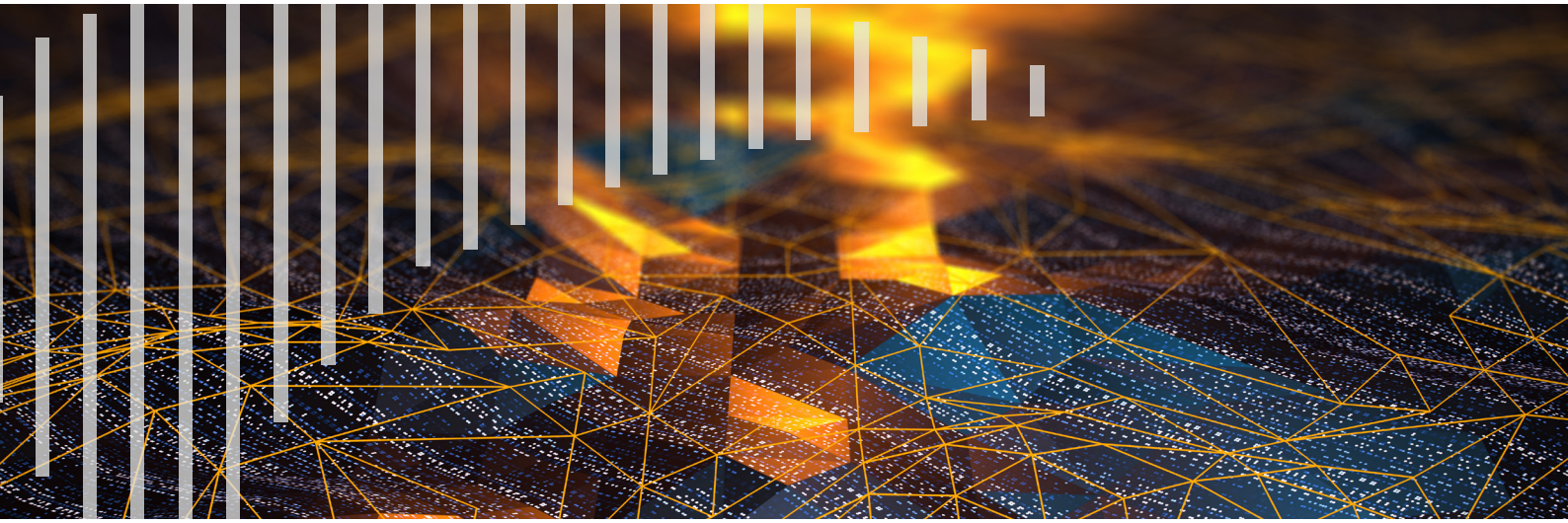

LÖSUNGSPROFIL:

Ein fortschrittlicher Ansatz für On-Prem Sandboxing

Gleichgewicht zwischen Genauigkeit, Kosten und Compliance beim Schutz sensibler Daten im Haus

Zusammenfassung

Große Organisationen und Behörden brauchen für die Abwehr komplexer Malware fortschrittliche Sicherheitstechnologien, wie Sandboxing. Viele dieser Organisationen unterliegen strengen Vorschriften, unter denen sensible Daten ausschließlich intern verwaltet werden dürfen. Für solche Organisationen kommen keine Cloud-basierten Lösungen in Frage. Dieses Lösungsbrief untersucht einen fortschrittlichen Ansatz für On-Prem Sandboxing, der schnell, hochpräzise und wirtschaftlich ist.

Warum ist Sandboxing erforderlich

Herkömmliche Sicherheitstechnologien für Netzwerke identifizieren bekannte Bedrohungen anhand deren Definitionen und Signaturen, können aber keine neuen und aktualisierten komplexen Bedrohungen wie Malware und Zero-Day Exploits erkennen. Heutige Schadcode-Urheber nutzen fortschrittliche Methoden, darunter individuelle Verschlüsselung, Verschleierung und Verpackung. Darüber hinaus verhält sich die Malware in Sandbox-Umgebungen friedlich und verbirgt damit ihr Gefahrenpotenzial. Mit diesen Methoden lassen sich oft hochkomplexe Angriffsarten verbergen, die nur während eines dynamischen Laufs entdeckt und mit statischen Erkennungsmethoden meist nicht in Echtzeit analysiert werden können.

Für eine bessere Identifizierung unbekannter Bedrohungen setzen Security-Experten heute fortschrittliche Technologien wie Sandboxen ein, durch die das Verhalten von verdächtigen Dateien vorab analysiert und versteckte Malware aufgedeckt werden kann. Netzwerk-Sandbox-Engines führen Dateien aus, protokollieren die resultierende Aktivität und suchen dann, nach der Ausführung, nach schädlichem Verhalten und versuchen Korrelationen herzustellen.

Bei vielen Arten von Attacken wird das Arsenal erst im Arbeitsspeicher offengelegt. Deshalb ist ein Arbeitsspeicher-basierter Ansatz sinnvoll, mit dem Angriffe erkannt und gestoppt werden können, bevor sie die Endpunkte erreichen.

Mit Sandboxing verbundene Herausforderungen

Cloud-basiertes Sandboxing erstellt die niedrigste Barriere in Bezug auf die Erkennung neuer und aktualisierter Angriffsvarianten. Auch wenn die Sicherheitsfunktion perfekt ist, ergeben sich bei diesem Modell doch zwei Herausforderungen. Zum einen verlässt sich dieses Modell auf Points of Presence (PoPs), also Knotenpunkte, an die Security-Appliances/Dienste und Security-Experten die Dateien zur Analyse senden. Bei einer langsamen Internetverbindung oder großen Entfernung zwischen dem Dienst und dem Absender kann dabei eine maßgebliche Latenz entstehen. Zum anderen ist es vielen mit sensiblen Daten arbeitenden und strikten regulatorischen Vorgaben unterliegenden Organisationen und Behörden untersagt, die Daten außer Haus (oder in einigen Fällen außerhalb des Landes oder der Region) zu verlagern. In diesen Fällen können keine verdächtigen Dateien zur Analyse in Cloud-basierte Sandboxen übertragen werden.

Diese Organisationen und Behörden verwenden infolge dessen On-Premise-Sandboxes, die innerhalb ihrer Rechenzentren implementiert werden. Dieses Sandboxing-Modell ist allerdings sehr kostspielig und wie bei den

meisten Cloud-basierten Sandboxen sind auch hier viele Ausweichtaktiken dokumentiert[1]. Des Weiteren neigen Korrelation und Bewertung der Aktivitäten und Verhaltensweisen in beiden Sandboxing-Modellen zu falsch-positiven und falsch-negativen Ergebnissen.

Ein balancierter Ansatz

Was Organisationen für eine wirksame Sicherheit unter Aufrechterhaltung der Konformität mit allen Vorschriften und Datenschutzrichtlinien brauchen, ist eine budgetfreundliche On-Prem Bedrohungsanalyseplattform, die von Schadprogrammen nicht erkannt oder umgangen werden kann und ein schnelles Urteil liefert.

Eine optimal balancierte Lösung inspiziert verdächtige Dateien innerhalb des Rechenzentrums mittels einer schnellen und präzisen im Arbeitsspeicher basierten Analyse, um so eine starke Schutzschicht zur Abwehr komplexer und gezielter Bedrohungen bereitzustellen. Gleichzeitig sollte sie leicht zu verwalten sein und die TCO reduzieren, um auch den Budgetanforderungen gerecht zu werden.

Lösung: SonicWall Capture Security *Appliance*

Die SonicWall Capture Security Appliance (CS*a)* ist eine On-Prem-Lösung für die Dateianalyse und Malware-Erkennung, die auch die zum Patent angemeldete Real-Time Deep Memory Inspection (RTDMI™) Technologie beinhaltet. RTDMI erweitert den Schutz auf Malware, die andere Erkennungsmethoden umgeht, und liefert weit über fünfzig Prozent aller Urteile in innerhalb von fünf Sekunden.

CS*a* erkennt mehr Malware und ist schneller als Netzwerk-Sandboxing-Lösungen. Des Weiteren hat CS*a* eine niedrigere Falsch-positiv-Rate, was zu mehr Sicherheit und einer besseren Endbenutzererfahrung beiträgt. Die Lösung analysiert und erkennt versteckte Malware in einer Vielzahl von Dateiarten, Dateigrößen und Betriebssystemen und bietet somit eine optimale umfassende Zero-Day Bedrohungserkennung.

Des Weiteren setzt CS*a* arbeitsspeicherbasierte Inspektionsmethoden ein, mit denen auch potenzielle Seitenkanal-Angriffe erkannt werden können. Da CS *a* die Malware proaktiv zwingt, sich im Arbeitsspeicher zu enttarnen, blockiert sie auch Massenmarkt- und Zero-Day Bedrohungen sowie unbekannte Malware.

So funktioniert diese Lösung

CS*a* erkennt und blockiert Schadcode, der kein schädliches Verhalten zeigt und seine zerstörerische Kraft durch Verschlüsselung verbirgt. Die Erkennung von Malware-Code, der zur Vermeidung einer Erkennung verpackt und komprimiert ist, wird durch die RTDMI-Engine ermöglicht. RTDMI entpackt den komprimierten Code im Arbeitsspeicher und legt so die enthaltene Malware offen. Dabei werden die enthaltenen Codesequenzen erfasst und mit den bereits durch mehrere andere dynamische Inspektionstechniken erkannten Codes verglichen. Die Identifizierung von bösartigem Code im Arbeitsspeicher ist weitaus genauer als eine Differenzierung zwischen dem Verhalten von bösartigen Systemen und gutartigen Systemen – ein Ansatz, der von den meisten anderen Analysetechniken verwendet wird.

CS*a* ist nicht nur genauer, sondern auch wesentlich schneller. Da der bösartige Code bzw. die Daten im Arbeitsspeicher in Echtzeit während der Ausführung des Codes erkannt werden, muss erst gar kein bösartiges Verhalten erfolgen, um eine Erkennung zu ermöglichen Das Urteil wird schneller gefällt, da die Gegenwart von bösartigem Code erkannt wird, bevor irgendein schädliches Verhalten stattfindet.

Im Gegensatz zu verhaltensbasierten Systemen, die nur bis auf Ebene der APIs und System-Calls suchen, können mit der granularen, bis auf Ebene der CPU-Anweisungen reichenden RTDMI auch neue Formen von Malware gestoppt werden, die sich Meltdown, Spectre oder andere Seitenkanal-Schwachstellen zunutze machen.

Analyse eines weiten Bereichs von Dateitypen

CS*a* mit RTDMI stoppt auch neue Formen von dokumentenbasierter Malware sehr effektiv, einschließlich in PDFs und MS Office-Dateien eingebetteten bösartigen Code. In einem Direktvergleich mit Netzwerk-Sandboxing-Technologien anderer Anbieter schnitt CS*a* in Bezug auf die Schnelligkeit der Erkennung wesentlich besser ab. Durch diese Schnelligkeit wird eine bessere Abwehr von Phishing-E-Mails, die solche Dateien enthalten, ermöglicht, da bei einigen anderen Sandboxing-Modellen in solchen Fällen eine maßgebliche Latenz verursacht wird.

Des Weiteren nutzt diese Appliance eine proprietäre Exploit-Erkennungstechnologie und statische Inspektionsmethode für die dynamische Analyse der Dokumente und kann somit viele bösartige Dokumentkategorien erkennen, einschließlich

- Bösartige Flash-basierte MS Office-Dokumente
- DDE(Dynamic Data Exchange)-basierte Exploits und Schadprogramme in Office-Dateien
- MS Office- und PDF-Dateien mit schädlichen ausführbaren Dateien
- PDF-Dokumente, die MS Office-Malware enthalten
- Shellcode-basierte schädliche Dateien
- Makro-basierte schädliche Dateien
- Bösartige mehrschichtige Dateien
- PDF-Dokumente mit „JavaScript-Infektoren“
- JavaScript-basierte Exploits in PDF-Dokumenten

- Dateien, die zu Phishing- und Malware-Websites weiterleiten
- Bösartige PDF-Dokumente im „Phishing-Stil“, die zu Phishing-Websites und Websites weiterleiten, auf denen Schadprogramme gehostet werden

CS*a* unterstützt die Analyse unterschiedlichster Dateitypen, darunter ausführbare Programme (PE), DLL, PDFs, MS Office-Dokumente, Archive, JAR und APK sowie unterschiedliche Betriebssysteme wie Windows, Android und Multi-Browser-Umgebungen. Administratoren können können den Schutz bedarfsgerecht einrichten, indem sie Dateien für die Cloud-Analyse auswählen oder von dieser ausschließen, z. B. nach Dateityp, Dateigröße, Absender, Empfänger und Protokoll. Dateien können auch manuell zur Analyse an die Appliance geleitet werden.

Einfaches Verwalten und Reporting

Leicht verständliche Berichte zeigen auf übersichtliche Weise die Gründe für eine Blockierung, Details zur den Analyseergebnissen für die an den Dienst gesandten Dateien, u. a. auch Session-Informationen, OS-Informationen, OS-Aktivität, Netzwerkaktivität und eine Kopie der Originaldatei (abhängig von den Datenschutzeinstellungen). Protokollmeldungen informieren über die an die CS*a* gesandten verdächtigen Dateien sowie über die Dateianalyse und das letztendliche Urteil.

Einbindungsoptionen

CS*a* kann in Ihrem Hauptrechenzentrum implementiert und per IP-Adresse oder FQDN referenziert werden und ist somit zugleich eine gute Ressource für Ihre SonicWall HQ Firewalls, E-Mail Security Appliances und Filialen-Firewalls. Mittels REST API können Administratoren und Security-Experten, die schnelle Ergebnisse brauchen, Dateien auch manuell in die CS*a* hochladen.

Fazit

Für die Bekämpfung raffinierter und gezielter Malware ist eine Sandbox-Analyse notwendig, damit auch unbekannte Bedrohungen erkannt und gestoppt werden können. Bei vielen Arten von Attacken wird das Arsenal erst im Arbeitsspeicher offengelegt. Deshalb ist ein Arbeitsspeicher-basierter Ansatz sinnvoll, mit dem Angriffe erkannt und gestoppt werden können, bevor sie die Endpunkte erreichen. Cloud-basierte Sandboxing-Engines können Latenz verursachen und sind oft nicht mit den digitalen Souveränitätsvorgaben behördlicher Organisationen vereinbar.

Mit der Capture Security Appliance können Sie verdächtige Dateien innerhalb Ihres Rechenzentrums inspizieren. Die schnelle und präzise Analyse erfolgt im Arbeitsspeicher, um eine starke Schutzschicht zur Abwehr komplexer und gezielter Bedrohungen bereitzustellen.

Erfahren Sie mehr. Wenden Sie sich noch heute an Ihren SonicWall-Vertreter oder besuchen Sie www.sonicwall.com.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

[1] Mitre.org; Virtualization/Sandbox Evasion, https://attack.mitre.org/techniques/T1497/ 26 September 2019

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

SONICWALL®

SolutionBrief-AnAdvancedApproach-US-VG-1641