EMA Vendor to Watch: Lumu Technologies

Value Proposition

The enterprise recognizes the value of security, as indicated by the myriad of services and solutions in the information security market. Even with year-to-year record spending in cybersecurity, organizations continue to experience breaches. Worse, the time to detect a breach—upwards of 200 days by some estimates—demonstrates that adversaries are staying hidden and exploiting compromises in the enterprise network, playing a longer, more orchestrated game of gathering intelligence and acquiring the most valuable assets.

Lumu's approach rethinks the security paradigm, one that has tried to keep attackers out of key enterprise networking assets. Instead, Lumu makes the assumption that cybercriminals are already inside the enterprise's environments and creates a Continuous Compromise Assessment model: collecting, normalizing, and analyzing network metadata, including DNS, Netflows, Proxy and Firewall Access Logs, and Spambox. This data assessment leads to a continuous review of the compromise levels within the enterprise environment.

Lumu's strategy is focused around three core tenants:

- **A Simple Solution for a Big Problem:** Alert fatigue is something that all enterprise security groups try to address. Lumu's solution is very easy to deploy and operate, allowing the enterprise to systematically measure compromise in a way that is non-intrusive yet valuable to decision makers and security operators.

- **Actionable Insights to Validate Current and Future Security Strategy and Spending:** Using Lumu, decision makers and security leaders gain immediate (and continuous) insight into which security tools are working, while also showing what gaps exist. This information can then be used for budgeting, resource prioritization, and future projects/development. Without these insights, business leaders will continue the cycle of spend and pray, never really knowing the ROI on their security spend.

- **Flexible for Any/All Security Environments:** Often, a new security solution augments, but also displaces, existing tools and services, adding to the environment's complexity and instability. Lumu integrates with these existing solutions and services—even in the most siloed and complicated environments—to produce a constantly evolving picture of how these solutions work together to protect the enterprise.

EMA Perspective

As a research firm, EMA is constantly hearing about the latest security services and solutions, and nearly all of these solutions and services are designed to keep the bad actors out of the enterprise environment and to protect business-critical resources. As good as these tools may be, business leaders look at the overall big picture: did the investment in these security tools and services really secure the business as advertised?

While signing that purchase order for the next big security tool may provide a certain level of comfort, the unfortunate truth is that the overall security of the business may not have improved, mainly because they were not asking the right questions.

Lumu asks the right question: through their Continuous Compromise Assessment, they use the metadata already available in the enterprise network to give a constantly changing and thorough evaluation of the security status of the enterprise. They have shifted the paradigm—they assume that a company has already been compromised. Put simply, instead of attacking using a shotgun approach, casting a wide pattern in hopes of hitting everything, Lumu takes the sniper's approach to security investment, identifying specific areas of weakness and providing insights to repair those areas where the company is most likely to experience a breach. As the environment improves/evolves or new technologies (for the good guys and the bad guys) change the threat landscape, the continuous assessment allows businesses to shift and retarget priorities and resources to react to emerging threats.

Enterprise Management Associates has declared Lumu a 2020 Vendor to watch due to the unique paradigm shift insights that it provides to business leaders and security analysts regarding the threats and vulnerabilities already in the environment. There are plenty of point solutions in the security market that the enterprise can use—sometimes even collaboratively—to protect the business. However, Lumu's approach to using these tools to continuously assess the vulnerabilities and compromises of the enterprise demonstrates that the company clearly qualifies as a Vendor to Watch.

EMA