Product Brief

Exposure Analysis and Response (ExAR) for Akamai Guardicore Segmentation

Enterprise environments change constantly, and as things shift, your static security perimeters naturally drift out of alignment. Attackers capitalize on these structural gaps. They now use artificial intelligence to collapse the traditional time to exploit from weeks down to roughly 20 hours. Human-speed patching and static security perimeters can no longer keep pace with machine-speed reconnaissance, AI-assisted exploitation, and automated lateral movement.

Akamai Guardicore Segmentation's **Exposure Analysis and Response (ExAR)** capabilities turn microsegmentation from a static network control into a dynamic, living security layer.

Integrating threat detection and exposure awareness into our methodology, the platform enables continuous reachability mapping, automated behavioral detection, and machine-speed response.

This closed-loop approach allows your security team to continuously validate policy effectiveness, pinpoint active threat chains immediately, quarantine vulnerable assets at machine speed, and autonomously disrupt attacks before they compromise your business.

Core challenge: The Asymmetry of Connected Pathing

Most security teams find themselves managing individual, disconnected signals while attackers focus on finding and exploiting pathways to your data. Traditional defense layers fail to isolate real-world risk for several reasons:

- **Siloed visibility lacks context:** Exposure management solutions, detection and response tools, and traditional segmentation solutions often exist in different silos that do not speak to each other. To provide the full picture of an attacker's true reach, it requires correlation of network, host, and identity detections combined with true reachability based on segmentation reality.
- **Severity does not equal reachability:** With AI, attackers can turn even low-severity vulnerabilities into major impacts. Vulnerability management based on severity or theoretical exploitability fails to highlight vulnerabilities left exposed based on segmentation. Traditional segmentation solutions lack native vulnerability detection, giving attackers an opportunity to exploit weaknesses in policy.

Benefits for your business

Prioritize what's real
Evaluate exposure using a multidimensional risk calculation driven by real-world reachability and business context. Instantly isolate the fraction of network access paths that present the highest potential blast radius to your crown jewels.

Disrupt at machine speed
Neutralize advanced post-exploitation tradecraft, malicious lateral movement, and unauthorized AI tools through native, active defense capabilities. Engage countermeasures, such as immediately quarantining vulnerable assets, directly at the application layer without operational latency.

Detect malicious activity
Replace passive alert triage with high-fidelity, fully correlated incidents that connect host processes, identities, and network telemetry into an undeniable attack chain.

Continuous posture assurance
Move from point-in-time configuration testing to an automated, continuous feedback loop. Verify that enforced Zero Trust rules are structurally containing threats and successfully preventing lateral movement.

Akamai Security

- **Static policies stagnate:** Rule exceptions, cloud sprawl, identity compromise, and unmanaged assets constantly erode the reality of Zero Trust architectures. Segmentation without continuous, automated validation provides nothing more than a theoretical baseline of protection.

In an era of AI-accelerated threats, relying on manual auditing and static policy walls leaves organizations highly exposed. Akamai Guardicore Segmentation, with ExAR, injects reality into your containment strategy. This new approach is designed to shift your teams from a state of constant firefighting to predictive, definitive control over your true internal attack surface.

The exposure-aware segmentation loop

ExAR delivers end-to-end security through a continuous, three-step closed-loop lifecycle:

1. Understand and analyze

ExAR models the exact attack path an adversary would interact with inside your enterprise. By integrating continuous asset discovery and observed network traffic with detailed host telemetry, identity context, and known software flaws, the platform calculates what the true risk to your business would be if that attack path is not resolved.

2. Detect activity

The built-in **AI threat investigator** moves beyond theoretical risk and static policies. It autonomously detects activity and correlates cross-domain telemetry to identify real adversary behavior.

- **Threat intelligence and indicators of compromise:** Utilizes Akamai's broad global intelligence and indicators of compromise (IOCs) to identify threats.
- **Advanced threat detection:** Native behavioral detections mapped against the MITRE framework to detect stealthy activity.
- **Cross-domain attack analysis:** Correlates security events across network boundaries, identity pools, and endpoints.
- **Lateral movement detection:** Fine-tuned to identify suspicious internal movement before data is staged.

ExAR delivers this advanced intelligence with zero agent resource overhead or CPU utilization spikes on your production servers.

3. Active defense

When a boundary violation or post-exploitation technique is verified, ExAR equips security teams with rapid response playbooks and automated mitigation tools. Defenses can be adapted immediately by introducing dynamic edge blocking via a native DNS firewall, deploying realistic deception honeypots to redirect and exhaust automated attacker tools, delivering segmentation policy adjustments that seal vulnerable paths, and isolating vulnerable assets with network controls.

Where it fits best

Akamai Guardicore Segmentation with ExAR is ideally tailored for:

Enterprises facing AI-driven threat actors
Organizations recognizing that human-speed patch cycles and legacy port-blocking firewalls cannot halt automated, sub–24-hour weaponization windows.

SecOps teams suffering from alert fatigue
Security teams that must adapt to today's reality by prioritizing risks and threats based on true reachability to corporate crown jewels.

Security leaders modernizing their segmentation strategy
Enterprises actively seeking a segmentation solution that future-proofs their defense by specifically accounting for AI-driven threat capabilities from day one.

Sensitive hybrid infrastructures
Highly regulated operations (such as financial, healthcare, or core manufacturing) that require deterministic proof that security control changes won't interrupt production uptime.

Maturing Zero Trust programs
Organizations seeking to add an unassailable layer of continuous validation to ensure their network boundaries always hold as applications and container configurations evolve over time.

Optimized, asset-based packages

In an age of AI-accelerated attacks, when threats can modify their own tactics in real time, deploying segmentation without continuous exposure mapping creates an unacceptable visibility gap.

To ensure your boundaries hold when prevention fails, every Akamai Guardicore Segmentation deployment can incorporate an integrated ExAR package across the entire enterprise estate from day one.

Feature matrix

Capability	Plus	Premier
High-fidelity correlated incidents (MITRE TTPs, forensic data)	✓	✓
Cross-domain telemetry detection (host, network, identity)	✓	✓
Interactive exposure dashboard (comprehensive posture analysis)	✓	✓
Agentic AI threat investigator (autonomous detection and reasoning)	✓	✓
Recommended actions (tailor-made response actions)	✓	✓
Deep host-level visibility (natively embedded osquery telemetry)	✓	✓
Akamai threat intelligence integration (global intelligence feeds)	✓	✓
24/7 human-led threat hunting (elite analyst investigation)	⊘	✓
Live support coordination (live guidance with incidents)	⊘	✓
DNS firewall edge protection (defense in depth)	Add-on available	✓
Dynamic deception honeypots (machine-speed disruption)	Add-on available	✓

Proven real-world outcomes

Case Study 1: Halting privilege abuse and stealth scanning

- **Environment:** Multinational electronics manufacturer
- **The incident:** An attacker compromised a privileged internal account, tunneled SSH traffic through abnormal ports to evade detection, and downloaded a custom network enumeration binary.
- **The ExAR difference:** ExAR's deep telemetry sees past normal network activity to identify the stealthy download of a suspicious executable, and its cross-domain engine attributed the network scanning activity to that same binary and privileged user. As a result, ExAR generated a single, high-severity incident and explicitly recommended segmentation rules required to close the target path.

Case Study 2: Mitigating active directory compromise

- **Environment:** Large health insurance provider
- **The incident:** Adversaries used a Cobalt Strike framework to quickly deploy 10 randomized Windows services. These services scraped credentials, enumerated directory configurations, and harvested Azure AD database files.
- **The ExAR difference:** Traditional alerting structures generated a series of minor, disconnected events. ExAR instantly stitched all 10 post-exploitation actions into an aligned attack chain, verifying an active breach and recommending specific microsegmentation boundaries to stop the attacker from reaching their goal.

Stay ahead of AI-accelerated threats. Request a demo today.

© 2026 Akamai Technologies | Support |

| Published 08/26