Produktbeschreibung

Exposure Analysis and Response (ExAR) für Akamai Guardicore Segmentation

Unternehmensumgebungen verändern sich ständig und das sorgt zwangsläufig dafür, dass Ihre statischen Sicherheitsgrenzen plötzlich nicht mehr greifen. Diese strukturellen Lücken machen sich Angreifer zunutze: Sie nutzen heute künstliche Intelligenz, um die Zeit bis zur Ausnutzung einer Schwachstelle, die früher noch Wochen betrug, auf nur noch rund 20 Stunden zu verkürzen. Manuelle Patches und statische Sicherheitsgrenzen können mit Ausspähung in Maschinengeschwindigkeit, KI-gestützten Exploits und automatisierter lateraler Netzwerkbewegung einfach nicht mehr Schritt halten.

Die **ExAR-Funktionen (Exposure Analysis and Response)** von Akamai Guardicore Segmentation verwandeln die Mikrosegmentierung von einer statischen Netzwerkkontrolle in eine dynamische, aktive Sicherheitsebene.

Indem sie Bedrohungserkennung und Risikoüberwachung integrieren, ermöglicht die Plattform eine kontinuierliche Erfassung der Erreichbarkeit, eine automatisierte Verhaltenserkennung sowie eine Reaktion in Maschinengeschwindigkeit.

Mit diesem geschlossenen Ansatz kann Ihr Sicherheitsteam die Wirksamkeit von Richtlinien kontinuierlich überprüfen, aktive Angriffsketten sofort lokalisieren, anfällige Ressourcen in Maschinengeschwindigkeit isolieren und Angriffe autonom unterbinden, bevor sie Ihr Unternehmen gefährden.

Zentrale Herausforderung: die Asymmetrie vernetzter Pfade

Die meisten Sicherheitsteams haben damit zu kämpfen, individuelle, fragmentierte Signale zu verwalten, während sich Angreifer darauf konzentrieren, Pfade zu Ihren Daten zu ermitteln und auszunutzen. Herkömmliche Verteidigungsebenen versagen bei der Isolierung realer Risiken, und zwar aus mehreren Gründen:

- **Isolierten Einblicken fehlt es an Kontext:** Risikomanagement-Lösungen, Erkennungs- und Reaktionstools sowie herkömmliche Segmentierungslösungen existieren oft in Silos, die nicht miteinander kommunizieren. Um die tatsächliche Reichweite eines Angreifers zu ermitteln, müssen Erkennungsergebnisse auf Netzwerk-, Host- und Identitätsebene korreliert und mit der tatsächlichen Erreichbarkeit auf Basis der realen Segmentierung kombiniert werden.
- **Schweregrad ist nicht gleichbedeutend mit Erreichbarkeit:** Mithilfe von KI können Angreifer selbst Schwachstellen mit geringem Schweregrad ausnutzen, um erhebliche Auswirkungen zu erzielen. Ein Schwachstellenmanagement, das nur auf Schweregrad oder theoretischer Ausnutzbarkeit basiert, kann keine Schwachstellen kennzeichnen, die aufgrund der Segmentierung weiterhin ungeschützt sind. Herkömmlichen Segmentierungslösungen fehlt eine native Schwachstellenerkennung, was es Angreifern ermöglicht, Lücken in den Richtlinien auszunutzen.

Vorteile für Ihr Unternehmen

Priorisieren Sie, was wirklich wichtig ist
Bewerten Sie das Risiko anhand einer Risikoberechnung, die mehrere Größen berücksichtigt und auf der tatsächlichen Erreichbarkeit und dem geschäftlichen Kontext basiert. So können Sie sofort die Netzwerkzugriffspfade isolieren, die den größten potenziellen Schaden für Ihre wertvollsten Ressourcen bergen.

Unterbrechen Sie Angriffe in Maschinengeschwindigkeit
Neutralisieren Sie fortgeschrittene Techniken nach Exploits, schädliche laterale Netzwerkbewegung und nicht autorisierte KI-Tools durch native, aktive Abwehrfunktionen. Leiten Sie Gegenmaßnahmen, wie die sofortige Quarantäne anfälliger Assets, direkt auf Anwendungsebene ein – ganz ohne operative Latenz.

Erkennen Sie schädliche Aktivitäten
Ersetzen Sie die passive Sichtung von Warnmeldungen durch hochpräzise, vollständig korrelierte Vorfälle, die Hostprozesse, Identitäten und Netzwerktelemetrie verknüpfen, um eine eindeutige Angriffskette zu erstellen.

Gewährleisten Sie kontinuierliche Sicherheit
Wechseln Sie von punktuellen Konfigurationstests zu einer automatisierten, kontinuierlichen Feedbackschleife, um sicherzustellen, dass die durchgesetzten Zero-Trust-Regeln Bedrohungen strukturell eindämmen und laterale Netzwerkbewegung erfolgreich verhindern.

Akamai Security

- **Statische Richtlinien veralten:** Regelausnahmen, unkontrollierter Cloud-Einsatz, Identitätsmissbrauch und unverwaltete Assets untergraben die Effektivität von Zero-Trust-Architekturen. Segmentierung ohne kontinuierliche, automatisierte Validierung bietet nicht mehr als eine theoretische Schutz-Baseline.

Im Zeitalter KI-beschleunigter Bedrohungen sind Unternehmen, die sich nur auf manuelle Audits und statische Richtliniengrenzen verlassen, einem hohen Risiko ausgesetzt. Akamai Guardicore Segmentation mit ExAR erweitert Ihre Eindämmungsstrategie um die tatsächlichen Gegebenheiten Ihrer Umgebung. Mit diesem neuen Ansatz müssen Ihre Teams nicht ständig Brände löschen, sondern erhalten stattdessen vorausschauende, zuverlässige Kontrolle über Ihre tatsächliche interne Angriffsfläche.

Der risikobewusste Segmentierungszyklus

ExAR bietet End-to-End-Sicherheit durch einen kontinuierlichen, geschlossenen Lebenszyklus mit drei Schritten:

1. Erfassung und Analyse

ExAR modelliert den genauen Angriffspfad, den Angreifer innerhalb Ihres Unternehmens nutzen können. Indem ExAR kontinuierliche Asset-Erkennung und beobachteten Traffic mit detaillierten Host-Telemetriedaten, Identitätskontext und bekannten Softwarefehlern kombiniert, kann die Plattform berechnen, wie hoch das tatsächliche Risiko für Ihr Unternehmen aussieht, wenn dieser Angriffspfad nicht behoben wird.

2. Erkennung von Aktivitäten

Die integrierte **KI-Bedrohungsuntersuchung** geht über theoretische Risiken und statische Richtlinien hinaus:
Sie erkennt Aktivitäten autonom und korreliert bereichsübergreifende Telemetriedaten, um das tatsächliche Angreiferverhalten zu ermitteln.

- **Threat Intelligence und Indicators of Compromise:** Die Lösung nutzt die umfassenden globalen Informationen und IOCs von Akamai, um Bedrohungen zu identifizieren.
- **Fortschrittliche Bedrohungserkennung:** Die native Verhaltenserkennung gleicht ihre Ergebnisse mit dem MITRE-Framework ab, um versteckte Aktivitäten zu erkennen.
- **Bereichsübergreifende Angriffsanalyse:** Die Lösung korreliert Sicherheitsereignisse über Netzwerkgrenzen, Identitätspools und Endpoints hinweg.
- **Erkennung lateraler Netzwerkbewegung:** Die Lösung ist darauf optimiert, verdächtige interne Netzwerkbewegung zu identifizieren, bevor Daten vorbereitet werden.

ExAR stellt diese erweiterten Einblicke ganz ohne zusätzliche Agentenressourcen oder erhöhte CPU-Auslastung auf Ihren Produktionsservern bereit.

3. Aktive Verteidigung

Wenn eine Grenzverletzung oder eine Technik nach dem Exploit erkannt wird, stattet ExAR Ihre Sicherheitsteams mit Playbooks und automatisierten Behebungstools aus, um eine schnelle Reaktion zu ermöglichen. Abwehrmaßnahmen lassen sich sofort anpassen: Sie können eine dynamische Edge-Blockierung über eine native DNS-Firewall aktivieren, können realistische Honeypots zur Täuschung von Angreifern einsetzen, um automatisierte Tools umzuleiten und auszulasten, können Ihre Segmentierungsrichtlinien anpassen, um anfällige Pfade zu sichern, und können anfällige Assets durch Netzwerkkontrollen isolieren.

Wo sich die Lösung am besten eignet

Akamai Guardicore Segmentation mit ExAR eignet sich ideal für folgende Kunden:

Unternehmen, die mit KI-gestützten Angriffen zu kämpfen haben
Unternehmen, die erkannt haben, dass manuelle Patchzyklen und veraltete Firewalls mit Portblockierung einfach nicht mehr ausreichen, wenn Schwachstellen in unter 24 Stunden ausgenutzt werden

SecOps-Teams, die unter einer Alarmflut leiden
Sicherheitsteams, die sich den modernen Gegebenheiten anpassen müssen, indem sie Risiken und Bedrohungen anhand der tatsächlichen Erreichbarkeit ihrer wichtigsten Unternehmensressourcen priorisieren

Sicherheitsverantwortliche, die ihre Segmentierungsstrategie modernisieren
Unternehmen, die aktiv nach einer Segmentierungslösung suchen, um eine zukunftssichere Verteidigung aufzubauen, die auch KI-gestützte Bedrohungen berücksichtigt

Sensible hybride Infrastrukturen
Streng regulierte Betriebsabläufe (z. B. im Finanz- oder Gesundheitswesen oder in der Fertigung), die deterministische Nachweise dafür erfordern, dass Änderungen an Sicherheitskontrollen nicht die Produktion unterbrechen

Reifende Zero-Trust-Programme
Unternehmen, die eine zuverlässige, kontinuierliche Validierung hinzufügen möchten, um sicherzustellen, dass ihre Netzwerkgrenzen auch dann bestehen bleiben, wenn sich Anwendungen und Container-Konfigurationen weiterentwickeln

Optimierte, Asset-basierte Pakete

Im Zeitalter KI-beschleunigter Angriffe, in dem Bedrohungen ihre Taktiken in Echtzeit anpassen können, sorgt eine Segmentierung ohne kontinuierliche Risikoerfassung für eine Transparenzlücke, die heute einfach nicht mehr tragbar ist.

Um sicherzustellen, dass Ihre Sicherheitsgrenzen auch dann standhalten, wenn Präventionsmaßnahmen versagen, können Sie jeder Akamai Guardicore Segmentation-Bereitstellung ab dem ersten Tag ein integriertes ExAR-Paket für die gesamte Unternehmensumgebung hinzufügen.

Funktionsübersicht

Fähigkeiten	Plus	Premier
Hochpräzise korrelierte Vorfälle (MITRE-TTPs, forensische Daten)	✓	✓
Bereichsübergreifende Telemetrieerkennung (Host, Netzwerk, Identität)	✓	✓
Interaktives Risiko-Dashboard (umfassende Sicherheitsanalyse)	✓	✓
Agentische Bedrohungsuntersuchung (autonome Erkennung und Schlussfolgerung)	✓	✓
Empfohlene Maßnahmen (maßgeschneiderte Reaktionen)	✓	✓
Umfassende Transparenz auf Hostebene (nativ integrierte osquery-Telemetrie)	✓	✓
Integration von Akamai Threat Intelligence (globale Informationsfeeds)	✓	✓
Rund um die Uhr aktives Threat Hunting durch Experten (Untersuchung durch erfahrene Analysten)	⊘	✓
Live-Supportkoordination (aktive Unterstützung bei Vorfällen)	⊘	✓
Edge-Schutz durch DNS-Firewall (mehrschichtige Verteidigung)	Add-on verfügbar	✓
Dynamische Honeypots zur Täuschung von Angreifern (Unterbrechung in Maschinengeschwindigkeit)	Add-on verfügbar	✓

Bewährte Ergebnisse aus der Praxis

Fallstudie 1: Verhinderung von Berechtigungsmissbrauch und versteckten Scans

- **Umgebung:** Multinationaler Elektronikhersteller
- **Der Vorfall:** Ein Angreifer hat ein internes Konto mit hohen Berechtigungen gehackt, SSH-Traffic über ungewöhnliche Ports umgeleitet, um der Erkennung zu entgehen, und eine nutzerdefinierte Binärdatei mit sensiblen Netzwerkinformationen heruntergeladen.
- **Der ExAR-Unterschied:** Die tiefgreifende Telemetrie von ExAR hat hinter die normale Netzwerkaktivität geblickt und den versteckten Download der verdächtigen Programmdatei erkannt. Darüber hinaus konnte die bereichsübergreifende Engine die Netzwerkscan-Aktivität dieser Binärdatei und dem berechtigten Nutzer zuordnen. Infolgedessen generierte ExAR einen einzigen Vorfall mit hohem Schweregrad und empfahl die nötigen Segmentierungsregeln, um den Zielpfad zu schließen.

Fallstudie 2: Abwehr eines Active-Directory-Angriffs

- **Umgebung:** Großer Krankenversicherer
- **Der Vorfall:** Angreifer haben ein Cobalt-Strike-Framework verwendet, um schnell zehn zufällig ausgewählte Windows-Dienste bereitzustellen. Diese Dienste haben Anmeldedaten gescrapt, Verzeichniskonfigurationen erfasst und Azure-AD-Datenbankdateien gesammelt.
- **Der ExAR-Unterschied:** Herkömmliche Warnstrukturen generierten eine Reihe geringfügiger, unzusammenhängender Ereignisse. ExAR fügte hingegen alle 10 Aktionen, die nach dem Exploit stattfanden, sofort zu einer zusammenhängenden Angriffskette zusammen, bestätigte den aktiven Sicherheitsverstoß und empfahl spezifische Mikrosegmentierungsgrenzen, um den Angreifer daran zu hindern, sein Ziel zu erreichen.

Seien Sie KI-beschleunigten Bedrohungen stets einen Schritt voraus. Fordern Sie noch heute eine Demo an.

© 2026 Akamai Technologies | Support | | Veröffentlicht: August 2026