corelight

White Paper

Network Detection & Response
A how-to instrumentation guide

Because most attackers traverse your network, Network Detection & Response (NDR)[1] is an indispensable security tool to defend against increasingly sophisticated cyber attack techniques. NDR gives you visibility into the activities occurring on the network, so you can identify patterns of anomalous behavior that indicate compromise.

Traditional approaches to NDR involve analyzing captured packets (PCAP) or network device IT logs (e.g., NetFlow or DNS server records). The challenge is these network data sources were designed for IT and not for security at scale and speed. More than a few hours or days of historical PCAP traffic is too much to store, and yields insights slowly via painstaking, manual packet analysis. Device IT logs like NetFlow and DNS server records are comparatively easier to store and search, but are difficult to correlate and ultimately data-thin, leaving massive network visibility gaps that attackers can easily slip through. DNS server records, for example, typically do not contain DNS query responses, that security analysts need to discover some DNS attack vectors.

The quality of inputs determines the quality of outcomes, and NDR is no exception. You need great network data to achieve great security outcomes. This data needs to be comprehensive, interconnected, extensible, and as lightweight as possible so security analysts and tools can make lightning-fast sense of it. That's why the open-source Zeek network security monitor has become the industry gold standard for network security data: it excels in all regards.

It's not only the quality of network data that determines NDR outcomes, but also the manner in which you instrument NDR in your environment. Let's look at four general areas where NDR can be applied to your network so you can get immediate enhanced visibility. As we introduce each area, several of the common MITRE ATT&CK tactics will be mentioned. A list of questions for each is also provided to help defenders identify anomalous activity using an NDR solution.

The trouble with data is too much of a good (and bad) thing

The most experienced defenders recognize that physical network metaphors such as perimeters are antiquated and have embraced a data-centric approach to NDR. After embracing a data-centric approach, the first challenge is to determine which data sets are valuable. This requires investing analyst time collecting and operationalizing those sets to help speed detection and establish prioritization and response. Identifying and operationalizing data is perhaps today's most difficult and urgent cyber challenge.

Defenders frequently collect a broad range of data types, but these are disconnected and require independent investment to build, deploy, and maintain. This results in personnel being inundated and besieged with stale, duplicate, and irrelevant information. In contrast, NDR with Corelight provides deep network visibility with lightweight, connected Zeek logs that parse protocols on the wire, delivering the network-derived information needed to investigate events in real-time or after a detection notice—without the administration overhead. Corelight data lets defenders operate at the rate at which adversaries are developing new attack vectors.

"The best organizations will have metrics to measure whether they are winning or losing an engagement with an adversary that is calculated in real-time and derived from data gathered using the broadest possible surveillance."
–The Second Age of Cyber[2]

How to use this guide

Using several deployment scenarios, we'll show you how defenders can win against adversaries by implementing a data-centric approach with NDR instrumentation. These scenarios address the fundamental deployments of NDR at network egress (aka north/south), and intra-network communication (aka east/west) points.[3]

To assist in understanding the value of NDR instrumentation at these locations, we reference tactics from MITRE ATT&CK and the information security tenet of auditing to frame value. The MITRE ATT&CK framework contains twelve tactics, each containing many techniques. Each technique may be accomplished via multiple methods, and the method employed by each adversary varies based on the adversary objective, victim security, operating system, credentials, and location within the network.

Each scenario posed includes a few questions for security architects and analysts to apply when evaluating the use of NDR on their organization's network. These questions are designed to help assess the network derived data available within each area of the network, and promote team dialogue about the development of hunting theories, dashboards, and the cultivated set of NDR data available to use to defeat adversaries.

Review each scenario with a Corelight engineer to establish how NDR can enhance and tune your existing security through verification, sighting, and investigation. The first NDR deployment selected will vary depending on the organization's existing security posture, level of risk acceptance, and security architecture.

How and where to apply NDR to your network

Deploy NDR in multiple locations

Treat NDR like endpoint detection solutions with a goal of complete coverage because all security professionals know a user somewhere will click a link—whether it is well crafted or not. By instrumenting networks with defenses that observe Initial Access, security personnel can act before adversaries achieve their objectives.

Deploying sensors at multiple locations increases the opportunity to detect ATT&CK tactics likely to be used and observed on that portion of the network. For instance, techniques that fall within the Initial Access, Persistence, Exfiltration, and Command and Control (C2) tactics are more likely visible at network egress points. Adversaries will use the tremendous volume of HTTP and HTTPS traffic as concealment to hide data exfiltration or C2 in the traffic "noise." Within a network, Persistence, Privilege Escalation, Discovery, Lateral Movement, and Collection tactics are more visible. Evidence of compromise visible with NDR could be if one or more internal devices are probing the network, consuming data, or reusing credentials.

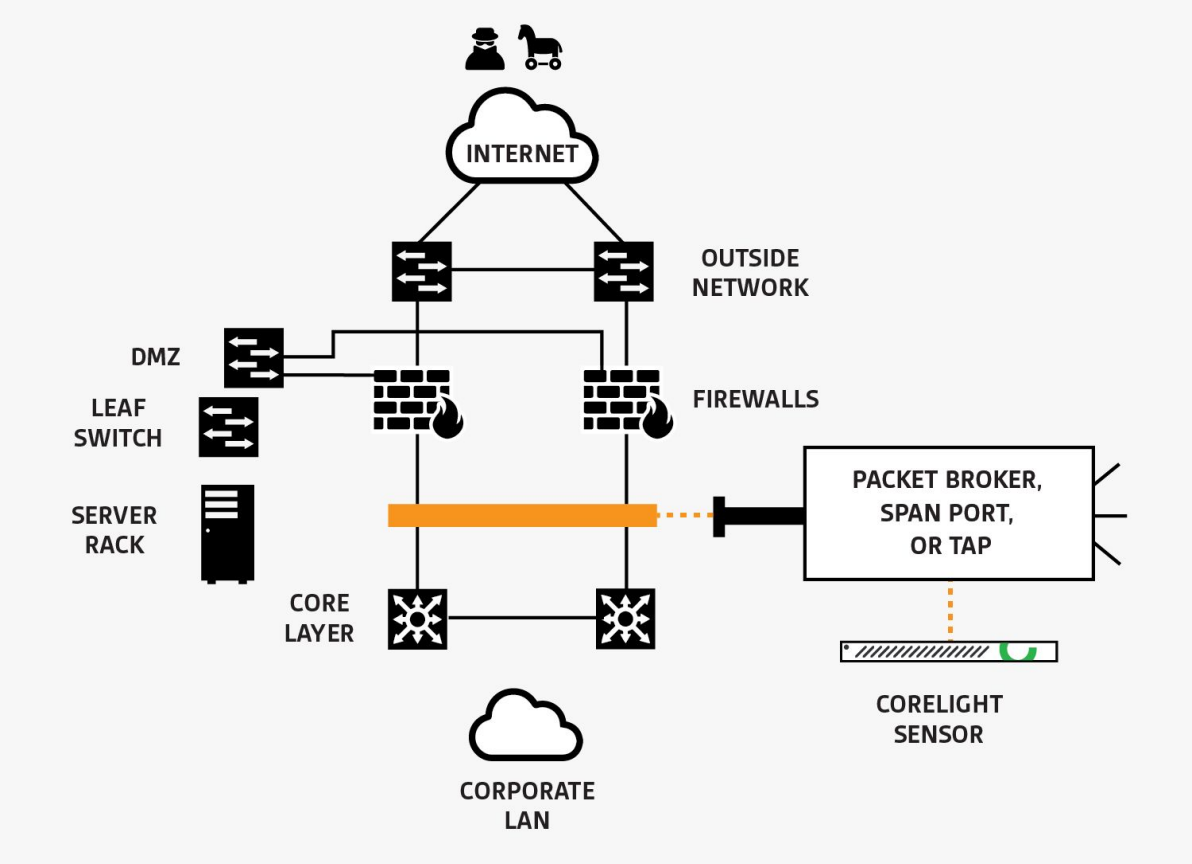
Scenario 1: Use NDR for network egress (aka internet access) monitoring

Instrumenting the enterprise to monitor at network egress points provides enhanced visibility for all communications with external networks. This location traditionally has been monitored by a firewall and intrusion detection/prevention system. Unfortunately, the value of a network is its ability to allow people and organizations to pass ever-changing data types and formats. This creates a changing, porous entry point into an organization, placing the network prevention tools at a significant disadvantage. To complement and improve an enterprise's prevention system, Corelight Sensors should be deployed to verify, sight, and tune the existing prevention devices. This process is fueled by network-derived data.

A Corelight Sensor should be deployed at the network egress point. If network address translation (NAT) is occurring, the tap or packet broker should be placed prior to the NAT. If TLS inspection (aka TLS break and inspect) is being performed, Corelight Sensors have additional monitoring ports and can combine streams to provide context-rich data for all ingress and egress network traffic.

When performing NDR at network egress, questions to ask include:

- Are any prohibited protocols traversing the network?
- Is there anything interesting in the HTTP transactions traversing the network?
- Which DNS servers are being, and have been, used?
- What insight do you have into encrypted sessions entering/leaving the network?



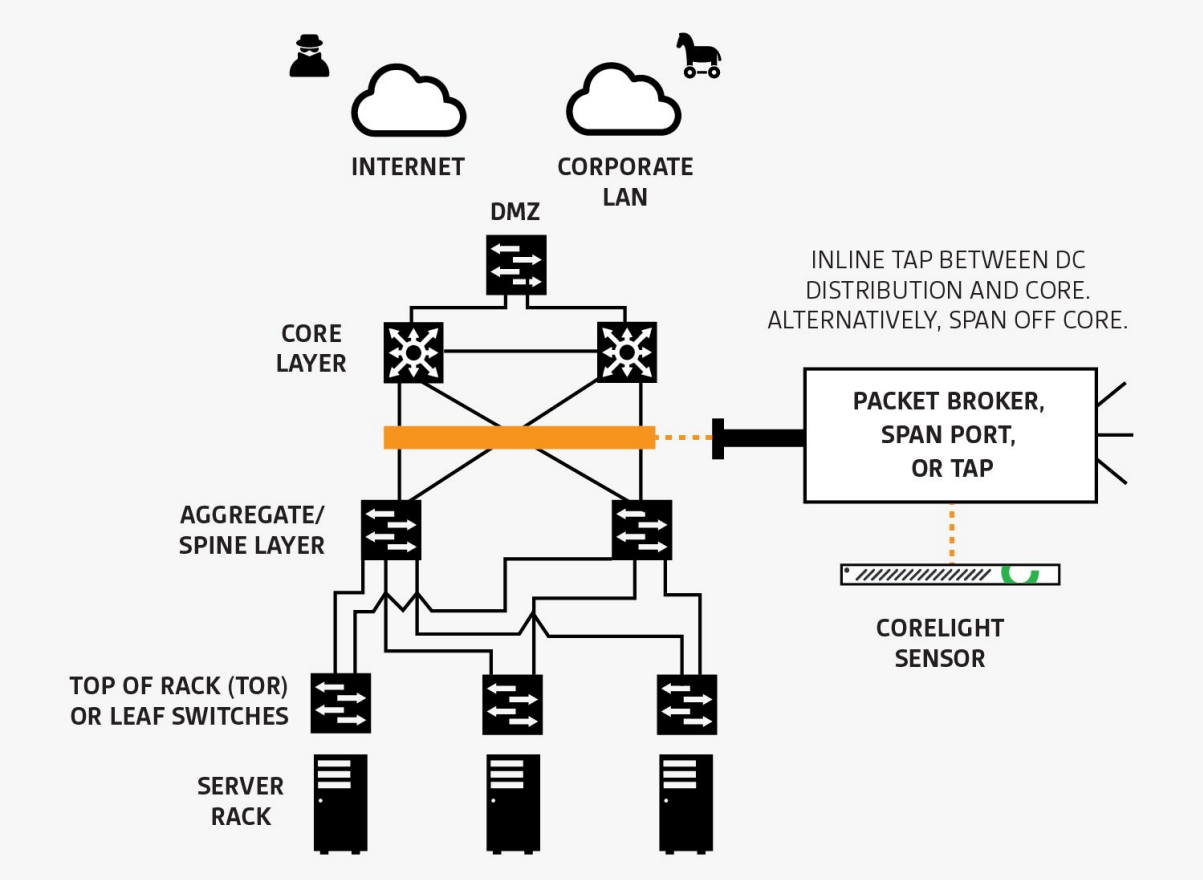
Scenario 2: Use NDR to monitor server farm egress (aka client to server)

Server farms are often locations where the most valuable data in an organization resides. Instrumenting the enterprise with NDR at server farm egress points provides visibility for internal and external network communications. Unfortunately, server farm demarcation is often only monitored by a router providing NetFlow data for intra-network communications. In some instances this demarcation may also be monitored by a firewall and/or intrusion detection/prevention system. These prevention and IT logs are data-thin and do not provide enough information to support a data-centric approach to discovering adversary actions and containing them.

A Corelight Sensor should be deployed at the server farm core layer to complement prevention systems. When NDR is deployed at the server farm egress, information formerly absent becomes available to answer questions, including:

- Is any suspect DCOM or RPC traffic occurring between servers and hosts?
- What volume of data is being transferred between individual servers and client(s)?
- Is there encrypted traffic that does not belong?
- Is there a history of files transferred?
- Are any hosts starving others for resources?

- Which Microsoft protocols are being used between servers and internal hosts?
- Are any prohibited protocols traversing the network?
- What insight do you have into encrypted sessions entering/leaving the network?



Scenario 3: Use NDR to monitor intra-data center activity.

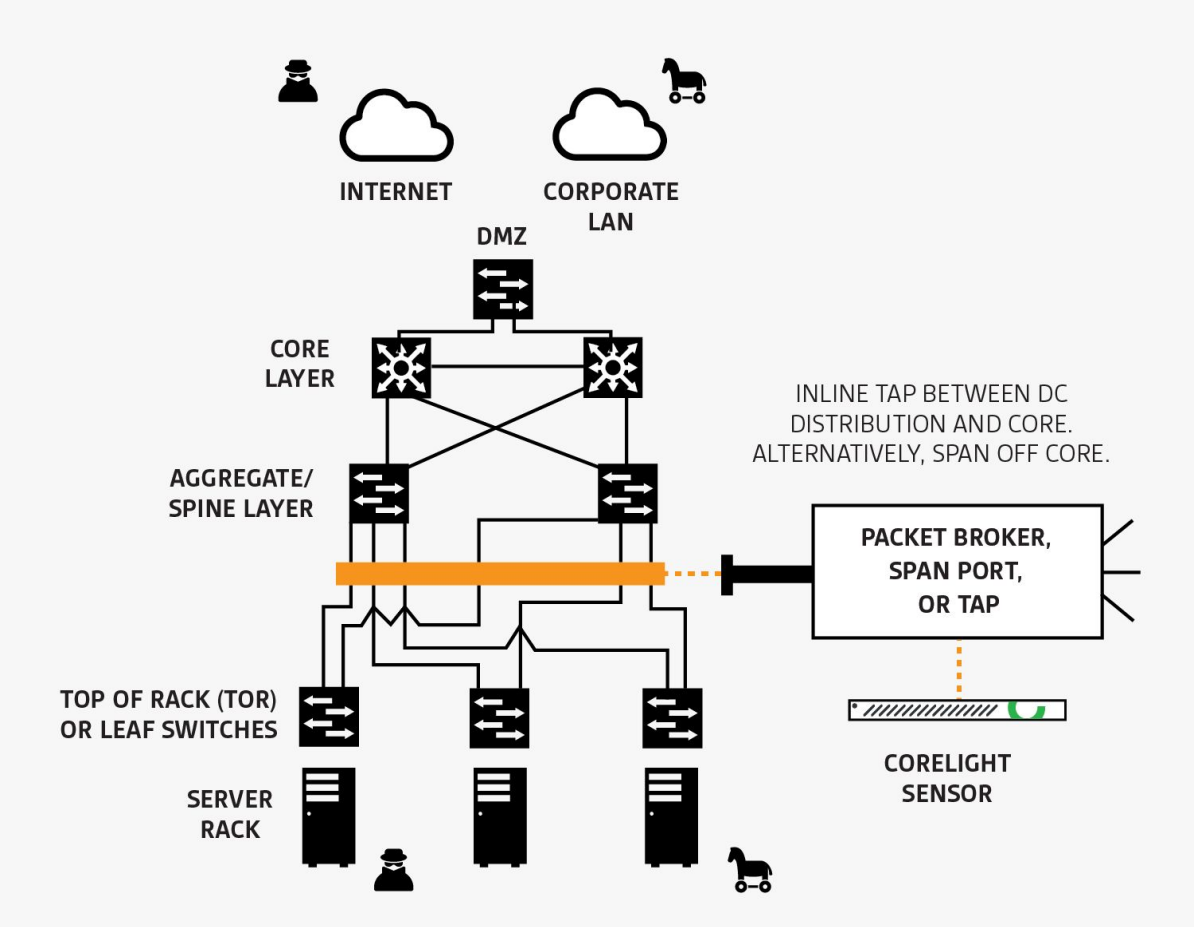
Communication between devices within a data center is often a security blind spot. Data centers have a heterogeneous mix of applications and operating systems that creates a broad attack surface adversaries can exploit to discover devices and services.

A Corelight Sensor should be deployed at the aggregate/distribution or spine layer of a data center. If NAT is occurring, the tap or packet broker should be placed prior to the NAT.

When using NDR to monitor communications within a data center, evaluate the data and ask:

- Are there hosts that switch from producing to consuming data?
- What are users/hosts authenticating?
- Are any prohibited protocols traversing the network?
- Are any unknown protocols in use?

- Are you performing attachment extraction and analysis?
- Is there suspect DCOM or RPC traffic between servers and hosts?
- What is the volume of data being transferred between individual servers and client(s)?
- Is there encrypted traffic that does not belong?
- Is there a history of files transferred?
- Are any hosts starving servers for resources?
- Which MS protocols are being used between servers and internal hosts?
- What insight do you have into encrypted sessions entering/leaving the network?

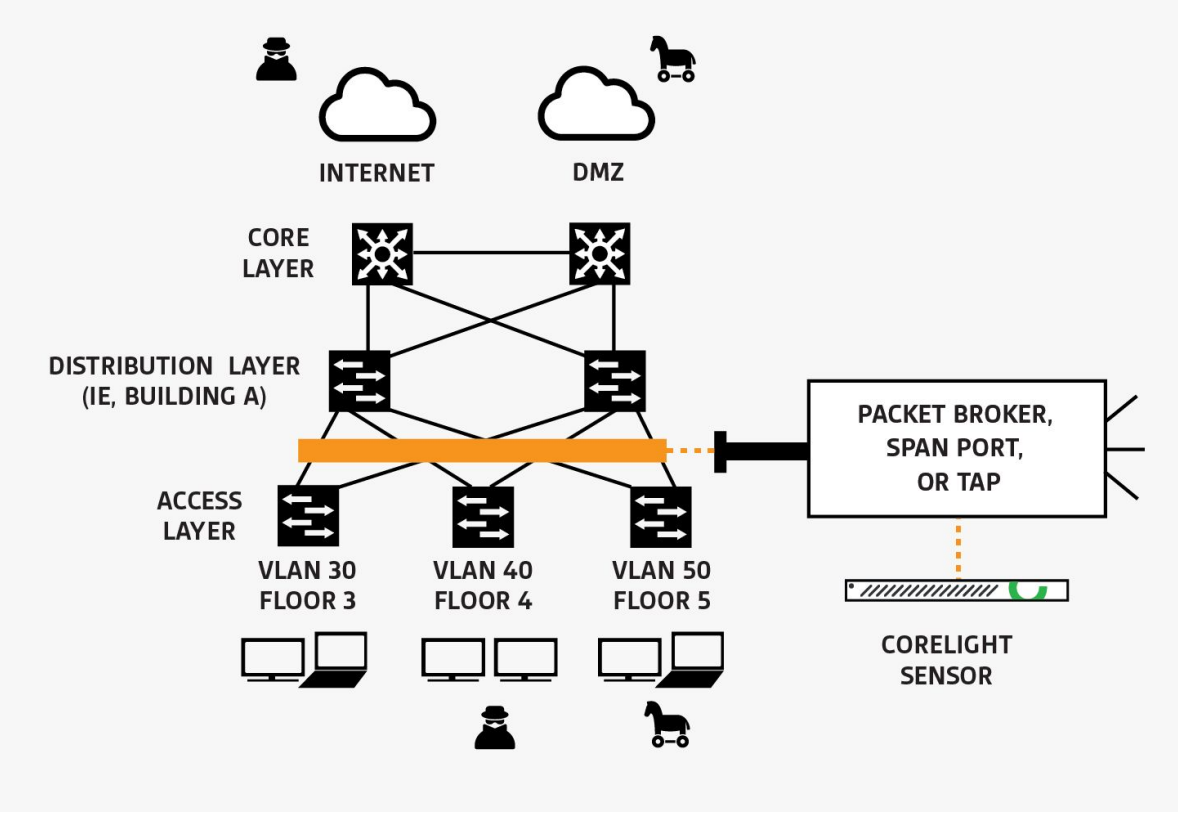


Scenario 4: Use NDR to monitor inter-workstation activity.
Another blind spot is communication between host device workstations within an enterprise. Enterprises have a heterogeneous mix of devices and operating systems that creates a broad attack surface adversaries can use to discover users, devices, and services to exploit.

A Corelight Sensor should be deployed at the aggregate/distribution or spine layer of the enterprise. If NAT is occurring, the tap or packet broker should be placed prior to the NAT.

When using NDR to monitor communications within enterprise hosts, a new data set is available when asking the following questions:

- Why are two end points communicating?
- Are any endpoints performing reconnaissance?
- Which software applications are installed?
- Is this in agreement with the enterprise inventory?
- Are administrative tasks occurring from the user area of the network?
- Are any users connecting to hidden or administrative shares?
- Which user agents are in use?
- Are any prohibited protocols traversing the network?
- What users/hosts are authenticating?
- Are there hosts that switch from producing to consuming data?
- Are any unknown protocols in use?
- Are you performing attachment extraction and analysis?



Corelight Sensors—network visibility made elegantly simple.

Corelight Sensors—available in appliance, cloud, and virtual models—deploy quickly and run Zeek, the NDR solution with more than twenty years of use in the largest SOCs in the world. Zeek has been

protecting large educational and government institutions for decades, but only within the past five years has it been made easy to access and install for a growing number of global organizations and enterprises. Our sensors complement existing security prevention measures, and position you to quickly begin identifying threat actors.

Corelight Sensors enable deployment of a grid that generates cultivated, rich sets of network data, forming an integral part of a knowledge base. This data speeds reliable observation and detection and assists in avoiding the pitfalls of prevention dependence, while providing context for a deeper and more accurate historical analysis. Improved data speeds reliable near-term, real-time observation of network activity, as well as forensic analysis, allowing your time to be invested on threat defense instead of administration. Corelight's NDR solution simplifies management, increases scalability, and provides incontrovertible data that both establishes a timeline for events that become incidents, and measures the severity of incidents.

[1] Network Detection & Response is often referred to as Network Detection & Response (NDR) or Network Security Monitoring (NSM).
[2] The Second Age of Cyber, https://www.fathom5.co/
[3] The same principles apply for cloud-based implementations.

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