speziell auf die Anwendung oder das Dienstprogramm abgestimmt. Ausnahmen von den Standardrichtlinien können gemacht werden, wenn ein Administrator entscheidet, in einem bestimmten Zusammenhang aus betrieblichen Gründen eine hochriskante Aktivität zu erlauben. Bei Unternehmenseinsätzen wird das im AppGuard Management System (AGMS) kontrolliert.

Ruhen Sie sich nicht auf begrenztem Anti-Virus-Schutz aus, verbessern Sie ihn

Traditionelle Anti-Virus-Tools erbringen eine gewisse Leistung, haben jedoch erhebliche Einschränkungen, denn sie greifen auf zuvor erkannte Malware zurück. Tatsächlich kommen Berichte zu der Einschätzung, dass viele populäre Anti-Virus-Lösungen lediglich 40% der Angriffe erkennen können, da viele erfolgreiche Einbrüche durch unbekannte, Zero-Day- oder dateilose Malware erfolgen - Kategorien, die von signaturbasierenden Anti-Virus-Erkennungssystemen nicht identifiziert werden können.



Darüber hinaus scannen sie nur periodisch und nicht in Echtzeit. Selbst, wenn sie Malware finden, ist es oft zu spät. AppGuard agiert als die perfekte Ergänzung, denn es unterbricht Malware-Aktivitäten in Echtzeit, indem es gewährleistet, dass nur akzeptable Prozesse ausgeführt werden können, die den Richtlinien entsprechen. Sie bleiben in Sicherheit, während Ihr Anti-Virus-Programm die Zeit erhält, die es braucht, um später aufzuräumen.

AppGuard: Endpunkte schützen, das Geschäft sichern

Gute Sicherheit erleichtert überlasteten IT- und Sicherheitsabteilungen das Leben, statt es ihnen schwerer zu machen. Organisationen müssen eine Präventionsstrategie entwickeln und dürfen sich nicht alleine auf Erkennungs- oder Reparaturlösungen verlassen. Wenn AppGuard eingesetzt wird, können sich Organisationen in Sicherheit wiegen, dass ihre Endpunkte nicht kompromittiert werden.

Einfache, effektive Sicherheit, die vor der Kompromittierung einsetzt

- Keine zu untersuchenden Alarme
- Keine zu pflegenden Whitelists
- Keine künstliche Intelligenz, kein Maschinenlernen
- Keine Isolierung von Anwendungen, kein Sandboxing
- Keine Indikatoren für Kompromittierung, keine Indikatoren für Angriffe
- Kein Scannen von Festplatten

Unterstützte Plattformen:

- Windows XP – Windows 10
- Windows Server OS, 2008 R2 SP1, 2012 R2, 2016 und 2019
- Red Hat Enterprise Linux Server OS, 7.4, 7.5 und 7.6

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
The Malware Disruptor

www.appguard.us | software@ingrammicro.ch