White Paper

An introduction to a data-first strategy for network security

Enterprise security teams must adopt a "data-first" strategy

We all know that data runs the modern world, whether you're getting directions with live traffic conditions on your phone, or part of a team tracking down bad actors across the globe. But most enterprises have not truly adopted a data-first strategy when it comes to their own internal security infrastructure, and that's a strategic mistake.

For years, most security solutions have been centered around detecting and stopping known or static threats. Of course that is necessary, but it's not enough to deal with the novel, dynamic, ongoing threats facing us today. Despite the massive investment and efforts of our best cybersecurity experts, serious breaches occur on a daily basis, sometimes causing massive financial, reputational, and operational damage. Something isn't working. But what?

Today's attackers are more sophisticated, more persistent, and more adept at hiding in normal traffic, "living off the land," or embedding themselves in management systems, often waiting patiently until the right moment to take action without triggering any alerts. An approach that is centered around passively collecting neutral, security-relevant evidence long before a threat is known or uncovered is essential to help defenders go back in time and understand what happened.

A data-first approach with Corelight

Corelight can help your organization implement a data-first security strategy that fits into your current cybersecurity ecosystem by using a proven methodology built on an open source technology platform. Our solutions have been battle-tested over decades and used in production at massive scale by the most-attacked, most sensitive and largest organizations in the world.

The fundamental idea behind a data-first approach is to collect security-relevant data from network traffic continuously, across your on-prem, cloud and virtual environments, instead of relying exclusively on alerts or AI-driven decisions made by imperfect algorithms and "black-box" security solutions. The fine-grained, security-relevant data that Corelight extracts from network traffic can be integrated into your SIEM, data lake, or XDR platforms. Once collected, that data can be used by your network defenders, your compliance organizations, your network operators, or your data analytics staff to meet a multitude of your organization's requirements.

The foundation of a data-first strategy has three key pillars

1. Don't rely on perimeter-based, alert centric tools alone; assume that attackers will circumvent them. Those tools like firewalls, threat intel, intrusion detection systems and the like are necessary, but insufficient.
2. Monitor network traffic at key locations 24/7 with security-specific, non-judgmental sensors, and combine the evidence collected with other data (like endpoint data). Network traffic, properly monitored for security threats, is an essential source of evidence for understanding the context around attacks.
3. Keep compact, curated, security-relevant data long enough (probably years) so it will be available (and useful) for investigations. In today's security environment, attacks can persist undetected for many months, or even years.

A data-first posture enables threat hunting and anomaly detection, and also reinforces the "intruder's dilemma:" We know that in modern attacks, intruders may make many moves over long periods of time across the network. But we defenders only need to find one of them. When the right data is available, that theory becomes reality.

Another critical benefit of this approach is that customers own their own data, it's not locked inside of a black box security solution that may become obsolete. That means as new threats emerge over time, defenders have access to revisit and reexamine the data for evidence of past attacks that may become more visible with new IOCs or other information.

Corelight provides critical evidence for defenders

Our solutions are built on the gold standard for network defenders: Open source technologies that have been deployed and relied upon by the most sophisticated defenders at global companies and governments agencies in defense, civilian and intelligence agencies around the world.

Our network detection and response (NDR) solutions scale from small networks to enterprise-level global IT infrastructure at the highest speeds (currently networks up to 100 Gbps can be monitored by a single 1U Corelight Sensor).

We also provide insights and detection capabilities beyond the raw data to help you understand threats that might be lurking in encrypted traffic (without break-and-inspect), as well as helping you detect potentially malicious behavior like command and control (C2) activity with techniques developed by our research arm, Corelight Labs.

For more information, visit www.corelight.com

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497