Lumu for SecOps

At every stage of the cyber kill chain, adversaries have to use the network. Accelerating Security Operations Maturity requires unmatched network visibility and automated response.

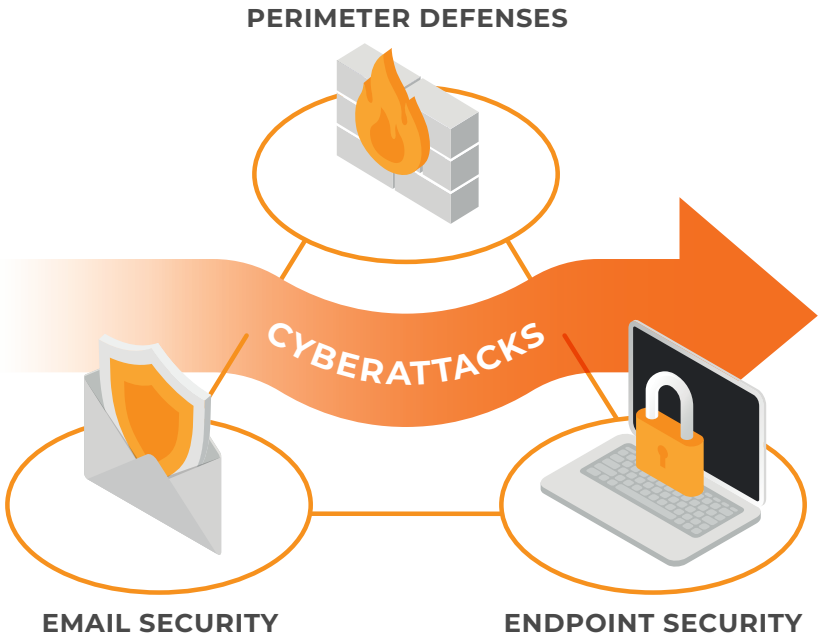
The Challenge

Every cyberattack is designed to bypass perimeter defenses solutions like firewalls, endpoint detection, or email security. When these siloed defenses are breached, attackers use the network to achieve their goals, leaving evidence of their movements.

Email Security:
Email remains one of the most common entry points for cyberattacks with 36% of data breaches caused by phishing.

Perimeter Defenses:
Perimeter defenses, including modern solutions like SASE and ZTNA as well as traditional firewalls frequently have vulnerabilities that can be exploited by threat actors to gain access to networks.

EDRs:
Endpoint Detection and response and antivirus programs are easily bypassed by adversarial techniques. A recent study found that for every EDR on the market, there exists a technique that hackers can use to bypass it.



SIEMs Have Failed SecOps Teams

SecOps strategies anchored on SIEMs have failed at detecting when adversaries attempt to bypass the triad of defenses that most companies rely on.

Enterprise SIEMs only detect

24%

of MITRE ATT&CK v13 Techniques

Enterprise SIEMs already ingest sufficient data to cover

94%

of all MITRE ATT&CK Techniques

SIEMs are evolving towards "detection-in-depth" across multiple security layers. **But container monitoring lags behind at only**

32%

12%

of SIEM rules are broken and will never fire due to misconfigured data sources and missing fields

© Lumu Technologies - All rights reserved.

The Solution

The cybersecurity stack needs to evolve to include visibility as the foundation upon which security operations are built.

Network Visibility Is Key to SecOps Efficiency

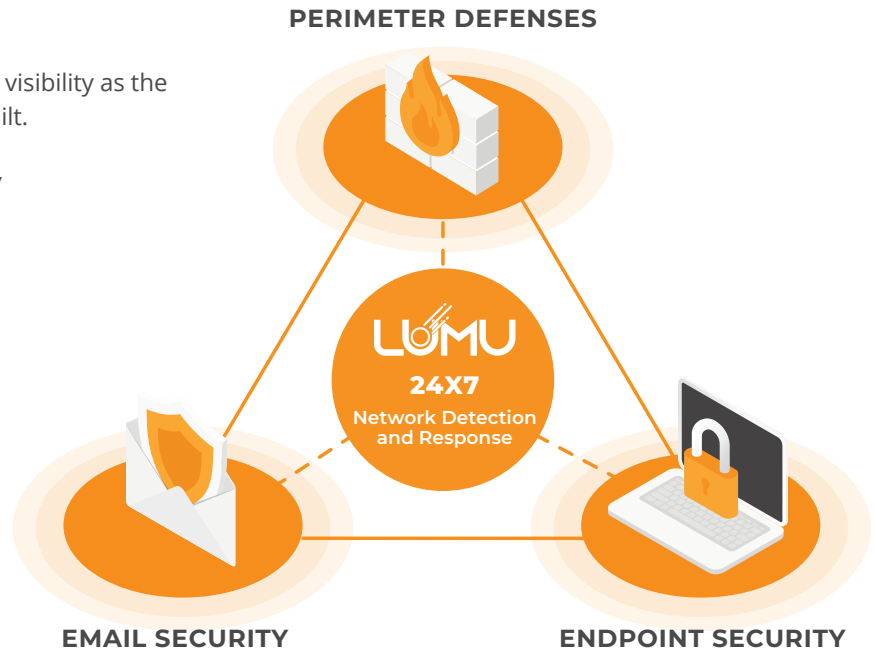
At every stage of an attack, the adversary needs to use your network. This leaves behind evidence of their actions.

Removing Silos Around Cybersecurity Tools

An integrated, coordinated stack can't be bypassed as easily as individual siloed tools.

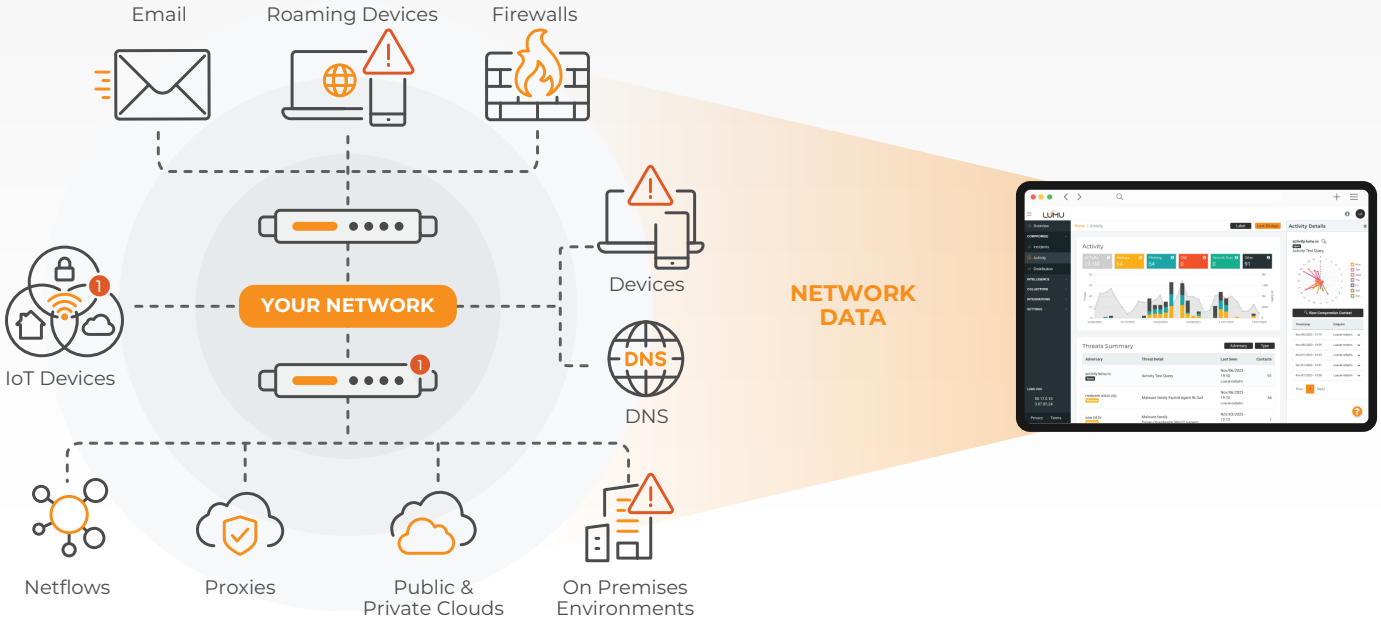
Reduce Alert Fatigue with Machine Learning and AI

Leverage AI to confirm compromises and conduct threat hunting so your team can spend their time on tasks best suited to humans.



How Lumu Works

At every stage, attackers use your network to achieve their goals. Lumu collects network metadata, leverages AI to analyze it against known IoCs, and identifies confirmed network compromises in real time.



© Lumu Technologies - All rights reserved.

Key SecOps Enablement

110+ 3rd Party Integrations
Maximizes your existing cybersecurity investments.

Compromise Context
Lets teams quickly understand the nature and critical details of attacks.

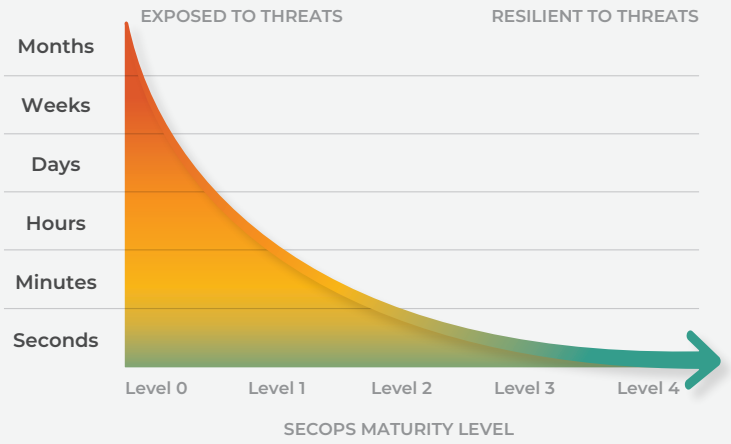
Automated Threat Hunting
Scans your network to identify and mitigate potential threats in real-time.

AI that Works for you
Leverages AI for deep correlation to confirm compromises and lower false positive rates.

24/7 Cyber Analyst
Constantly hunts threats, wherever you are.

Global MITRE Matrix
See which TTPS are being used by attackers to target your network.

Accelerate SecOps Maturity



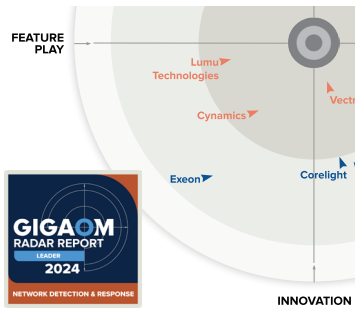
How Lumu Lowers MTTR

SecOps Maturity is not about complexity or expense, but how quickly you can respond to threats measured in Mean Time to Response (MTTR). Lumu lowers your MTTR to only milliseconds, by automating responses through integrations with your existing stack and without adding complexity.

Analyst Validation

Forrester Wave: NAV Leader

GigaOm Radar: NDR Leader



Frost and Sullivan: NDR Market Assessment Leader

Lumu Technologies Inc. | 8600 NW 36th St., Suite 150 Doral, FL 33166 | sales@lumu.io | +1 (877) 909-5868