LUMU

ENLIGHTENMENT BRIEF:
Lumu and DNS Firewalls

How does Lumu compare to a DNS firewall?

Lumu and DNS firewalls are different technologies, designed with different purposes in mind.

For starters, Lumu is a technology that was built from the ground up with a single objective: **help to measure and understand your unique 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.

On the other hand, a DNS firewall is a network security solution that prevents network users and systems from connecting to known malicious internet locations. DNS firewalls work by employing DNS Response Policy Zones (RPZs) and correlating them with threat intelligence.

How can Lumu and DNS Firewalls work together?

If your company already has a DNS firewall like OpenDNS (currently, Cisco Umbrella), Infoblox, or the like, Lumu Insights seamlessly integrates with your DNS firewall to continue to benefit from blocking malicious DNS requests, while layering real-time compromise assessment. In order to assess compromises effectively, one must take into consideration a wide range of network metadata sources. For this reason, DNS is only one of many network metadata collected and analyzed. Lumu Insights also collects network flows, proxy logs, firewall logs, and spambox to have a complete and detailed view to detect and understand compromise incidents and build the ability to respond in a precise and timely manner.

> The ability to measure real-time compromise helps to fight the false sense of security provided by technologies focused on only blocking threats, such as DNS firewalls and the like. **Blocking malicious DNS requests is good, but the ultimate goal is to eliminate the residual compromise** from the device that triggered the blocked DNS request. Today's malicious threats like ransomware, banking trojans, and others include DGA (Domain Generating Algorithm) capabilities. That means that the compromised device will continue to trigger malicious DNS requests generated by the DGA indefinitely until it can finally reach its C&C and cause harm to the enterprise.

If you do not have a DNS firewall in place, Lumu provides full and enhanced visibility of the DNS requests made to adversarial infrastructure and provides more insight into compromises with the broad network metadata collected. Even when most attacks use DNS infrastructure, it is critical to visualize the attacks that go directly to IP addresses and to know the lateral movements inside the organization.

In addition, Lumu includes Compromise Context and the automated MITRE ATT&CK® Matrix that enriches confirmed compromise with factual data related to each compromise's distribution, behavior, movement, and more. By accessing our Threat Triggers, you can enable policies that contain these compromises using your current cybersecurity infrastructure. Consequently, you can invest time to understand and eradicate each compromise, so you and your team can respond in a precise and timely manner.

Can Lumu replace the DNS Firewall?

DNS firewalls and Lumu are solutions used to address different challenges. Lumu can add incredible value to the security strategy of your organization whether you have a DNS firewall or not.

Organizations that have not invested in a DNS firewall 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

DNS firewalls serve a specific purpose and it is critical to understand that they are unable to provide conclusive evidence of compromise levels or serve as a compromise detection solution. Lumu's patent-pending data collection and analysis process is built to effectively detect compromise and allow organizations to respond to compromises quickly and precisely via Lumu API to orchestrate the defense.

Learn more at: **lumu.io/product/**