Nomic Networks
https://nomicnetworks.com
(972) 991-5005

ENHANCED NETWORK SECURITY

WHY OPERATIONALIZE THREAT INTELLIGENCE?

IT administrators and security analysts spend an enormous amount of time normalizing disparate threat intelligence feeds, and integrating a mountain of information into SIEMs and other visibility tools, and to what end? Lots of great data and good ideas, but sifting through the data fast enough to take action can be a challenge.

Enter the foundational premise of a Threat Intelligence Gateway - to operationalize threat intelligence data more proactively for threat prevention, not just analysis. That means consolidating threat sources, automatically blocking known threats with minimal false positives, and streamlining security operations.

Not convinced that active threat intelligence should be a critical part of your network security? Consider this:

Improved Security and Network Efficiency

Threat intelligence gateways clear the way for a firewall to be much more effective in detecting advanced and unknown threats because they greatly reduce the noise-to-signal ratio that the firewall is bombarded with. By applying active threat intelligence, the incidence of catching blocked malware and ransomware before it penetrates the network goes up from as little as 40% to as much as 85%.

Reduced Staff Workload

Threat intelligence gateways reduce the IT staff workload while significantly increasing threat prevention. Threat intelligence gateways are fixed-function devices that autonomously collect, process and analyze all types of internal and external security data, giving real-time network protection.

A Simple, Effective Layer of Security

Threat intelligence gateways can help IT staff create policy management rules for blocking industry-focused attacks, targeted attacks, and “noise” from threat actors. The key is to manage these devices consistently, which ensures the network will be protected by accurate and timely data with low incidences of false positives.

By applying active threat intelligence, the incidence of catching blocked malware and ransomware before it penetrates the network goes up from as little as 40% to as much as 85%.

Clearly, threat intelligence is key to mitigating security risk and preventing damaging network breaches. But, traditionally, this level of sophisticated network security was only available to large enterprise customers. For relatively little cost, threat intelligence gateways give all organizations access to the same enterprise-level data and pro-active monitoring that larger organizations enjoy.