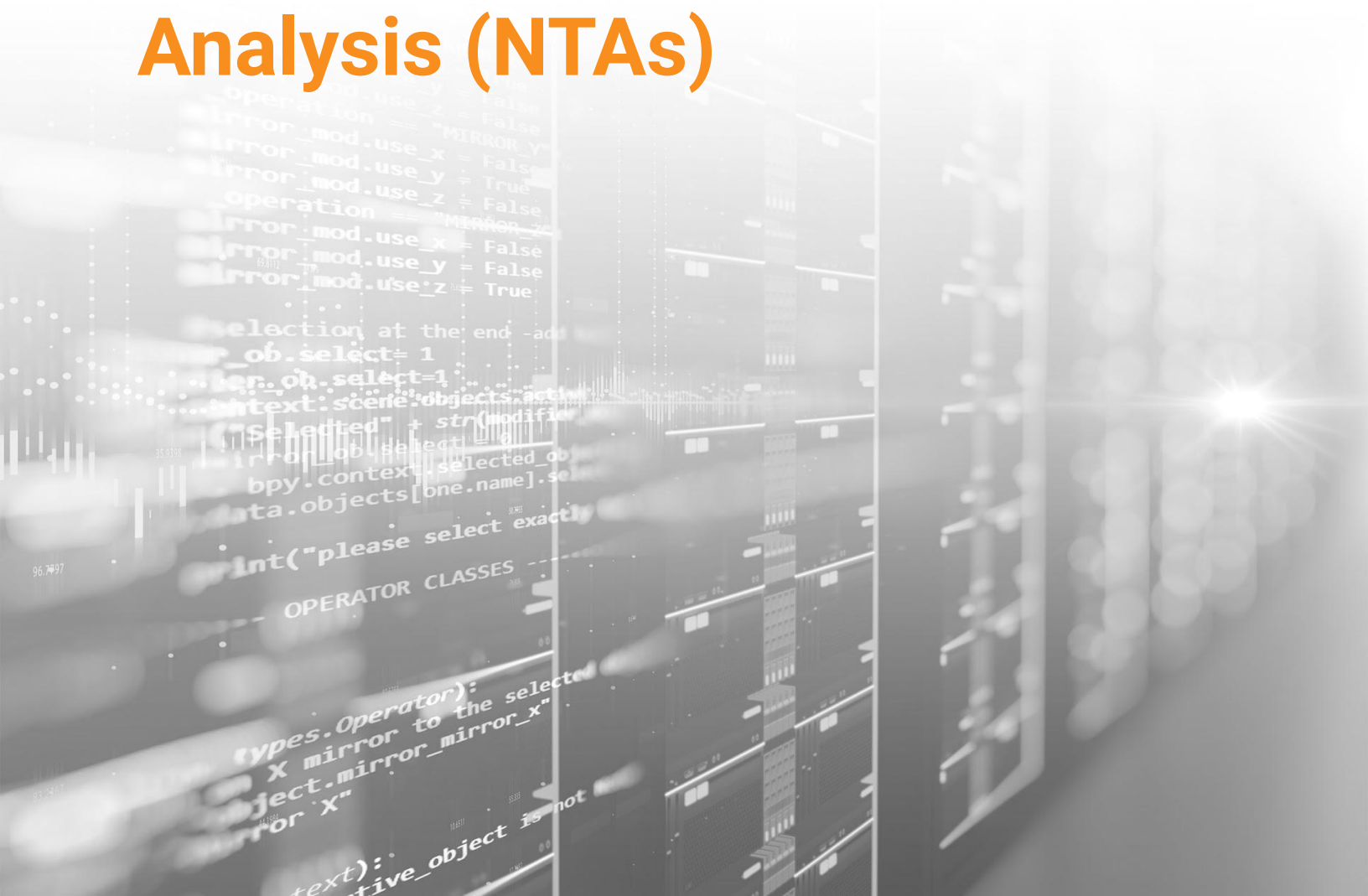
LUMU

ENLIGHTENMENT BRIEF:

Lumu and Network Traffic Analysis (NTAs)



With more than 1,200 vendors in the cybersecurity industry, it is critical to understand how Lumu compares with and complements other technologies in the space to maximize the output of your cybersecurity strategy.

How does Lumu compare with a legacy NTA?

According to Gartner "Network traffic analysis (NTA) uses a combination of machine learning, advanced analytics, and rule-based detection to detect suspicious activities on enterprise networks. NTA tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior." This is a broad definition and generally speaking, it includes solutions that were primarily designed for network performance (better known as Network Performance Monitoring) that pivoted their use case to cybersecurity in pursuit of a larger market.

Lumu fits into Gartner's definition of an NTA, or more recently NDR (Network Detection and Response). But it is important to note that **not all NTA solutions are designed in the same way.** Lumu is a technology that was built from the ground up with a single goal: **help the world to measure and understand its compromise level in real time.** This is done via Lumu's patent-pending Illumination Process which systematically collects, normalizes, and analyzes your company's **network metadata**, resulting in the identification of enterprise assets in contact with adversarial infrastructure. Simply put, Lumu identifies confirmed compromises.

How can Lumu and NTAs work together?

If your company already has a legacy NTA solution such as Cisco Stealthwatch, Darktrace, Extrahop, Fireye, or the like, Lumu can improve your cybersecurity posture with novel and unique information about the compromises inside your organization. You can also have flawless integration with other NTA solutions because of Lumu's API-driven architecture.

Unlike legacy NTAs that—because of their architecture and complex implementation—end up monitoring specific segments of your IT environment (typically critical assets); Lumu follows the premise that to measure the security of a system, you have to measure the entire system. Therefore, Lumu allows enterprises to monitor their entire hybrid ecosystems: all on-premise assets, IoTs, OT, hybrid cloud environments, and the growing amount of WFH assets.

Furthermore, Lumu analyzes a broad range of network metadata that no other vendor is analyzing as a whole—including DNS, Firewall and Proxy logs, Network Flows, and Spambox—to tell your organization's unique compromise story. The amicable licensing model enables enterprises to jumpstart their journey towards Continuous Compromise Assessment by monitoring assets or network metadata sources, such as spambox, that are blindspots to their current NTA deployment.

In addition, Lumu goes beyond the detection that most NTAs can provide and includes context around the compromise, including compromise dissemination, the attacker's objective, spreading patterns, compromise time-lapses, and more.

If you are curious about the value that Lumu provides compared with your existing NTA solution, we invite you to eliminate your doubts by opening a free account or requesting proof of concept.

If your organization does not have an NTA solution in place, Lumu can close the gap between network anomalies and ***Continuous Compromise Assessment***. Taking advantage of network metadata that your organization already has, Lumu unlocks this valuable data for you, without the need for a learning process or intricate adjustments.

Additionally, Lumu runs in the cloud so you don't need to invest in expensive hardware and is scalable according to your needs. If you have multiple locations or environments we offer unlimited virtual appliance data-collectors and we store your network metadata for up to 2 years for further analysis with our exclusive Playback™ feature.

Can Lumu replace my current NTA?

Absolutely. Lumu can add incredible value to the security strategy of your organization, whether you have a legacy NTA or not.

Organizations that have not invested in an NTA find Lumu sufficient to reduce the impact of cyber attacks, maximize their security team's efficiency, and drastically improve their compromise detection efforts. With Lumu, businesses become empowered by the intelligence provided and use it to make informed decisions on future investments that allow for a stronger cybersecurity program.

Conclusion

Not all NTA solutions are designed the same way. The raw material may be similar, but the critical thing is what we do with the data. We can only find what we look for. According to ESG Showcase: The Missing Link in Cybersecurity "Many NTA products available today were designed as network performance tools and later evolved into cybersecurity solutions. However, Lumu was purposely designed to analyze network traffic to measure compromise intentionally and continuously."