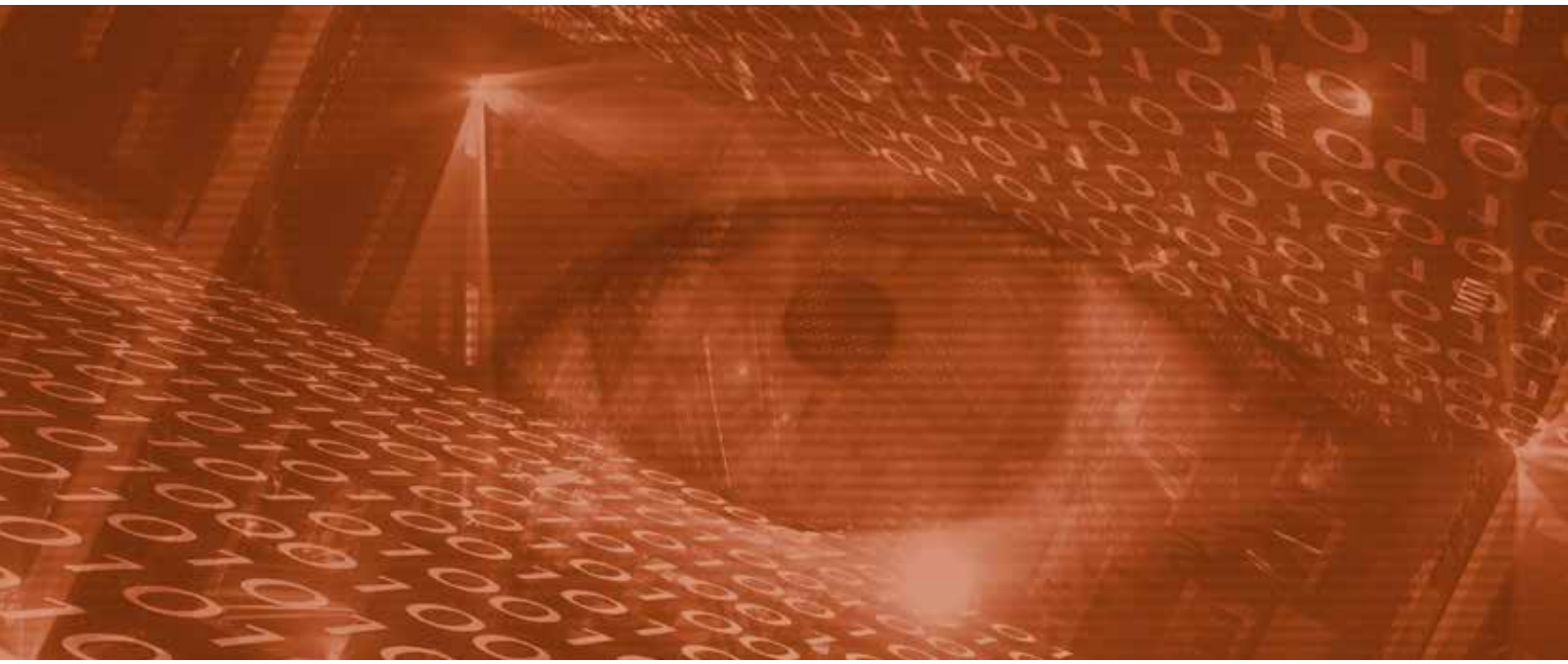
ANFORDERUNGEN AN DAS NEXT GENERATION SANDBOXING ZUR BEWÄLTIGUNG DER KOMPLEXEN BEDROHUNGSLANDSCHAFT



ZUSAMMENFASSUNG

Da die Netzwerkinfrastrukturen um neue Technologien und Dienste für mehr Agilität im Unternehmen erweitert werden, muss sich auch die IT-Sicherheit weiterentwickeln, um die wachsende Verwundbarkeit durch neue, noch nicht bekannte Bedrohungen zu antizipieren. Sandboxing ist ein wichtiger Teil der Security-Infrastruktur, um Bedrohungen zu erkennen und zu verhindern, bevor sie sich auf eine Organisation auswirken. Viele Sandbox-Lösungen – alte und neue – sind jedoch für die aktuellen Anforderungen moderner Netzwerke nicht hinreichend geeignet. Beim Hinzufügen oder Ersetzen einer Sandbox sollten sich Organisationen Lösungen zuwenden, die eine Reihe spezifischer Funktionen und Fähigkeiten der nächsten Generation bereitstellen.

WAS EINE SANDBOXING-LÖSUNG BIETEN SOLLTE

Angesichts der digitalen Transformation (DX) von Netzwerkinfrastrukturen, einer sich schnell verändernden Bedrohungslandschaft und neuen Geschäftsanforderungen mussten die Sandboxing-Technologien weiterentwickelt werden, um Fähigkeiten der nächsten Generation bereitzustellen. Es gibt jedoch immer noch viele veraltete Lösungen auf dem Markt, die sich selbst nicht als „erste Generation“ identifizieren oder nur unvollständige Funktionen für die Anforderungen der aktuellen Bedrohungslandschaft bieten. Es ist die Aufgabe des Käufers, zu wissen, was ihm eine Sandbox bieten muss, um seine bestehende und zukünftige Architektur umfassend zu ergänzen.

Unternehmen, die ihre aktuelle Sandboxing-Lösung evaluieren, sollten auf die folgenden zentralen Sandboxing-Attribute achten, die sie benötigen, um der komplexen Bedrohungslandschaft erfolgreich zu begegnen:

1. Integration und Automatisierung

Viele Sandboxing-Technologien befinden sich in ihren eigenen Silos als isolierte Einzelgeräte. Das bedeutet, dass sie keine Bedrohungsdaten mit anderen Security-Elementen in Ihrer Organisation teilen und im Gegenzug von solchen Informationen auch nicht profitieren können.

Das ist ein Problem, da komplexe Bedrohungen häufig auf eine breite Angriffsfläche zielen, wenn sie versuchen, in das Netzwerk einer Organisation einzudringen. Sie können auch so neu sein, dass sie in Bewertungstests Dritter nicht einbezogen wurden. Um derartige Angriffe zu vereiteln, ist eine Sandbox erforderlich, die mit der breiteren Security-Architektur verbunden ist und es ermöglicht, dass Ihre Lösung Zero-Day-Daten an alle Inline Security Controls weitergibt, die automatisch geeignete Schutzfunktionen anwenden. Somit können manuelle Prozesse eliminiert, Reaktionsfenster verkleinert und der Verwaltungsaufwand verringert werden – was besonders für Organisationen wichtig ist, die nur über eine geringe Zahl von IT-Security-Mitarbeitern verfügen.

Die nahtlose „Plug-and-Play“-Integration ermöglicht zudem eine umfassende Transparenz und ein vereinfachtes Sicherheitsmanagement sowie eine schnelle und einfache Sandbox-Implementierung: Vermeiden Sie Geräte, die über Netzwerk-TAPs verbunden werden müssen, was zu langen Implementierungszyklen führt und bei jeder Änderung von Netzwerk-Ports oder virtuellen lokalen Netzwerken (VLANs) fortlaufenden Verwaltungsaufwand verursacht.

2. Erkennung und Prävention

Viele Sandboxing-Lösungen bieten nur Erkennungsfunktionen, aber die Einbeziehung von Advanced Threat Prevention (ATP) zum Schutz vor komplexen Bedrohungen ist entscheidend, um die Gefährdung Ihrer Organisation zu minimieren. Laut NSS Labs sind die Fenster für die Bedrohungserkennung und die Verhinderung von Angriffen eng miteinander verflochten: „Die Fähigkeit des Produkts, erfolgreiche Infektionen rechtzeitig zu blockieren und zu melden, ist entscheidend für die Aufrechterhaltung der Sicherheit und Funktionalität des überwachten Netzwerks. Infektion und Übertragung von Malware müssen schnell und präzise gemeldet werden, sodass Administratoren die Möglichkeit haben, die Infektion einzudämmen und die Auswirkungen auf das Netzwerk zu minimieren.“[1]

Um sicherzustellen, dass die von Ihnen evaluierte Sandbox-Lösung über wirkungsvolle Erkennungs- und Präventionsfunktionen verfügt, sollten Sie diese anhand von Zertifizierungen durch Dritte und aktuellen Empfehlungen von vertrauenswürdigen, externen Testern überprüfen. Die Evaluierungsbereiche sollten die Gesamtbetriebskosten (TCO), die Zeit bis zur Erkennung, Umgehungen und Sicherheitseffektivität sowohl bei der Angriffserkennung als auch bei der Angriffsverhinderung umfassen. Lösungen, für die es Warnungen oder keine Bewertungen gibt oder für die überhaupt keine Angriffserkennungs- oder Angriffspräventionstests verfügbar sind, sollten vermieden werden.

3. SSL/TLS-Prüfung

Um den Branchenvorschriften zu entsprechen, müssen viele Unternehmen bestimmte Arten von sensiblen Daten mit Secure Sockets Layer-(SSL-) oder Transport Layer Security-(TLS-) Verschlüsselung schützen. 60 % des Netzwerkverkehrs entfällt heute auf verschlüsselte Inhalte, und dieses Volumen wächst von Jahr zu Jahr weiter.[2] Cyber-Kriminelle können aber auch Verschlüsselung verwenden, um Malware und Ransomware vor traditionellen Sicherheitslösungen zu verbergen.

Dies stellt viele der am Markt verfügbaren Sandboxing-Lösungen vor Probleme. Sie erfordern zusätzliche Appliances von Drittanbietern, um verschlüsselte Daten zu überprüfen. In diesem Fall sollten Netzwerk- und Security-Verantwortliche nach einer Sandbox suchen, die über die Integration mit bestehenden Security Controls, wie z. B. Next Generation Firewalls, auf robuste Funktionen zur Verschlüsselungsprüfung zugreifen kann.

4. Skalierbarkeit

Ein weiterer Aspekt für eine geeignete Sandbox für Ihre Security-Architektur ist die Antizipation des Wachstums Ihrer Infrastruktur. Eine ideale Lösung sollte einen hohen Durchsatz und Skalierbarkeit für potenzielle oder geplante Erweiterungen des Unternehmens unterstützen.

Im Hinblick auf die Skalierbarkeit trägt eine hohe Anzahl von Knoten pro Cluster dazu bei, die Sandbox zukunftssicher für Änderungen zu machen, die die Security-Anforderungen im Laufe der Zeit steigern können. So wollen Organisationen beispielsweise Sandboxing-Fähigkeiten in die Cloud erweitern, um die Vorteile der Cloud-Elastizität zu nutzen. Im Zeitalter der digitalen Transformation (DX), in dem sich Unternehmensnetzwerke natürlich ausweiten, sind Skalierbarkeit und hohe Verfügbarkeit unerlässliche Anforderungen an Lösungen.

5. Original-Technologien

Viele Sandboxing-Anbieter lizenzieren generische Technologien von größeren Originalgeräteherstellern (OEMs) und verwenden diese in ihren Produkten. Da diese Unternehmen nicht die gesamte genutzte Hardware und/oder Software besitzen oder selbst entwickeln, sind sie davon abhängig, dass die Lizenzgeber die Produkte aktualisieren und Patches bereitstellen, damit sie effektiv bleiben. Wenn die Drittanbieter-Lizenz des Lösungsanbieters jedoch abläuft oder geändert wird, bevor Ihr Produkt das Ende seiner Lebensdauer erreicht hat, können Sie möglicherweise nicht von Ihrer Sandbox-Investition profitieren. Noch beunruhigender ist, dass einige Sandboxen auf Open-Source-Technologie basieren – die Malware-Entwickler aufgrund des offenen, gleichberechtigten Zugangs frei nutzen können.

Suchen Sie nach Anbietern, deren Lösungsdesigns auf modernen, selbst entwickelten Technologien basieren. Netzwerk- und Security-Verantwortliche brauchen Lösungen, die aktuell, vollständig gepatcht und mit den neuesten und besten Funktionen ausgestattet sind. Lösungen, die vom Anbieter selbst entwickelt wurden, sind gewöhnlich Produkte, für die kontinuierlich Weiterentwicklungen, kompetente Unterstützung und Schulungsressourcen sowie – besonders wichtig – zeitnahe Fehlerbehebungen und Sicherheits-Updates bereitgestellt werden.

6. Formfaktor

Suchen Sie nach einer Sandbox, die über mehrere Formfaktoren verfügt. Mit zunehmender Virtualisierung und Cloud-Nutzung sind lokale Sandbox-Lösungen für viele Organisationen nicht mehr ausreichend. In der DX-Ära benötigen Organisationen die Flexibilität, Sandboxen über mehrere Formfaktoren hinweg zu nutzen – lokal, als virtuelle Maschine (VM) und/oder in der Cloud.

Ein kleines oder mittelständisches Unternehmen mit einer gehosteten Cloud möchte möglicherweise keine lokale Sandbox verwalten. Mehrere Formfaktor-Optionen ermöglichen auch eine nahtlose Migration von einer Umgebung in eine andere. Wenn ein Unternehmen z. B. plant, im Rahmen einer DX-Initiative über einen Zeitraum von drei Jahren schrittweise in die Cloud zu wechseln, um interne und externe Anwendungen und Dienste aus dem Rechenzentrum in die Cloud zu verlagern, muss es in der Zwischenzeit noch Ressourcen in seinem aktuellen Rechenzentrum sichern. Eine lokale Lösung kann ihre bestehende Infrastruktur schützen und gleichzeitig eine nahtlose Migration in die Cloud mit einheitlichem Schutz, Konfiguration und Lizenzen angemessen unterstützen.

7. Niedrigere Gesamtbetriebskosten (TCO)

Eine moderne Sandbox sollte eine einheitliche Lösung sein, die sich in die breitere Sicherheitsarchitektur einfügt. Suchen Sie nach einem Gerät, einem Subscription, das sich mit den anderen Komponenten Ihrer Security-Architektur integrieren lässt, um die gesamte Angriffsfläche (Netzwerk, Endgeräte, Internet, E-Mail und Cloud) ohne zusätzliche Lizenzen oder Kosten abzudecken. Vermeiden Sie Sandboxing, das mehrere Geräte, Lizenzen und/oder Threat Intelligence Subscriptions erfordert.

Vergleichen Sie das Preis-Leistungs-Verhältnis (Kosten pro geschütztem MBit/s) von Lösungen, wie es in Tests von Drittunternehmen berechnet wird. Dieser Wert bezieht nicht nur die Anschaffung und Lizenzierung einer Sandbox ein, sondern auch die Betriebskosten, wie z. B. Personalaufwand für Lösungsmanagement, Wartung, Logs und Berichte.

SUCHEN SIE NACH „NEXT GENERATION SANDBOXING“

Es gibt viele veraltete oder anderweitig begrenzte Produkte auf dem Markt, die es zu vermeiden gilt. Zu wissen, nach welchen Funktionen Sie suchen müssen, hilft Ihnen dabei, Fallstricke zu vermeiden und die für Sie beste Sandbox zu finden. Nur so können Sie Malware und andere bösartige Bedrohungen aus Ihrem Netzwerkverkehr aussieben.

Auch wenn eine Sandbox möglicherweise nicht explizit als Lösung der nächsten Generation gekennzeichnet ist, erfüllt eine Sandbox mit folgenden Funktionen die Anforderungen moderner Netzwerke:

- Prävention komplexer Bedrohungen
- Erkennung neu auftretender Bedrohungen durch proaktive Threat Resarch/-Intelligence
- Zertifizierungen und Testbewertungen von Drittunternehmen
- Unterstützung der Verschlüsselungsprüfung (SSL/TLS)
- Hohe Anzahl von Knoten pro Cluster für Skalierbarkeit
- Moderne, vom Anbieter entwickelte Technologien
- Mehrfache Formfaktor-Optionen
- Ein Gerät, eine Lizenz, ein Subscription

[1] William Dean Freeman and Jessica Williams, „Breach Prevention Systems Test Report: Fortinet Advanced Threat Protection“, NSS Labs, 13. Dezember 2017.

[2] Siehe z. B. J. Michael Butler, „SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL“, November 2013; Johnnie Konstantas, „SSL Encryption: Keep Your Head in the Game“, SecurityWeek, 15. März 2016.

Dezember 4, 2018 5:13 nachm.