Akamai Partner Story

Lumu Enabled Simpler Zero Trust Enforcement

The company integrated its compromise assessment with Akamai's microsegmentation to automate real-time threat containment

- Automated threat containment
- Eliminated security team workload
- Simplified Zero Trust rollout

Delivering real-time cyber resilience across hybrid environments

Lumu Technologies helps organizations continuously identify and respond to cyber compromise across complex environments. To help customers stop **ransomware**, reduce lateral movement, and simplify **Zero Trust** adoption, Lumu integrated with Akamai Guardicore Segmentation. Combining Lumu's Continuous Compromise Assessment® capabilities with Akamai's **microsegmentation** created an automated, threat-aware solution that detects malicious activity and instantly applies containment policies across hybrid cloud environments.

Exposing threats hidden in plain sight

Attackers increasingly rely on stealth instead of disruption. Rather than launching loud, destructive attacks, they now abuse legitimate tools already trusted inside organizations.

"Because attackers use everyday tools — think VPNs, anonymizers, cloud services, and encrypted channels — malicious activity can hide in plain sight," explained Nicole Ibarra, VP of Product Marketing at Lumu Technologies.

Traditional security tools often struggle to identify these threats because they operate in silos. **Endpoint** tools, cloud controls, identity systems, and network monitoring platforms rarely communicate effectively with one another, leaving organizations reactive instead of proactive.

"We see organizations investing heavily in cybersecurity tools that don't necessarily work together," Ibarra explained. "In today's environment, siloed security is the wrong approach."

Lumu addresses this challenge through its patent-pending **Continuous Compromise Assessment** model. The model continuously ingests telemetry across the enterprise to identify indicators of compromise, attacker intent, and abnormal behavior in real time.

"Real-time visibility is essential to knowing at all times if you're compromised," Ibarra said.

Location
Doral, Florida
lumu.io

Industry
Software and SaaS

Solution
Security

Product
Akamai Guardicore Segmentation

Akamai Security

Connecting visibility with automated Zero Trust enforcement

While visibility is critical, Lumu recognized that detection alone is no longer enough. Organizations also need the ability to act immediately when threats appear. "Continuous response is key to preventing bad things from happening," continued Ibarra.

That requirement made **Akamai Guardicore Segmentation** a natural option. Akamai's solution maps application flows and dependencies across hybrid environments and provides real-time workload visibility. It also enables Zero Trust policy enforcement to reduce lateral movement and contain ransomware across hybrid cloud environments.

Integrating Lumu threat intelligence with Akamai's microsegmentation policy engine creates a closed-loop security workflow:

- Lumu continuously analyzes network metadata and telemetry to identify malicious or unusual behavior.
- Akamai Guardicore Segmentation visualizes workloads, applications, and communication flows.
- Confirmed threats automatically trigger Zero Trust segmentation policies that isolate affected assets and block lateral movement.

This approach simplifies ransomware containment and real-time threat response.

"Organizations can't afford delays between detection and response," Ibarra said. "Integrating Lumu with Akamai Guardicore Segmentation means we update the policy in real time automatically, without human intervention. And that enables customers to quickly and automatically isolate threats in real time before they become a larger problem."

Delivering real-time response without operational overhead

The partnership between Lumu and Akamai enables organizations to move from reactive security operations to automated cyber resilience. Say Lumu detects a compromised asset attempting to communicate with a malicious command and control (C2) server. It can instantly trigger Akamai Guardicore Segmentation to isolate that asset and sever suspicious communication flows.

That automation dramatically reduces attacker dwell time. It also eliminates the need for security teams to manually investigate and apply policies during an active threat. "We combine visibility plus response and implement policies in a way that simplifies the process for customers," Ibarra said.

Moreover, the integration helps organizations address increasingly sophisticated AI-driven attacks. "Today's threat landscape is complex and always changing," Ibarra explained. "Our detection engine uses AI to identify emerging threats and abnormalities across the environment."

Lumu extends that automation through capabilities such as its **Autopilot**™ autonomous SOC functionality. This feature can orchestrate response actions across firewalls, VPNs, endpoint tools, and Akamai Guardicore Segmentation. "We add automation to the tools we integrate with and save security teams from the guesswork," Ibarra said. "Autopilot acts as an autonomous AI security operator that can manage incidents from start to finish."

Together, Lumu and Akamai enable customers to automatically isolate threats in real time.

Nicole Ibarra
VP of Product Marketing, Lumu Technologies

Simplifying microsegmentation and Zero Trust adoption

Many organizations recognize the value of Zero Trust and microsegmentation but hesitate because they believe implementation will be too complex. According to Ibarra, lack of visibility often prevents companies from understanding the scale of their lateral movement risks in the first place. “You don’t know what you don’t know,” she said. “And once you do, it might be too late.”

The integration between Lumu and Akamai enables organizations to proactively identify threats, automate segmentation, and reduce the operational burden of implementing Zero Trust security. Because Lumu continuously monitors network activity and orchestrates enforcement actions through Akamai Guardicore Segmentation, organizations can implement Zero Trust policies in a practical, manageable way.

“Customers often think segmentation is too complicated or that they don’t have lateral movement issues. Lumu is the engine of visibility and orchestration that enables Akamai Guardicore Segmentation to apply Zero Trust workflows in a sensible way,” Ibarra concluded.

Lumu is a cybersecurity company that helps organizations operate cybersecurity proficiently by measuring and understanding compromise in real time. Through its Continuous Compromise Assessment model, Lumu empowers security teams to act immediately on confirmed compromises and minimize risk exposure. For more information, visit lumu.io.