corelight

White Paper

Why Zero Trust requires uncompromising network visibility

Recent attacks on SolarWinds, Microsoft Exchange, and the Colonial Pipeline highlight the need to accelerate security modernizations across both private and public infrastructure. President Biden's new executive order[1] for improving U.S. cybersecurity outlines a rapid path forward, which includes a mandate for federal agencies to "advance toward Zero Trust Architecture," which "eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."

However, an organization's operational picture will be as precise and reliable as the telemetry that informs it. Information collected for this purpose should therefore be:

- **In a uniform data format**—security analysts, automation tools, and machine learning algorithms need clean, consistent data formats to make quick judgment calls, convict and remediate threats with confidence, and train detection models.

- **Purpose-built for security**—the data should be designed for security use cases to avoid the pitfalls of common telemetry sources intended for IT and compliance. Their data collection biases leave gaping security visibility holes behind.

- **Resistant to compromise**—adversaries will attempt to muddle the "operational picture" by compromising upstream telemetry, up to and including generating false information from hijacked sources.

- **Designed for interoperability**—information collected should interoperate with tools and complementary data sources to facilitate fast correlations for analysis and investigation tasks.

While endpoints provide a critical source of information to form this picture, organizations who single thread their operational awareness on EDR technology do so at their peril. Endpoints offer an excellent depth of information, but that depth does not reach where EDR agents cannot (e.g., BYOD, Cloud, etc.). That depth is also rendered meaningless when adversaries succeed in evading or compromising the endpoints or EDR agents themselves.

Comprehensive network monitoring can address these security gaps left by EDR with complementary coverage that excels in the aforementioned information collection requirements, notably in its "resistance to compromise." No matter the environment, nearly all cyberattacks must communicate over networks and organizations that can silently capture, analyze, and store those communications to gain an immutable record of malicious activity. Unlike endpoints, the network cannot lie.

The attacks on SolarWinds and the investigation that ultimately led to its discovery provide strong evidence for these claims. Consider that the SUNBURST malware specifically looked for the presence of EDR agents in the target environment to inform its evasive maneuvers.[2] What SUNBURST couldn't avoid, however, was communicating over the network. While it took pains to obfuscate and disguise the nature of its communications, it ultimately left indelible evidence of its activity for organizations with comprehensive network monitoring capabilities in place. The Mandiant research team that discovered these attacks was able to do so in part because they had these capabilities on hand, a fact publicly acknowledged by one of the researchers involved in the investigation:

> *We leveraged a *lot* of tech, and this investigation only solidified my belief that an NSM stack isn't complete without Zeek. Obfuscatory attacker actions had a hard time hiding from all the research done by the folks at @corelight_inc.*[2.]

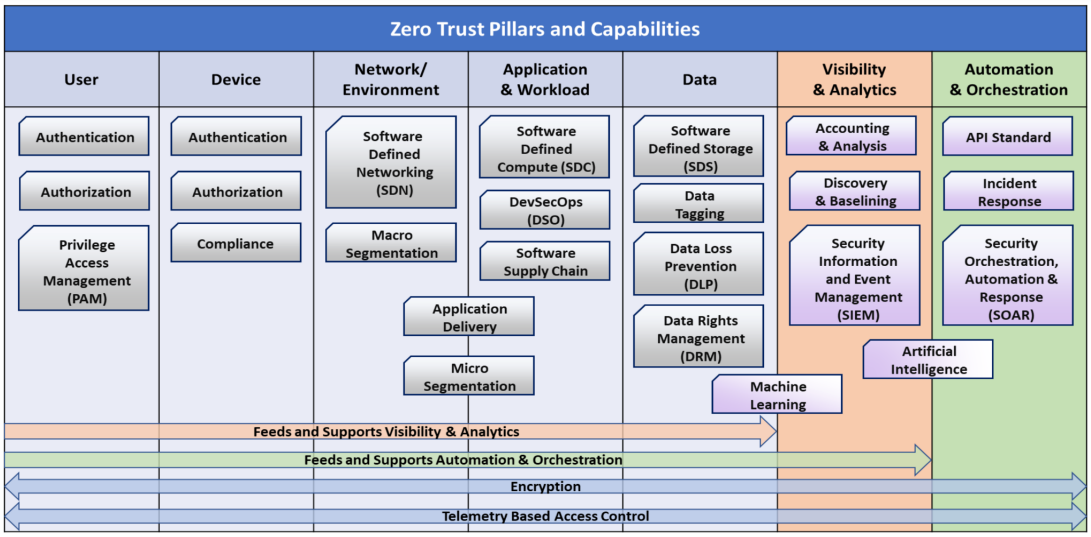
Thus, it becomes clear why robust Zero Trust architectures require uncompromising network visibility. Network vantage points can give organizations a strategic data reserve that's resistant to compromise and can support security operations in a Zero Trust environment from continuous verification to deep, dark investigations.

Endpoints and networks together provide a complementary and multilayered data surface critical to supporting Zero Trust implementations. Recent guidance from the National Security Agency on "Embracing a Zero Trust Security Model" supports this notion, as the NSA lists "Inspect and log all traffic before acting" among its four key guiding design principles for implementing Zero Trust:[3]

> **Inspect and log all traffic before acting**—Establish complete visibility of all activity across all layers —from endpoints and the network—to enable analytics that can detect suspicious activity

Corelight's role in supporting Zero Trust architectures

The most recent Zero Trust Reference Architecture from the Department of Defense enumerates seven focus areas (pillars) and more than two dozen supporting capabilities within and across these areas.[4]



The table below maps to this DOD framework and highlights focus areas where Corelight's platform can deliver value:

Pillar	Corelight capability
User: *The ability to continuously authenticate, authorize, and monitor activity patterns to govern users' access and privileges while protecting and securing all interactions*	EDR only provides a limited subset of the context required to validate the authenticity of authenticated logins. Corelight delivers the evidence necessary to prove, without repudiation, that the user connected from an authorized system, using an authorized protocol/application, at an authorized time and that the connection was terminated after the authorized duration expired.
Device: *The ability to identify, authenticate, authorize, inventory, isolate, secure, remediate, and control all devices.*	Corelight can provide evidence that encryption was not only used with a given device but includes all metadata associated with the connection, including IP, packet size, protocol, port(s), and time. Corelight can also provide visibility around software versions used on the device.
Network and environment: *The ability to segment (both logically and physically), isolate, and control the network/environment (on-premises and off-premises) with granular access and policy restrictions. It is critical to (a) control privileged access, (b) manage internal and external data flows, and (c) prevent lateral movement.*	Corelight offers network sensors capable of monitoring logically and physically separated networks, providing visibility around internal and external data flows and lateral movement via its connection-oriented logging framework that deeply parses a wide range of protocols, including those associated with lateral movements such as SMB and RDP. As one Corelight customer remarked, "with Corelight, the ability to track lateral movement in your network skyrockets."[5]

Pillar *(continued)*	**Corelight capability** *(continued)*
Visibility and analytics: *The ability to understand performance, behavior and activity baseline across other Zero Trust pillars and capture and inspect traffic, looking beyond network telemetry and into the packets themselves to accurately discover traffic on the network, observe threats that are present, and orient defenses more intelligently.*	Corelight's platform excels in this area by providing comprehensive network visibility, parsing dozens upon dozens of protocols, including encrypted protocols Kerberos, SSL, and SSH. Each log includes a unique connection UID that allows security analysts to quickly pivot and see the full protocol activity of a given connection. Corelight also verifies the traffic's identity via a dynamic protocol detection process that looks past the port and header information to validate the correct protocol. This means Corelight can reliably identify unencrypted and encrypted traffic streams no matter the port or protocol. Corelight's Encrypted Traffic Collection has dozens of unique insights around SSL, SSH, and RDP connections that go beyond logging the protocol, with dozens of inferences such as brute force attack detections. Corelight's C2 Collection helps analysts discover command and control activity with over 50 unique insights and detections. Battle-tested by some of the world's most sophisticated organizations, these directions cover both known C2 toolkits and MITRE ATT&CK C2 techniques to find novel attacks.
Automation and Orchestration: *The ability to automate manual security processes to take policy-based actions across the enterprise with speed and at scale.*	An effective Zero Trust SIEM/SOAR strategy relies on the ingestion and correlation of NDR and EDR activity logs. Corelight's network data and insights are uniformly formatted and ready for automation. Corelight has built automation playbooks for Splunk's Phantom platforms to accelerate investigations.[6]

[1]*"Executive Order on Improving the Nation's Cybersecurity" President Joseph R. Biden Jr. May 12, 2021.*
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2]https://twitter.com/srunnels/status/1338329916304199680

[3]*"Embracing a Zero Trust Security Model." National Security Agency. February 2021.*

[4]https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[5]*"Zero Trust Reference Architecture." Department of Defense. Version 1.0. February 2021*
https://dodcio.defense.gov/

[6]https://www3.corelight.com/education-first-use-case

[7]https://corelight.com/integrations/soar-playbooks/

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