APPGUARD
The Malware Disruptor

DATENBLATT

Schadsoftware unterbrechen, **bevor** sie Schaden anrichtet

Endpunkte sind verletzlich und das Bekämpfen von Malware ist schwer. Trotz erhöhter Ausgaben für Cybersecurity-Tools und Mitarbeiter umgeht Malware weiter bestehende Sicherheitstools, um Zugang zu den Endpunkten zu erhalten. Traditionelle Sicherheitsbarrieren wie Firewalls, sichere E-Mail-Gateways, IPSs, signaturbasierte Lösungen und Endpunkt-Absicherungsplattformen der nächsten Generation können bei Ihrer tiefgehenden Abwehrstrategie eine Rolle spielen. Jedoch sind sie beim Schutz vor fortschrittlichen Bedrohungen und Zero-Day-Aktivitäten unzulänglich.

Endpunkte ohne Kompromisse

Das ultimative Ziel bei der Investition in Endpunkt-Absicherungstools ist zu gewährleisten, dass das Unternehmen seinen Aufgaben nachgehen und Malware nicht machen kann, was sie will. 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 an den Endpunkten verringert den Aufwand an den äußeren Ebenen (keine zu verfolgenden Alarme, keine zu erkennenden Signaturen, kein Heer von in der Datenflut ertrinkenden Sicherheitsanalysten) und erhöht damit die Effizienz von Sicherheitsteams und die Effektivität von Sicherheitsprogrammen.

Datenschutzverletzungen mit der 3-Punkte-Regel-Absicherung verhindern

Zero-Trust-Bereich
STANDORTBASIERTE REGEL

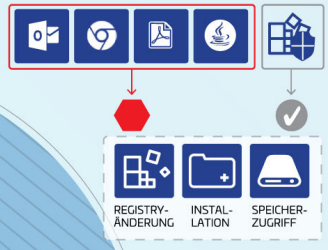
Wichtige Ordner des Betriebssystems werden im Systembereich separiert. **Anwendungen und Dienstprogramme können nur aus dem Systembereich heraus gestartet werden**, außer es wurde die Ausnahme „Vertrauenswürdig" gewährt.

Der Anwenderbereich ist „nicht vertrauenswürdiges" Terrain, in dem ausführbare Dateien nicht gestartet werden können.

Isolierung
OS-INTERAKTIONSREGEL (PATENTIERT)

Anwendungen im Systembereich sind in **hochriskante** und „normale" Anwendungen unterteilt.

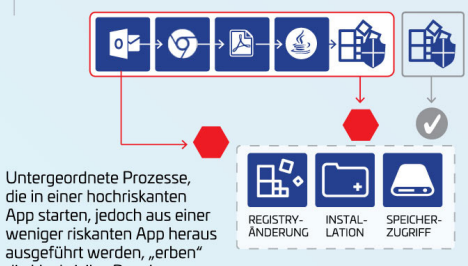
Hochriskante Apps werden daran gehindert, Prozesse auszuführen, die von der Malware benötigt werden, um Schaden anzurichten.



Vererbung
PROZESSAUSFÜHRUNGS-ABLAUFREGEL (PATENTIERT)

Die Vererbung stellt sicher, dass die Isolationsregeln für genauere Kontrollen und weniger Administrationsaufwand **automatisch angepasst** werden.

Fortschrittliche Malware kann ihre Aktionen nicht in einer normalerweise unbeschränkten Anwendung verbergen.



Untergeordnete Prozesse, die in einer hochriskanten App starten, jedoch aus einer weniger riskanten App heraus ausgeführt werden, „erben" die Hochrisiko-Regeln.

POST-START-RICHTLINIEN

Prävention ohne Detektion

AppGuards „Prävention ohne Detektion"-Philosophie beseitigt das Rätselraten bei der Unterscheidung von guten und schlechten Aktivitäten. Durch das Kontrollieren und Eingrenzen des Verhaltens von Anwendungen und Dienstprogrammen stellt AppGuard sicher, dass ausgeführte Prozesse im Rahmen der festgelegten Richtlinien stattfinden. Dadurch werden riskante Aktivitäten von Malware ungeachtet der Form reduziert, die sie annimmt - neu oder alt. So kann AppGuard Vermögenswerte vor böswilligen Prozessen unbekannter Herkunft schützen, ohne dass die Malware oder ihre Auswirkungen bekannt sein müssen.

Malware an der Quelle unterbrechen

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.

Sichere Architektur

Bei Unternehmenseinsätzen werden Richtlinien zentral im AppGuard Management System (AGMS) kontrolliert. Die AGMS-Konsole generiert Agenten-Installationspakete, erstellt und verteilt Richtlinien und sammelt und prüft Endpunkt-Logs. Richtlinien werden über einen Relais-Server verteilt, die der Agent regelmäßig prüft und die Möglichkeit einer Hintertür beseitigt. Standardmäßig sind die Agenten mit ihren Eingangs-Richtlinieneinstellungen voll funktionstüchtig und üben ihre Schutzfunktion aus. Die Agenten laufen monate- oder jahrelang reibungslos ohne Richtlinienupdates oder Internetanschluss. 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.

Einfache, effektive Sicherheit, die vor der Kompromittierung eingreift

- 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

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

Prävention ohne Detektion

Überlisten Sie böswillige Akteure, bevor Malware Schaden anrichten kann. AppGuard verhindert das Ausführen von böswilligem Code, ohne dass die Malware oder ihre Auswirkungen erkannt werden müssen. Alternativen sind nur erfolgreich, wenn sie die böse Absicht erkennen. AppGuards Erfolg ist nicht davon abhängig.

Zero Trust innerhalb des Endpunkts

Adaptive Eingrenzung und Isolation blockieren die beabsichtigten Aktivitäten der Malware. AppGuard grenzt das Starten von Anwendungen auf nachweislich vertrauenswürdige Aktivitäten ein und begrenzt die Möglichkeiten von hochriskanten vertrauenswürdigen Aktivitäten.

Universelles, virtuelles Patching

Nicht gepatchte Anwendungen sind attraktive Angriffsflächen für Gegner. Es ist nicht einfach, mit Patches auf dem Laufenden zu bleiben. Die adaptive Eingrenzung von AppGuard blockiert Gegner, die das Fehlen von Patches zu ihrem Vorteil ausnutzen wollen.

Größere Sicherheit, weniger Aufwand, weniger erforderliche Ressourcen

Adaptive Präventionskontrollen heißt keine Alarme, keine Untersuchungen, kein Threat-Hunting und keine zu pflegenden Whitelists - nur erhöhter Schutz mit geringeren Betriebs- und Arbeitskosten.

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