Erhöhte Sicherheit. Weniger Ressourcen.

Cylance verbessert den Endpunktschutz ohne Auswirkungen auf die PC-Leistung

CYLANCE™

Einführung

Wenn man sich die Anzahl der Schlagzeilen ansieht, die täglich über kritische Datenschutzverletzungen zu lesen sind - trotz immer höher werdender Ausgaben für die Sicherheitstechnologie - ist klar, dass irgendetwas nicht funktioniert.

Tatsächlich sind die traditionellen Methoden zum Schutz der IT-Ressourcen heutzutage angesichts der immer komplexer werdenden Bedrohungen nicht mehr effizient genug. Viele Anbieter vertreten die Meinung, dass es besser ist, mehrere verschiedenartige Technologien einzusetzen, um gegen Bedrohungen besser geschützt zu sein, da diese jeweils auf andere Typen spezialisiert sind. Diese Produkte sind jedoch nicht skalierbar und ihr Schutz wird mit der Zeit immer schwächer. Auch die Verwendung von mehreren Produkten dieser Art ist nicht ausreichend, um moderne Malware-Angriffe zu identifizieren und zu stoppen.

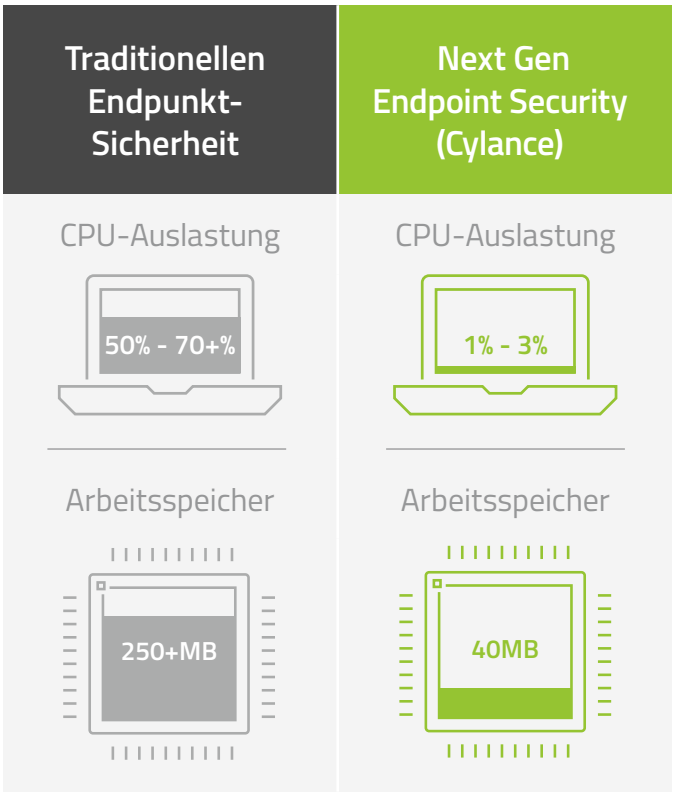
Ein Teil des Problems ist, dass bei der Anwendung von immer mehr Sicherheitstechnologien auch die Kosten steigen, denn es sind mehr Infrastrukturen, Ressourcen, Server, Bandbreiten, Anwendungen etc. erforderlich. Außerdem haben viele dieser Produkte negative Auswirkungen auf die Systeme und Anwendungen, wodurch die Produktivität der Endbenutzer und der Organisation reduziert wird. Ältere Sicherheits-Tools kosten mehr Zeit und Geld, als es sich viele Unternehmen bewusst sind.

Die Zeit ist reif für einen neuen Ansatz in der Cyber-Security, der die Schwächen der alten Systeme überwindet. Heute haben Organisationen die Gelegenheit, sich für Sicherheitslösungen zu entscheiden, die auf modernen Technologien - wie künstlicher Intelligenz und maschinellem Lernen - aufbauen. Diese Methoden sind speziell konzipiert, komplexe, moderne Angriffe zu stoppen, ohne, dass es dabei zu Einbußen der Systemleistung oder erhöhten Kosten kommt. In diesem Whitepaper werden einige der wichtigsten Nachteile der traditionellen Methoden für die Endpunktsicherheit beschrieben. Außerdem wird erklärt, wie Organisationen unterschiedlicher Größen und aus verschiedenen Branchen die Fortschritte auf dem Gebiet der Sicherheitstechnologien nutzen können, um Ihre Systeme und Daten so kosteneffizient wie möglich gegen Bedrohungen zu schützen.

Die traditionelle Sicherheit beeinträchtigt die Systemleistung und erhöht die Kosten

Einer der größten Nachteile von traditionellen Sicherheitslösungen ist, dass Sie sich sowohl nachteilig auf die Systemleistung auswirken als auch zu höheren Kosten führen.

Unternehmen, die traditionelle Sicherheitswerkzeuge verwenden, müssen riesige Signaturdatenbanken pflegen, in denen bekannte Malware bzw. zugelassene Anwendungen gespeichert werden. Außerdem müssen sie immer wieder zusätzliche Hardware und Software bereitstellen (mit geringer oder fehlender Integration); neue Dateisignaturen



TES – CPU-Verwendung: 50 -70+ %; Arbeitsspeicher: 250+ MB

NGES (Cylance) – CPU-Verwendung: 1-3%; Arbeitsspeicher: 40MB Leichtgewichtig und kaum wahrnehmbar

herunterladen, um die Datenbank aktuell zu halten; und tägliche Scans sowie Echtzeitscans des Arbeitsspeichers, von E-Mails etc. durchführen.

Dies benötigt viele CPU-Ressourcen und führt zu einem ineffizienten Betrieb. Durchschnittlich verwenden traditionelle Endpunkt-Sicherheitsprodukte 50 bis 70 % der CPU-Zyklen, wenn intensive Scans durchgeführt werden.

Dies führt bei vielen Unternehmen zu konstanten Beschwerden der Endbenutzer, die sich fragen, warum ihre Systeme so langsam sind und warum sie jeden Morgen 15 Minuten warten müssen, bis ihr PC startet. Dies erhöht die Kosten und reduziert die Produktivität noch weiter, da durch die Anrufe von Benutzern beim Helpdesk noch mehr Ressourcen verschwendet werden.

Eine solche negative Auswirkung auf die Leistung steht im Gegensatz zum Ziel eines modernen Unternehmens: moderne Systeme und effiziente Anwendungen, die es den Angestellten ermöglichen sollen, ihre Aufgaben schneller und effizienter zu erledigen. Wenn die Systeme langsam sind, werden auch die Aufgaben des Kunden nur langsam erledigt, und die Entwicklung neuer Produkte und Dienstleistungen oder der Start neuer Marketingkampagnen können verzögert werden.

Die Auswirkung auf das operative Geschäft und die Tätigkeit Ihres Unternehmens kann dabei dramatisch sein. Es ist klar, dass Sicherheitslösungen Angriffe effizient stoppen müssen, allerdings nicht auf Kosten der Leistung und der Zufriedenheit der Angestellten und Kunden.

Neue Studien zeigen, was für schwerwiegende Auswirkungen die Sicherheitstechnologie auf die Benutzererfahrung haben kann. Eine Online-Befragung von 460 IT-Experten und 301 Geschäftsbenutzern in den USA, im Vereinigten Königreich und in Deutschland, die 2015 von Dimensional Research als Auftrag von Dell durchgeführt wurde ergiebt, dass 91% der Befragten durch konventionellen Sicherheitsmaßnahmen ihrer Arbeitgeber negativ beeinträchtigt werden. Die große Mehrheit der Befragten (92%) gab an, von den zusätzlichen Sicherheitsmaßnahmen für Remote-Arbeit negativ betroffen zu sein. Untersuchungen der Änderungen der Sicherheitsrichtlinien der Unternehmen in den letzten 18 Monaten ergaben, dass bei der Hälfte der Befragten die negativen Auswirkungen auf die tägliche Arbeit zugenommen haben.

Der negative Effekt auf die Effizienz und die Benutzererfahrung kann auch andere Konsequenzen für Organisationen haben. So gaben z. B. fast 70% der IT-Experten in einer Umfrage von Dimension Research an, dass die Behelfslösungen von Angestellten zur Vermeidung von Sicherheitsmaßnahmen das größte Risiko für eine Organisation darstellen. Was das Problem der Systemleistung noch erschwert, ist, dass die Entscheidungsträger bei der Evaluierung von Sicherheitslösungen nur selten die Auswirkungen solcher Produkte auf Systeme und Ressourcen in Betracht ziehen.

Abgesehen von den Leistungseinbußen sind auch die erhöhten Kosten ein Problem der auf signaturbasierten Sicherheitsprodukte - sowohl aufgrund der zeitlichen und monetären Ressourcen als auch aufgrund der Kosten der Sicherheitsvorfälle, die bei einer unzureichenden Sicherheitsarchitektur auftreten können.

So sind zum Beispiel signaturbasiert Produkte oft ineffizient gegen Malware, weshalb viele Organisationen zusätzliche Sicherheitstechnologien - inkl. Endpunktschutz- und Response-Lösungen - implementieren müssen, wodurch weitere Kosten entstehen. Anstatt zu versuchen, die Malware zu stoppen, bevor sie auf den Systemen ausgeführt werden kann, suchen diese Lösungen nach Indizien einer Kompromittierung, die von einer ausgeführten Malware hinterlassen wurde. Für die Bedienung dieser Tools sind gut ausgebildete und hoch bezahlte Fachleute erforderlich.

In vielen Fällen wird dies erst dann gemacht, wenn die Malware bereits innerhalb der Organisation von einem System zum anderen gesprungen ist - was die Organisation oft teuer zu stehen kommt. Außerdem erfassen solche Lösungen, welche die meisten Systemereignisse zum Zwecke der Erkennung und Reaktion erfassen und speichern, oft mehr Informationen also notwendig, was zu einer noch höheren Ressourcenauslastung führt.

Was den Zeit- und Kostenaufwand betrifft, führen genaue Scans von Signatur-basierten Anti-Malware-Programmen oft zu Arbeitsverzögerungen und dementsprechend zu einem Verlust der Produktivität. Wenn zweimal täglich 10 Minuten lange Scans durchgeführt werden, und man dies mit der Anzahl der Benutzer innerhalb eines Netzwerks multipliziert, so wird klar, dass diese Scans schwerwiegende finanzielle Auswirkungen auf ein Unternehmen haben können.

Es entstehen zusätzliche Kosten, wenn immer mehr Malware in eine Organisation eindringt. Dies betrifft die Beseitigung von Malware-Problemen, die Neuinstallation von Geräten, die reduzierte Produktivität der Anwender, Schulungs- und Ausbildungsbedarf sowie Kosten von Rechtsstreitigkeiten (sollten externe Ansprüche entstanden sein).

Signatur-basierte Produkte müssen auch gewartet werden, insbesondere in Hinblick auf die Verteilung der Signaturen. Dies wird normalerweise einmal pro Tag gemacht, in manchen Fällen aber auch mehrmals pro Stunde. Bei Offline-Systemen sind noch intensivere Wartungsmaßnahmen notwendig, da die Updates nicht direkt von der Internetseite des Anbieters bezogen werden können. Die Administratoren müssen deshalb jedes einzelne Update manuell herunterladen, die Daten auf Wechselmedien kopieren, diese wiederum auf Malware überprüfen und die Updates dann auf die Systeme im Offline-Netzwerk übertragen.

Traditionelle Sicherheitsanbieter zwingen Ihre Kunden dazu, immer mehr Abwehrstufen auf den Endpunkten einzusetzen, um zu versuchen, den Schutz zu verbessern. Diese zusätzliche Technologie, z. B. Host Intrusion Prevention und reputationbasierte Datei-Lookups, führt zu zusätzlichen Installationen, Hardware und Verwaltungsmaßnahmen. Viellfach kann es vorkommen, 10 und mehr verschiedene Prozesse zur Endpunktsicherheit innerhalb einer Organisation angewendet werden.

Fehlender Schutz

Nicht nur haben Signatur-basierte Sicherheitsprodukte negative Auswirkungen auf die Systemleistung und führen zu erhöhten Kosten, sie erfüllen Ihren Zweck nicht mehr, nämlich die Organisationen gegen schädliche Inhalte zu schützen. Keiner der Anbieter von traditionellen Endpunkt-Sicherheitslösungen kann ausreichend verhindern, dass Malware ausgeführt wird. Per Definition haben Signatur-basierte Antivirus-Systeme immer einen “Patienten Null”, da Malware bereits zuvor gesehen werden muss, bevor eine Signatur geschrieben werden kann. Fast alle neuen Bedrohungen sind “Zero Day”-Angriffe, die verschiedene Techniken verwenden, deren Ausführung unbedingt vermieden werden muss.

Dies ist einer der Nachteile der Überwachung von Software nach der Ausführung. Meistens besteht ein böswilliges Verhalten aus einer Reihe Aktionen. Wenn diese nicht rechtzeitig identifiziert werden, kann es bereits zu spät sein, um Malware zu blockieren. Bei manchen Lösungen dauert es mehrere Minuten oder sogar Tage und Wochen, um solche Feststellungen zu treffen.

Ein weiterer bedeutender Nachteil von Signatur-basierten Sicherheitsmethoden ist, dass Organisationen abhängig vom Risiko oft bis zu 72 Stunden auf eine Signatur warten müssen. Um eine Signaturdatei zu entwickeln, sind mehrere Schritte erforderlich. Je mehr Zeit jedoch ohne Schutz verstreicht, desto mehr Endpunkte werden infiziert, was mehr Geld kostet.

Das Ponemon Institute fand in einer Studie über die Kosten von Datenverletzungen 2016 heraus, dass die durchschnittlichen Gesamtkosten von 383 an der Studie teilnehmenden Unternehmen bei ca. 4 Millionen USD lagen. Die durchschnittlichen Kosten für jeden einzelnen verlorenen oder gestohlenen Datensatz mit vertraulichen Informationen lagen bei 158 USD.

Außerdem entstehen durch Attacken, welche von Signatur-basierten Tools nicht gestoppt werden können, auch indirekte Kosten. Dies betrifft unter anderem den Schaden am guten Ruf einer Marke, die unbekannten Kosten gestohlener oder verlorener Unternehmensinformationen oder Staatsgeheimnisse etc.

Die Sicherheitsbedrohungen haben sich im Laufe der Jahre weiterentwickelt und sind wesentlich raffinierter geworden; außerdem können sie leicht mutiert werden und somit neue, nur schwer zu erkennende Formen annehmen. Heutzutage ist fast jede Malware-Variante polymorph, also sehr zielgerichtet und anpassbar. Es ist für mutierte Malware-Typen sehr leicht, traditionelle Analysmittel wie Dateisignaturen, heuristische Methoden oder Crosschecks zu umgehen. Und da die Malware ihre Umgebung auf dynamische Analysetechniken wie Sandboxing kontrolliert, sind solche Techniken nach wie vor umgehbar.

Obwohl sich die Cyber Security ständig verändert, sind die grundlegenden Komponenten der Malware-Erkennung seit über drei Jahrzehnten gleich geblieben.

Die veraltete Antivirus-Technologie ist ineffizient gegen die enormen Wellen an raffinierten Attacken mit zahllosen Malware-Varianten, die heute zu beobachten sind. So können z. B. Angreifer eine “mutierte” Malware mit leicht erhältlicher Packer-Software ganz einfach “verkleiden”. Diese Software modifiziert die Attribute der Software und ändert die kryptographischen Hash-Schlüssel, was eine einfache Penetration und Umgehung der Signatur-basierten Antivirusprogramme ermöglicht; so einfach, wie der Wechsel des Kennzeichens bei einem gestohlenen Auto. Analysen zeigen dass 99% von Malware-Hashes höchstens 58 Sekunden lang zu sehen sind, und dass die meiste Malware nur einmal zu sehen ist. Dies bestätigt, wie einfach Hacker ihren Code ändern können, um einer Erkennung zu entgehen.

Wenn man sich die große Anzahl an erfolgreichen Angriffen der letzten Jahre ansieht, wird klar, dass die traditionellen Ansätze nicht mehr funktionieren. Und die Situation wird auch sicher nicht besser werden. Diese Produkte werden sich nicht verbessern, da sie auf reaktiver Technologie basieren. Sie basieren auf Code, der vor Jahrzehnten geschrieben wurde und einen reaktiven Schutz bietet, wodurch die Wahrscheinlichkeit eines Schadens erhöht wird. Außerdem müssen die Kunden dadurch mehrere Technologien erwerben und zusammenstückeln, was wiederum zu erhöhten Betriebs- und Hardwarekosten führt.

Letztlich verkaufen die traditionellen Anbieter heute verschiedene Add-on-Technologien, die immer höhere Anforderungen an die Endpunktsysteme stellen, mit noch mehr Agenten, auszuführender Software und Verwaltungsschnittstellen - all dies führt zu einem Kostenanstieg. Doch das ist noch nicht alles! Durch diese verschiedenen Schichten an Code werden die bestehenden Programme immer instabiler und laufen nicht mehr optimal.

Ein intelligenterer Sicherheitsansatz

Ein neuer, moderner Ansatz zur Sicherheit bietet eine Alternative zu den veralteten Signatur-basierten Werkzeugen und Helfer-Produkten Die Technologie von Cylance konzentriert sich auf proaktiven Schutz und Prävention, also nicht auf der Reaktion nach dem Auftreten von Vorfällen. Durch künstliche Intelligenz und maschinelles Lernen werden Malware und “Zero Day”-Bedrohungen sofort erkannt und ihre Ausführung auf der Host-Maschine wird verhindert. Dies ermöglicht es den Organisationen, sich gegen solche Bedrohungen auch ohne Signaturen zu schützen. Mathematische und auf maschinellem Lernen basierte Modelle verhindern, dass die Systeme infiziert und beschädigt werden.

Da sich diese Lösung auf den einzelnen Endpunkten befindet und auf proaktive Weise gegen Malware arbeitet, können sich die Organisationen effizienter gegen moderne, fortschrittliche Angriffe schützen.

Im Gegensatz zu den herkömmlichen Methoden, die reaktiv sind und es oft nicht schaffen, die Malware zu stoppen, ist dies also ein proaktiver Ansatz. Dadurch kann 99% der Malware, die Endpunkte angreift, gestoppt werden, verglichen mit 60 bis 70% bei den traditionellen, Signatur-basierten Produkten.

Dieser Ansatz garantiert also nicht nur eine verbesserte Sicherheit, sondern löst auch die Probleme der reduzierten Systemleistung. Da keine Signaturen verwendet werden

und weniger Technologie notwendig ist, werden viel weniger Ressourcen - z. B. CPU und Arbeitsspeicher - verwendet. Eine gute Schutzarchitektur sollte von den Benutzern kaum wahrgenommen werden und muss für die Administratoren leicht bereitzustellen und zu verwalten sein.

Wie oben erwähnt, ist es ein kritischer Schwachpunkt das traditionelle Sicherheitstechnologien sich auf umfangreiche Signaturdatenbanken verlassen, in denen bekannte Malware und zugelassene Anwendungen gespeichert werden. Moderne Lösungen sind in der Lage, in Echtzeit Entscheidungen an einem Endpunkt zu treffen, und zwar durch die Anwendung von Modellen der künstlichen Intelligenz, die nur wenige Male pro Jahr aktualisiert werden. Es ist also nicht mehr notwendig, ständig neue Dateisignaturen herunterzuladen.

Diese neue Sicherheitslösung benötigt weniger Systemressourcen, da ein Endpunkt nicht mehr mit großem Aufwand überwacht werden muss. Als Resultat davon ist die Präsenz dieser Lösung auf dem Betriebssystem und den Anwendungen sowohl für den Endbenutzer als auch den Endpunkt kaum wahrnehmbar.

Diese Lösungen ermöglichen es den Organisationen auch, den hohen finanziellen Aufwand zu vermeiden, der mit den traditionellen Methoden verbunden sind. Dank effizienteren Abwehrmechanismen gegen Malware müssen die Organisationen keine Endpunkt-Erkennungs- und Sicherheitstools verwenden, für deren Bedienung gut ausgebildete Experten angestellt werden müssen. Diese ersetzen veraltete Methoden, die nur in der Lage sind, Malware zu finden, nachdem diese bereits ausgeführt wurde und der Organisation möglicherweise bereits geschadet hat.

Es sind keine ständigen erneuten Scans an den Endpunkten mehr notwendig, und langen Arbeitsverzögerungen werden vermieden. Bei Unternehmen mit hunderten Benutzern innerhalb eines Netzwerks führt dies zu einer deutlichen Reduzierung der Ausgaben. Außerdem wird die kostenintensive Wartung von Signatur-basierten Produkten eliminiert.

Durch den soliden Sicherheitsansatz moderner Lösungen können sich Organisationen also besser gegen Angriffe schützen. So können Kosten in Millionenhöhe wegen Datenverlust, Anwaltskosten, Strafen von Aufsichtsbehörden etc. vermieden werden. Außerdem kommt es nicht zu immateriellen Kosten wie Schäden am Ruf einer Marke.

Ein weiterer Vorteil moderner Lösungen ist, dass sich das Sicherheits- und IT-Personal auf strategischere, innovativere Projekte konzentrieren kann. Dies ist möglich, da verglichen mit Signatur-basierten Tools ein geringerer Zeitaufwand nötig ist.

Zusammenfassung und Fazit

Organisationen, die sich auf Signatur-basierte Sicherheitsprodukte verlassen, haben nichts falsch gemacht. Sie hatten einfach keine andere Wahl, da es keine besseren Lösungen auf dem Markt gab. Es ist allerdings eine Tatsache, dass diese Produkte keinen angemessenen Schutz gegen die Sicherheitsbedrohungen von heute gewähren und mit der Zeit immer ineffizienter werden.

Da die Komplexität der Angriffe deutlich zugenommen hat, können die alten Methoden heute nicht mehr schritthalten. Durch Malware-Mutation können Angreifer dieselben Angriffsvektoren und Werkzeuge bei neuen, nicht erkennbaren Angriffen anwenden. Deshalb ist eine intelligentere Antivirus-Lösung notwendig, um die Ausführung von bisher unbekannten Bedrohungen zu verhindern und die ständige “Zero Day”-Malware-Offensive abzuwehren

Außerdem haben diese veralteten Lösungen negative Auswirkungen auf die Effizienz wichtiger Unternehmenssysteme und -anwendungen und führen zu einer Erhöhung der Gesamt-Sicherheitskosten, da mehrere Schichten von Verteidigungsmechanismen notwendig wurden.

Jetzt gibt es aber eine Alternative. Proaktive Sicherheitslösungen, die Angriffe abwehren und Bedrohungen erkennen, bevor diese zuschlagen, führen zu einem verbesserten Sicherheitsniveau sowie einer Steigerung der Systemleistung und einer Kostenersparnis. Sie verfolgen die Aktivität von Angreifern und Malware-Autoren und stoppen Angriffe, bevor Sie die Schaden anrichten.

Dieser moderne Ansatz zur Sicherheit wirkt sich vor allem in drei Schlüsselbereichen aus: maximaler Schutz für Daten und Systeme, Bereitstellung des Schutzes ohne Beeinträchtigung der Leistung, Kostenersparnis sowie strategische Vorteile, da die IT- und Sicherheitsmitarbeiter an wichtigen, langfristigen Projekten arbeiten können, anstatt durch die Reaktion auf tägliche Vorfälle Zeit zu verlieren.

Anstatt sich auf die Behauptungen von Anbietern zu verlassen, empfiehlt es Cylance Ihren IT- und Sicherheitsexperten, unsere Lösung in einer realen Umgebung mit einem traditionellen Sicherheitsprodukt zu vergleichen. Cylance bietet kostenlose Machbarkeitsstudien an, welche die Evaluierung der Technologie gegenüber vorhandene Lösungen erlaubt. Die notwendigen Informationen finden Sie unter www.cylance.com.

+49-89-244455571
sales@cylance.com
www.cylance.com
Second Floor, 89/90 South Mall, Cork City, Ireland T12 RPP0

CYLANCE™

20161213