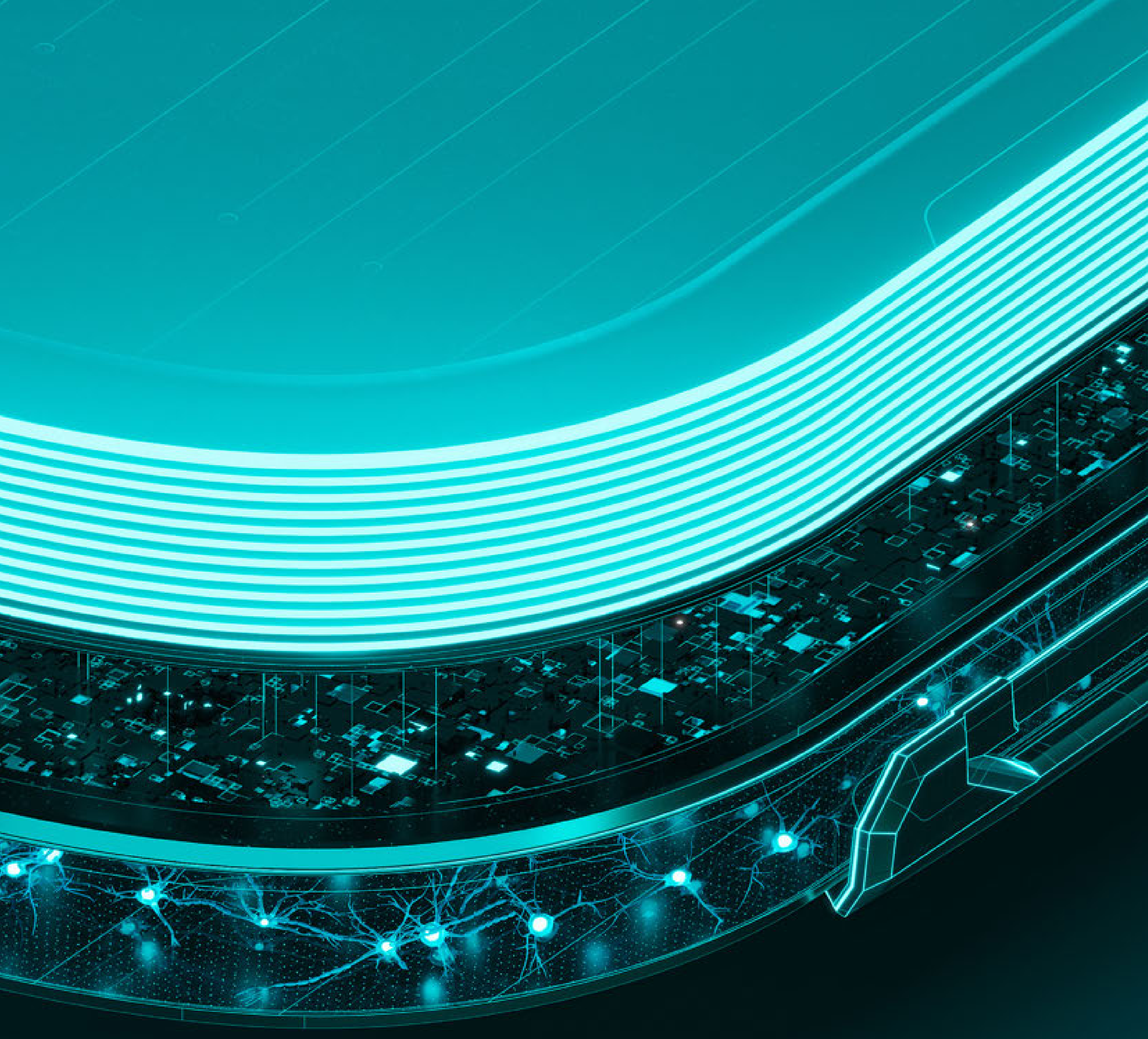
ESET and Lumu

Automated compromise detection and real-time threat intelligence for your business



Cybersecurity
Progress. Protected.

SOLUTION BRIEF

Real-time visibility for a faster, smarter response

Security professionals face mounting pressure to stay ahead of constantly evolving threats while managing multiple cybersecurity tools, often with limited resources. Traditional solutions provide visibility but often require manual correlation and constant updates, which can slow down detection and response.

ESET's integration with Lumu provides automated management of threat indicators, enhancing web protection by dynamically updating ESET PROTECT policies with real-time intelligence. By focusing on confirmed compromises, this integration minimizes exposure windows, reduces false positives, and ensures security teams can respond quickly and efficiently.

KEY BENEFITS

AUTOMATED IOC MANAGEMENT

Eliminates manual updates by automatically synchronizing threat indicators from Lumu to ESET PROTECT policies, saving time and reducing human error.

REAL-TIME PROTECTION

Continuously updates ESET policies with the latest malicious domains, IPs, and URLs, ensuring near real-time defense against evolving threats.

REDUCED FALSE POSITIVES

Muted incidents in Lumu automatically remove associated IOCs from ESET policies, minimizing disruptions and improving the user experience.

FLEXIBLE DEPLOYMENT

Supports cloud and on-premise ESET PROTECT deployments with options for Linux, Windows, or via Docker.

IMPROVED VISIBILITY

Aggregates network metadata from multiple sources, providing a clearer picture of attacker behavior and enabling automatic enforcement of protection policies.

KEY FEATURES

REAL-TIME IOC SYNC

Continuous, automated synchronization of compromise indicators from Lumu to ESET PROTECT.

WEB ACCESS PROTECTION INTEGRATION

Malicious domains are fed directly into ESET web control policies for proactive blocking.

CUSTOM SCRIPT OR DOCKER DEPLOYMENT

Flexible deployment tailored to various customer environments and infrastructure.

INCIDENT MUTE FUNCTIONALITY

Automatically removes associated IOCs from ESET when muted in Lumu, reducing false positives.

MULTI-SOURCE METADATA COLLECTION

Enriches threat detection with network metadata from agents, proxies, DNS logs, and cloud services.

HOW IT WORKS

Lumu aggregates network metadata and correlates it with global threat intelligence to detect patterns of attacker behavior. When Lumu detects signs of infrastructure used in an ongoing campaign (e.g. command & control or phishing domains), it generates IOCs in real time. These IOCs are automatically pushed into ESET PROTECT's Web Access Protection policy using the integration script. All endpoints with ESET agents enforce the updated policies within minutes, blocking access organization-wide to those malicious assets.

About ESET

PROACTIVE DEFENSE. MINIMIZE RISKS WITH PREVENTION.

Experience best-in-class protection thanks to ESET's in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers. ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities. ESET protects your business so you can unlock the full potential of technology.

About Lumu

Lumu is a cybersecurity company that enables organizations to measure and understand compromise in real time. By collecting and analyzing network metadata, Lumu identifies confirmed points of compromise and enables immediate, automated response across existing infrastructure. Headquartered in Miami, Lumu is trusted by thousands of organizations around the world to close the breach detection gap.

Cybersecurity
Progress. Protected.

SOLUTION BRIEF