Enterprise Strategy Group™
by TechTarget

Open NDR: A Flexible Platform for Detection and Data Across Hybrid Environments

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

SEPTEMBER 2024

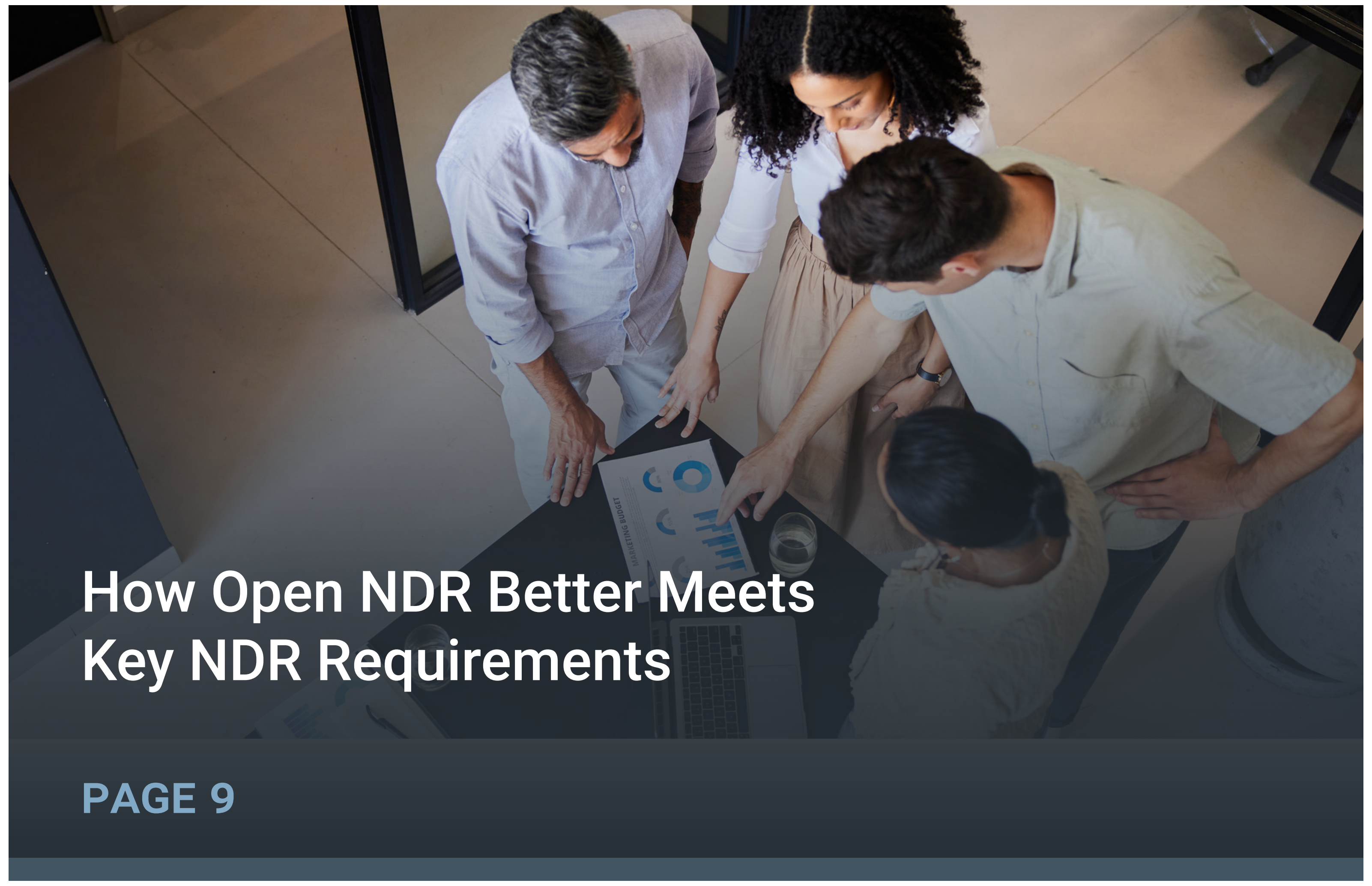
Introduction

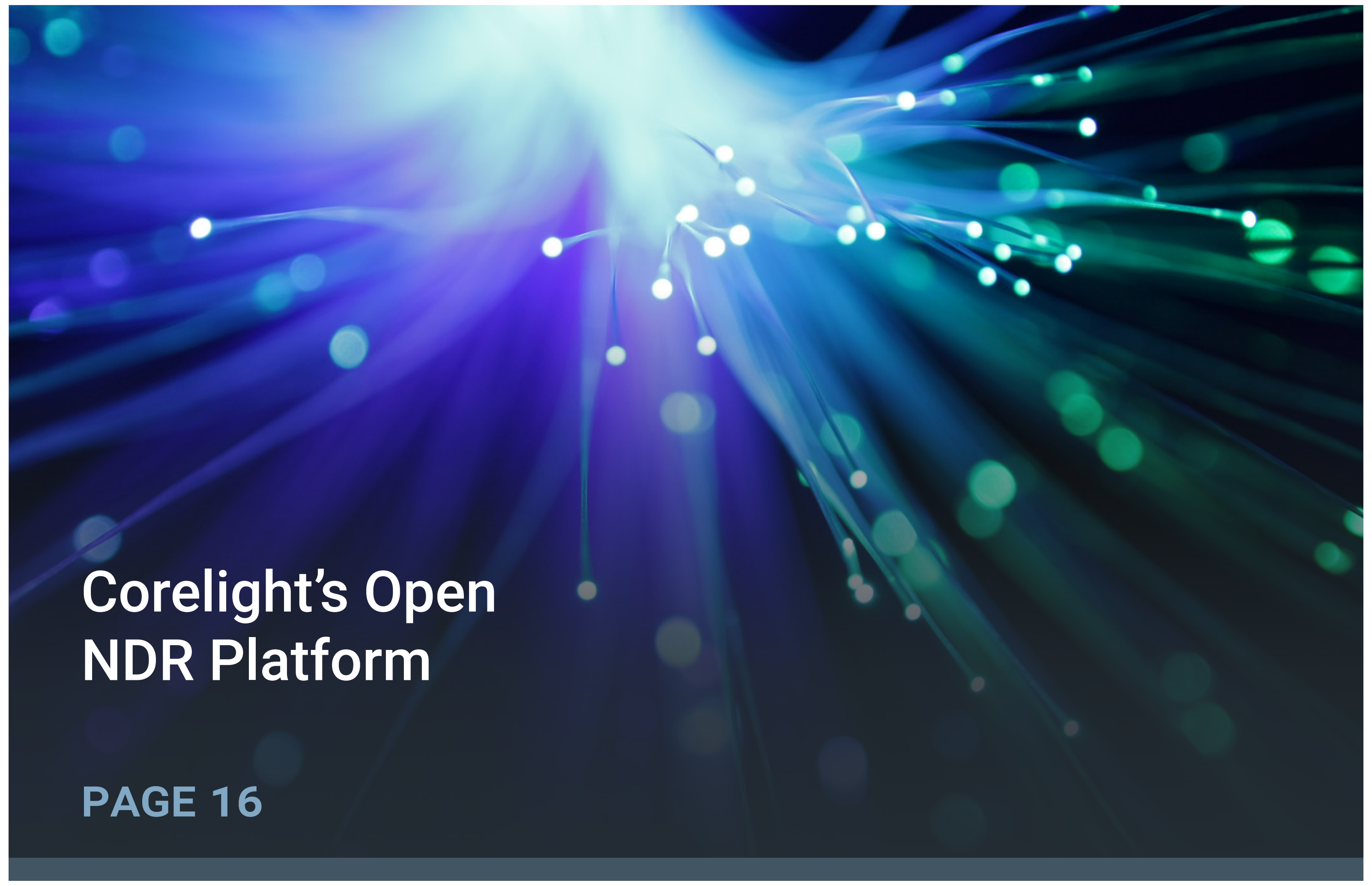
Network detection and response (NDR) is a critical component of today's security operation center (SOC) strategy. It should be evaluated by any security team rightly concerned by the gaps created by increasingly hybrid, multi-cloud environments and left unfilled by an architecture overly dependent on endpoint detection and response (EDR) and security information and event management (SIEM).

Part of that evaluation should be understanding the fundamental differences between open NDR and closed NDR. Closed NDR is predicated on proprietary detection and data formats that can make it difficult for customers to understand, modify, and extend their capabilities. Closed NDR often provides alerts without the full context needed to validate them, creating excessive noise that can quickly overwhelm security teams.

Open NDR is based on open source detection and data formats, which empowers customers with a transparent, flexible, and standardized data set that can be leveraged across the SOC to accelerate response, improve detection coverage, and expand visibility. The architecture of open NDR enables it to evolve with the organization and deliver the rich data and detections, flexibility, and broad use case support today's security teams need.

CONTENTS





"There's no single, consistent blueprint organizations can follow as they build their SOC."

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

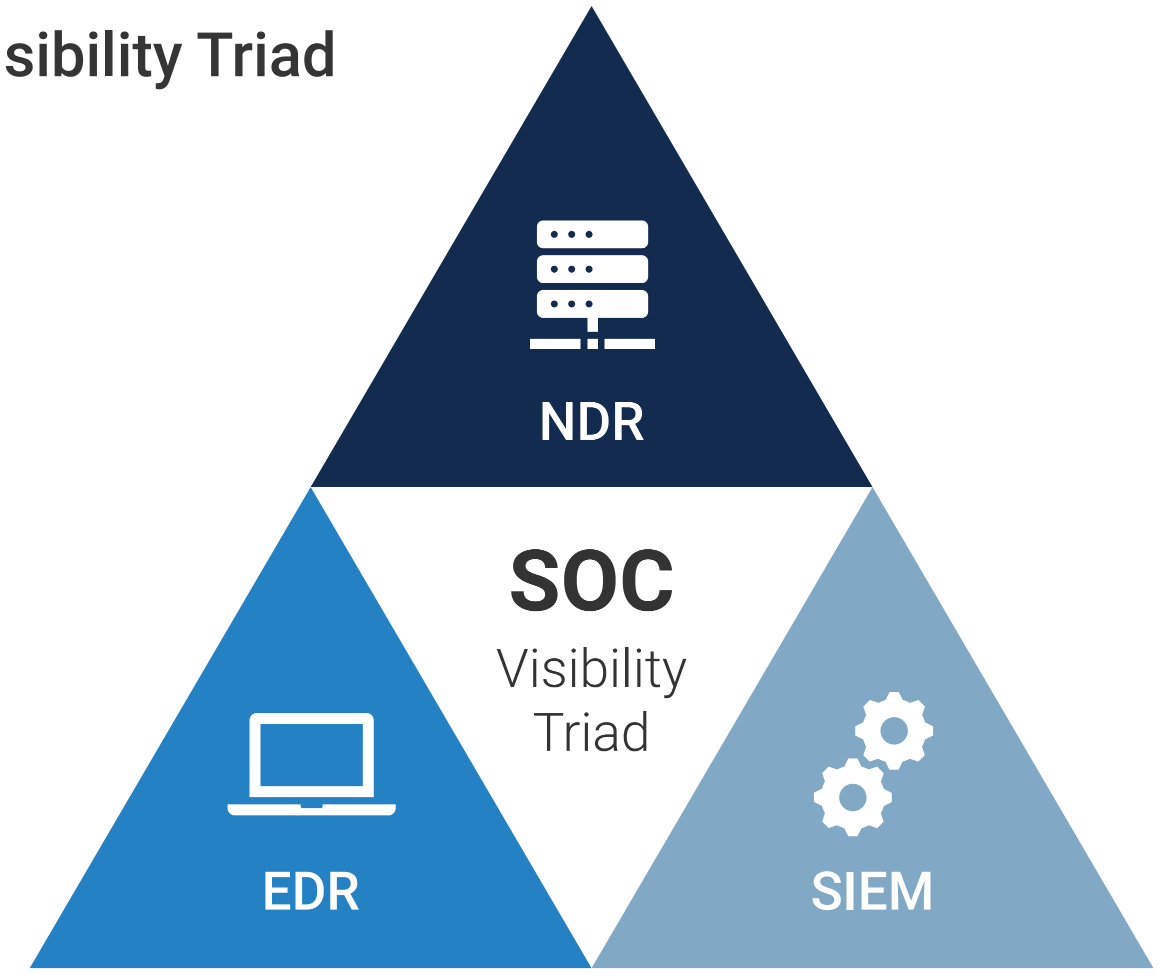
Network Visibility Remains Critical to Threat Detection and Response

The SOC Visibility Triad Aims to Close Threat Detection and Response Gaps

There's no single, consistent blueprint organizations can follow as they build their SOC. The broad range of practices, tools, and services, coupled with the varying levels of sophistication and skills, require every organization to find their own combination for success. Yet, with this said, the SOC visibility triad has emerged as an important framework that security teams need to consider as they work to improve their cybersecurity posture. It identifies the need to aggregate data from three core pillars to detect threats early, ensure comprehensive visibility across the environment, and reduce alert fatigue. The components of the SOC visibility triad include:

- **EDR to provide visibility into endpoint activity and processes.**
- **SIEM for log and user behavior data.**
- **NDR for network traffic analysis and threat detection.**

Figure 1. SOC Visibility Triad



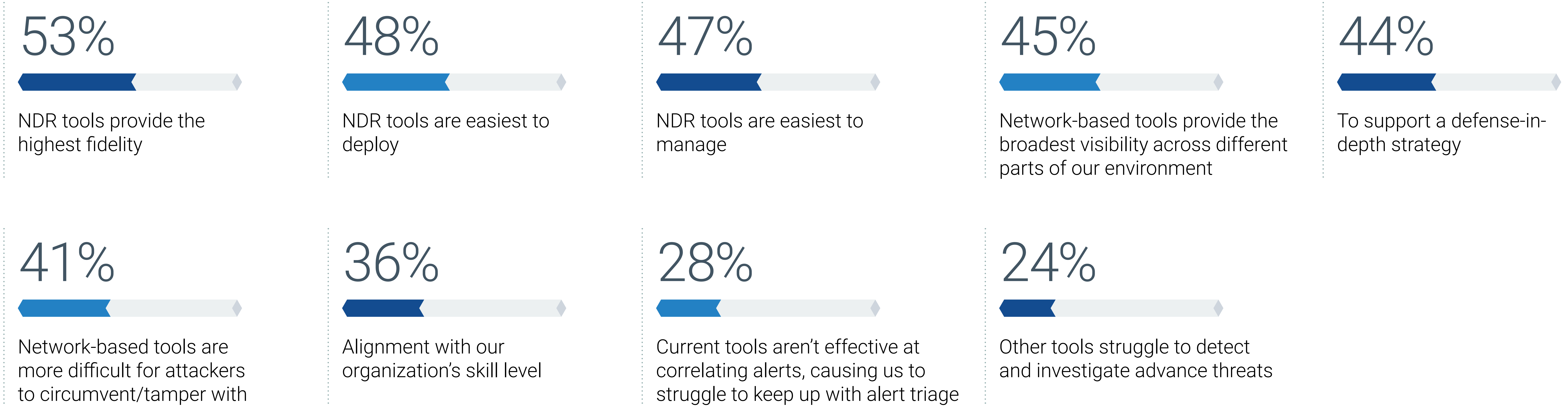
The Importance of NDR

NDR has emerged over the last few years as an updated approach to network traffic analysis (NTA). Rather than simply baseline traffic, as legacy NTA systems have, NDR solutions typically use a mix of signature, behavioral, and machine learning techniques on collected network data to identify potentially malicious activity. Further, NDR tools enable analysts to respond to incidents, either natively or through integrations with other tools, and also support threat hunters for proactive defense.

With enterprise environments now including cloud infrastructure and remote workers, some have questioned the role of network-based security solutions. Yet, this visibility and control remains critical to overcoming the key limitations of EDR and SIEM tools. For example, EDR agents do not deploy in cloud environments or on unmanaged and IoT endpoints. Full EDR deployments can take months, quarters, or even years in large organizations with tens of thousands of endpoints. Further, one of the first actions an attacker will take after compromising an endpoint is to disable the EDR agent to prevent detection.

NDR offers distinct advantages in some of these areas. Respondents to research from TechTarget's Enterprise Strategy Group cite the ease of deployment, ease of management, broad visibility, and difficulty for attackers to circumvent as key reasons they use or plan to use NDR tools. But at the top of the list, more than half of organizations (53%) call out the high fidelity NDR provides as a primary reason to use NDR tools.[1] As the adage goes, "The network doesn't lie."

Figure 2. Primary Reasons NDR Tools Are Used



[1] Source: Enterprise Strategy Group Research Report, *The Evolving Role of Network Detection and Response*, March 2023. All Enterprise Strategy Group research references and charts are from this research report unless otherwise noted.

BACK TO CONTENTS

Organizations Struggle With Cloud Adoption, Stealthy Attacks, Tools, and SOC Overload

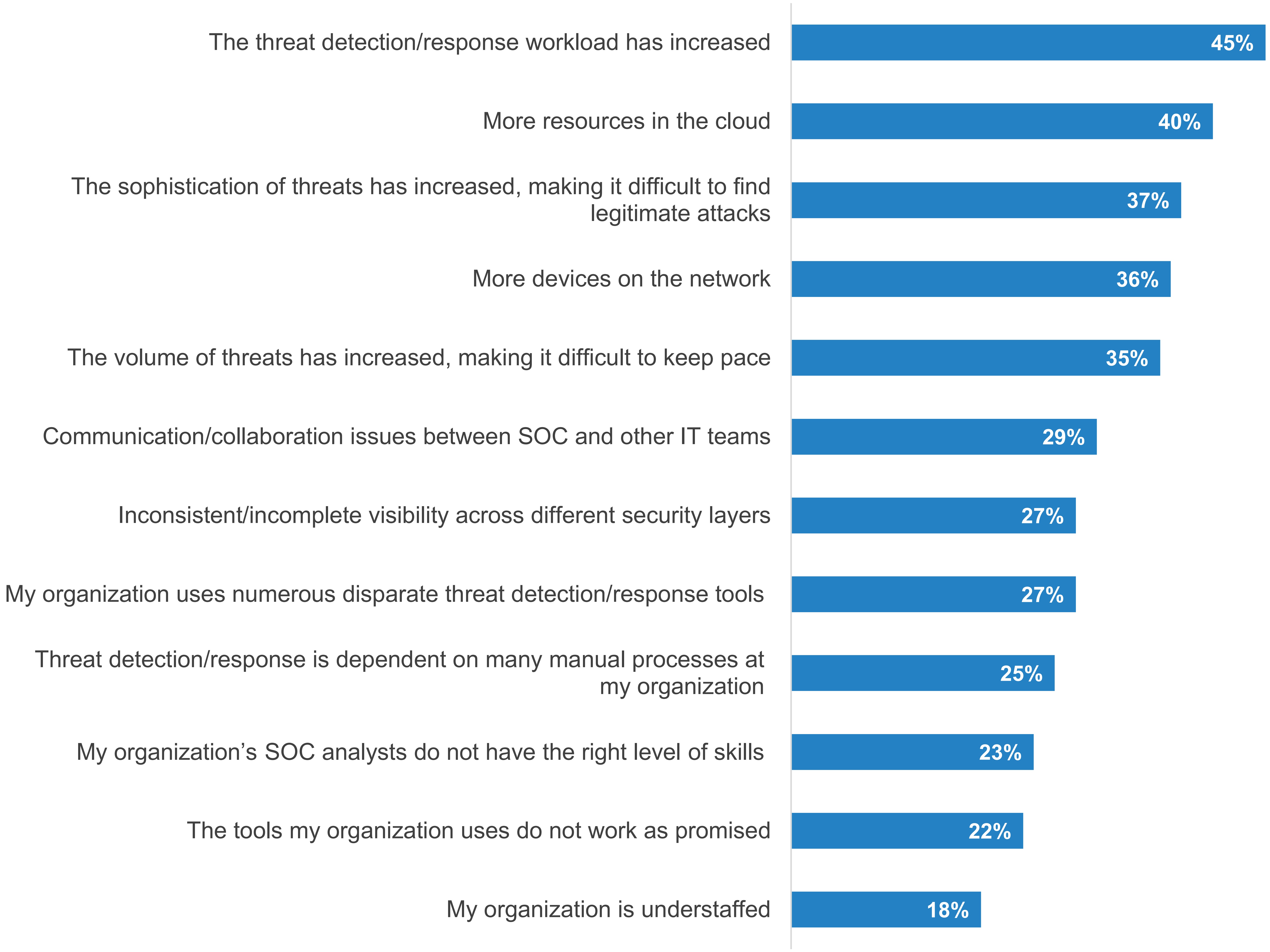
Even as many organizations have come to rely on the SOC visibility triad, security teams continue to face a variety of challenges when it comes to threat detection and response (TDR). Some of the most common are:

- **Cloud adoption and tool proliferation.** 40% cite the increase of resources in the cloud as a top TDR challenge, while 27% say the disparate tools their organization uses poses an issue. There are a variety of security tools available to protect cloud resources; many are cloud-only (such as cloud security posture management and cloud-native application protection platforms) or difficult to deploy at scale (such as EDR and cloud workload protection platforms). This fragmentation prevents security teams from gaining a comprehensive picture of what is happening across both the on-premises and cloud aspects of their environment, allowing attackers more time to discover and exfiltrate sensitive data. Further, these tools often use VPC flow logs based on traffic metadata rather than the packets themselves, making the detection of stealthy attacks more difficult.

- **Stealthy attacks.** 37% of organizations cite the sophistication of threats and difficulty finding these attacks as a top challenge they face with TDR. Attackers are opportunistic, and when their attacks rely on zero days, targeted malware, encryption, and other advanced tactics, the attacks often lead to longer dwell times and, as a result, are more damaging.

- **SOC overload.** These issues, coupled with the skills shortage many organizations face, negatively impact SOC analysts. Nearly half (45%) say the increased TDR workload is their biggest TDR challenge.
  The need for analysts to manually integrate data sources, sort through alerts that may not be indicative of malicious activity, and generally try to keep pace leads to dissatisfaction and staff turnover.

Figure 3. Threat Detection and Response Challenges

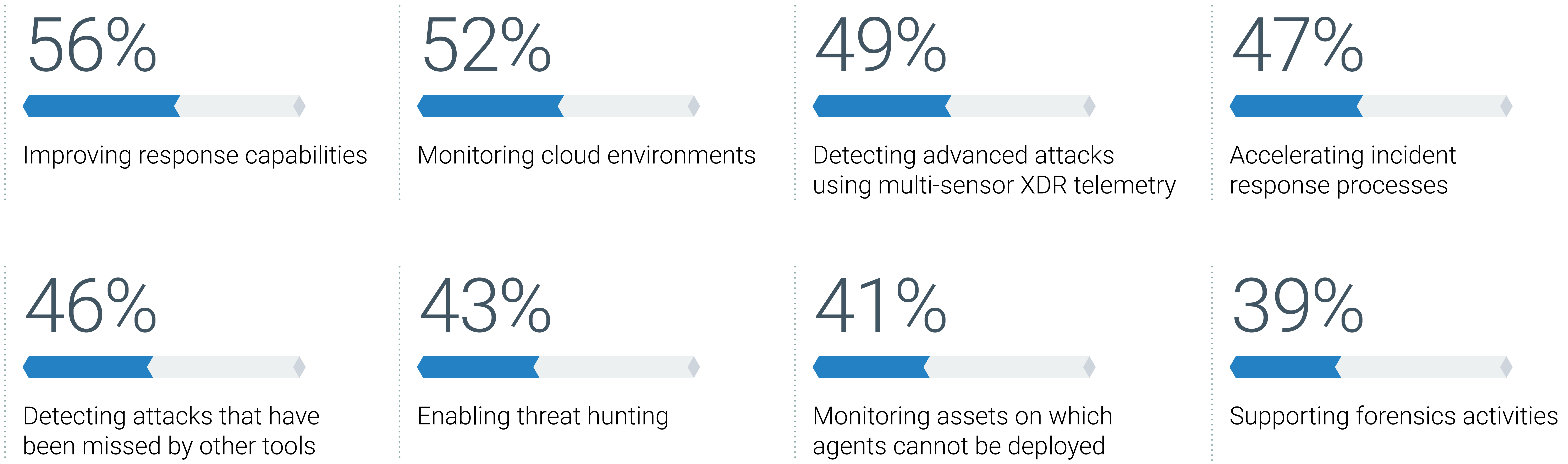


Spotlight: The Role of NDR in Cloud Security

While network-based tools have not always been primarily associated with protecting cloud environments, perceptions have begun to shift. In fact, when asked what use cases their organization does or will support with its NDR tools, more than half (52%) of respondents cited monitoring cloud environments. A variety of tools are available to support cloud security from endpoint vendors, workload protection vendors, as well as the cloud providers themselves. So why do so many organizations use NDR to detect threats in their cloud environment?

The agentless architecture is attractive from a scalability and management perspective. Rather than IT or application teams having to deploy agents across countless workloads, network and security teams can deploy a sensor once on a VPC or VNet and collect traffic without slowing development teams down. Additionally, the reality that attackers do not act in on-premises or cloud silos means security teams must defend in the same way. The ability to correlate activity across different locations and resources and paint a comprehensive picture of the environment is critical for organizations to defend against these modern attacks and respond efficiently when activity is discovered. Finally, the out-of-band detection offered by NDR ensures that attackers cannot disable tools during an attack to avoid detection.

Figure 4. Top NDR Use Cases



"When asked what use cases their organization does or will support with its NDR tools, **more than half (52%) of respondents cited monitoring cloud environments.**"

How Open NDR Better Meets Key NDR Requirements

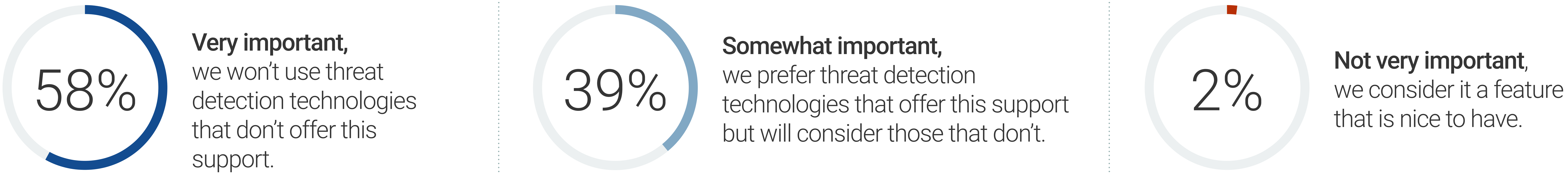
Limitations of Closed NDR Platforms

Most NDR solutions are proprietary, or closed, meaning the vendor owns the source code, detection mechanisms, data models and format, and underlying platform. In many cases, these tools are positioned as easy to use: Once deployed, they will alert on suspicious activity without significant analyst intervention. Unfortunately, the lack of customization and focus on alerts can lead to high alert volume. Further, because analysts are not provided with the underlying data triggering the alert, the triage and investigation process to validate whether something malicious has occurred is much more onerous.

Additionally, these solutions are often designed to support a narrow set of use cases or fill a specific need. Some NDR solutions are designed for smaller organizations that do not use a SIEM and, thus, do not offer strong SIEM integrations. Others may be focused on supporting more advanced organizations that do use a SIEM and, as a result, do not offer a native investigative console. Because closed NDR tools are not customizable, it often is not possible to expand to additional use cases or modify the platform to fill adjacent needs. Ultimately, the rigidity of this closed model can limit the use cases addressed, efficiency of SOC analysts, and overall effectiveness of the security organization.

Security practitioners seem to recognize this and have begun to gravitate toward more customization to achieve better results. As an example, Enterprise Strategy Group research has found that 58% of organizations indicate it is very important that their TDR technologies support the ability to develop custom rules and/or custom machine learning models, with another 39% saying it is somewhat important.[2]

Figure 5. Importance of Custom Rules and/or Machine Learning Models



Very important, we won't use threat detection technologies that don't offer this support.

Somewhat important, we prefer threat detection technologies that offer this support but will consider those that don't.

Not very important, we consider it a feature that is nice to have.

[2] Source: Enterprise Strategy Group Complete Survey Results, *SOC Modernization and the Role of XDR*, September 2022.

BACK TO CONTENTS

Rich Detections and Data, Flexibility, and Broad Use Case Support Are Critical

Every organization is unique and may use NDR in a different way. As a result, NDR tools must have a few key attributes to help organizations overcome the TDR challenges they face and effectively support the SOC visibility triad. Among the most important of these are high-fidelity detections and data, flexibility, and support for a range of use cases.

High-fidelity detections.

While security analysts need to be made aware of suspicious activity on the network, there is a point of diminishing returns when alerts turn into noise. The value of a true positive detection is greatly diminished, if not rendered irrelevant, if an analyst is overwhelmed by meaningless or low-priority alerts and cannot quickly triage an alert queue and validate the true positive. Consequently, the accuracy, transparency, and tunability of detections in NDR tools have an enormous impact on incident response outcomes. Buyers should prioritize tools that deliver high-fidelity detections that make it easy for analysts to quickly triage and validate the alerts generated.

Rich network data across on-premises and the cloud.

Capturing basic quintuple-connection data via flow logs from on-premises sources is simply not sufficient to detect suspicious behavior in most cases. NDR tools must provide mechanisms for cloud data collection, normalization, and correlation with on-premises data. Further, NDR tools should provide not only flow data but also direct access to raw packets and files to derive meaningful insights. At the same time, as dwell time has increased, so has the need to access data beyond the typical 30- or even 60-day retention window many packet capture (PCAP) solutions support. Solutions that provide metadata or summarized protocol data across the network bridge the gap and ensure security teams can identify attacks retroactively. Additionally, the prevalence of encrypted traffic, coupled with the cost, complexity, and privacy implications of decryption, is a growing issue: 83% of organizations say scanning encrypted traffic for threats is a significant or notable concern. Tools that can provide visibility and identify potential threats in encrypted traffic without decrypting provide significant value and help alleviate these issues.

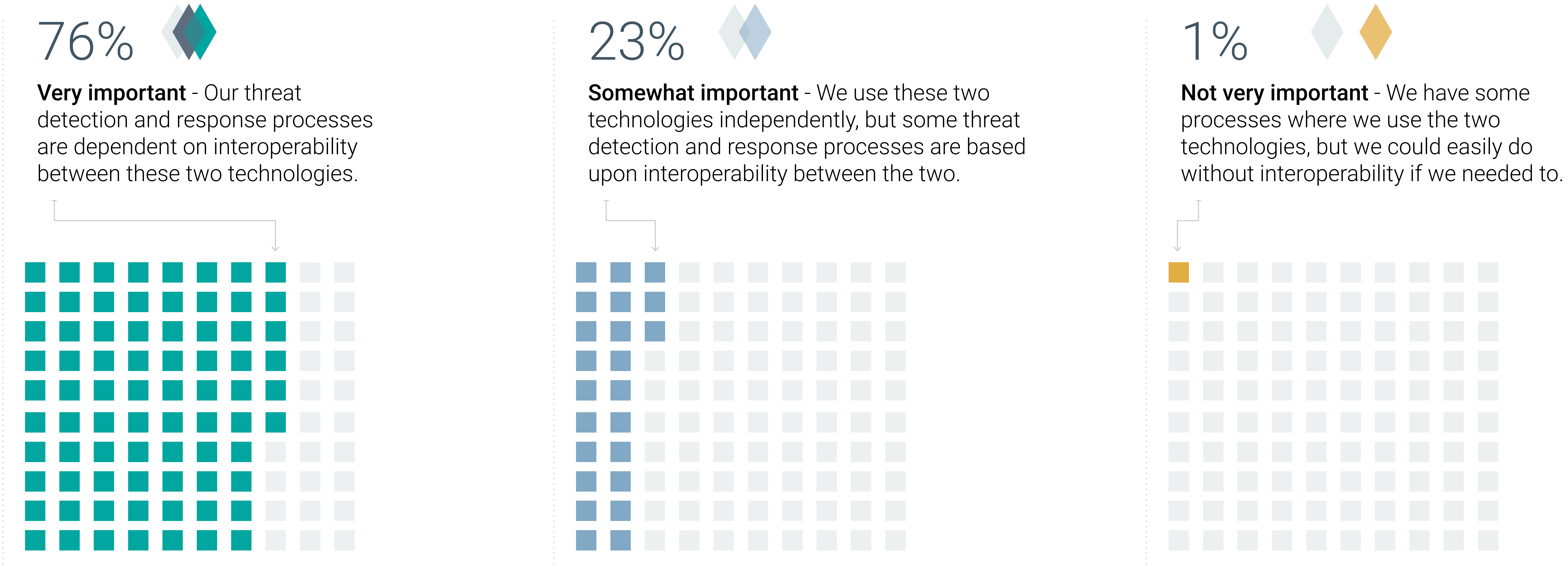
Flexibility.

Every environment is different, requiring NDR tools to offer hardware and software options to address both on-premises and cloud deployments for comprehensive coverage. Solutions that present on-premises and cloud data in a unified view are important to improve analyst understanding of the data and accelerate response actions. Similarly, every security team and each analyst works differently, meaning NDR tools must support a variety of usage scenarios. Some organizations may want to forward network data or detections into the SIEM for further investigation, while others may want to triage directly in the NDR console. 76% say interoperability between NDR and other threat detection and response technologies is very important because of processes that are dependent on those tools working together. Tools that provide both SIEM and security orchestration, automation, and response (SOAR) integrations, as well as native response capabilities, enable analysts to work in the manner they're most comfortable.

Support for a range of use cases.

Along these lines, the power of network data plays a critical role in activities such as triaging alerts from other sources, incident response, threat hunting, network hygiene, and compliance. The ability to customize how the data collected by NDR tools is correlated, set custom detections, and dive into the weeds of the data itself rather than simply relying on the detections the tool provides is critical in these cases.

Figure 6. Importance of Interoperability of NDR and Other TDR Tools



76%

Very important - Our threat detection and response processes are dependent on interoperability between these two technologies.

23%

Somewhat important - We use these two technologies independently, but some threat detection and response processes are based upon interoperability between the two.

1%

Not very important - We have some processes where we use the two technologies, but we could easily do without interoperability if we needed to.

BACK TO CONTENTS

What Is Open NDR?

In contrast to proprietary or closed NDR, open NDR has emerged as an option for organizations prioritizing rich data, flexibility, and broad use case support. Open NDR is based on open source detection and data formats, which empower customers with a transparent, flexible, and standardized data set that can be leveraged across the SOC to accelerate response, improve detection coverage, and expand visibility. The architecture of open NDR enables it to evolve with the organization and deliver the rich data and detections, flexibility, and broad use case support today's security teams need.

Open NDR delivers these capabilities through its adherence to three main principles: open source, open data, and open architecture.

Open source.

The reliance on open source software lends its name to the open NDR concept. Rather than rely on a single vendor for stewardship of the technology and capability advances, open source software is community-driven, providing a broader base for innovation and the ability to leverage community-driven detections and visibility capabilities.

Open data.

An open source foundation leads to an open data model, allowing organizations to hire and train people based on broad knowledge of the data model in the industry (being industry standard), iteration and improvement of the model through a community rather than a company, and the power to influence transformative technology that has been trained with open data and open models that are continuously present on the internet (e.g., large language models).

Open architecture.

Coming back to a key point made earlier, NDR does not operate in a silo. Organizations adhering to the SOC visibility triad require interoperability between tools to achieve success. Because they are built on an open architecture, open NDR solutions can more easily plug into environments with a diverse and changing set of tools. The open data model helps security teams consume network telemetry where it makes the most sense for them. Ecosystem and integration partnerships mean less work for security teams to incorporate open NDR into the existing tool stack.

The Advantages of Open Core

The security industry has relied on open source tools for a variety of functions for years. These options provide a different cost model, the benefit of community-driven feedback and development, and avoidance of vendor lock-in. Examples include Wireshark for network protocol analysis, Suricata for network analysis and threat detection, and Zeek for security logging and behavioral detections.

Yet while open source can provide key benefits, there are some drawbacks. Open source products are free to procure, but there can be unclear implementation and management costs since more is left to the practitioner to manage. Additionally, while the security of open source code has the benefit of many eyes, the lack of specific responsibilities can lead to flaws or vulnerabilities.

Open core merges the best of both the open source and proprietary models by leveraging an open source foundation with a commercial business model to deliver an open architecture with the flexibility and usability organizations need. There is a long, successful history with open core products both in and outside the security space that backs up this model. Examples of open core solutions include:

- Snort and ClamAV, which are widely used both in open source form and through tools delivered by Cisco.
- OpenVPN, which offers free, open source point-to-point and site-to-site VPNs, as well as paid versions.
- The Elasticsearch Platform and Elastic Stack, which are available as free, open source software or as commercial offerings from Elastic.

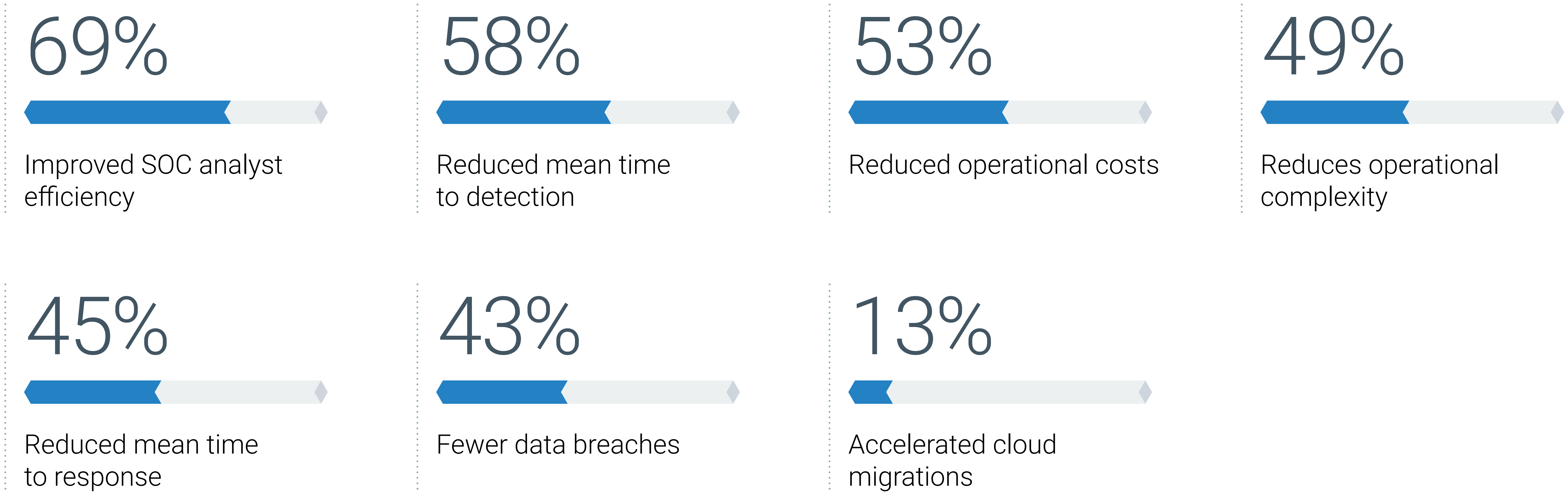
All of these examples provide organizations with the ability to choose the option that works best for them. Their success highlights how strong communities can collaborate to build strong software offerings and the value organizations place on open core approaches. From an open NDR perspective, this comes down to the power of shared detection and visibility development via the community. A single vendor can use its team to respond to a topical threat, whereas an open source community can have members from across the world, with a diverse set of perspectives and data, create and iterate on a detection for the strongest security outcomes.

The Clear Value of Open NDR

Rather than stitching together a variety of network telemetry sources, the consolidation of intrusion detection system (IDS), PCAP, and rich network data on an open NDR platform yields operational benefits in terms of management and configuration as well as investigation and response. Additionally, the ability to identify all services across cloud environments with consistent network telemetry and host data enrichment provides comprehensive visibility integrated with the cloud control plane. The open data model provided by open NDR helps security analysts curate and analyze a broader set of network information than they otherwise would. As a result, analysts can work more efficiently and effectively.

A number of organizations are already leveraging open source tools for NDR and seeing tangible benefits from this approach. Specifically, 28% classify their NDR as built from open source software, while an additional 37% indicate they use a mix of open source and commercially available tools. Those using open source tools have seen both operational and security improvements from their deployments and cite improved SOC analyst efficiency (69%), reduced mean time to detection (58%) and response (45%), lower operational costs (53%), less operational complexity (49%), and, ultimately, fewer data breaches (43%).

Figure 7. Benefits Realized From Open Source NDR



Corelight’s Open NDR Platform

Corelight Open NDR

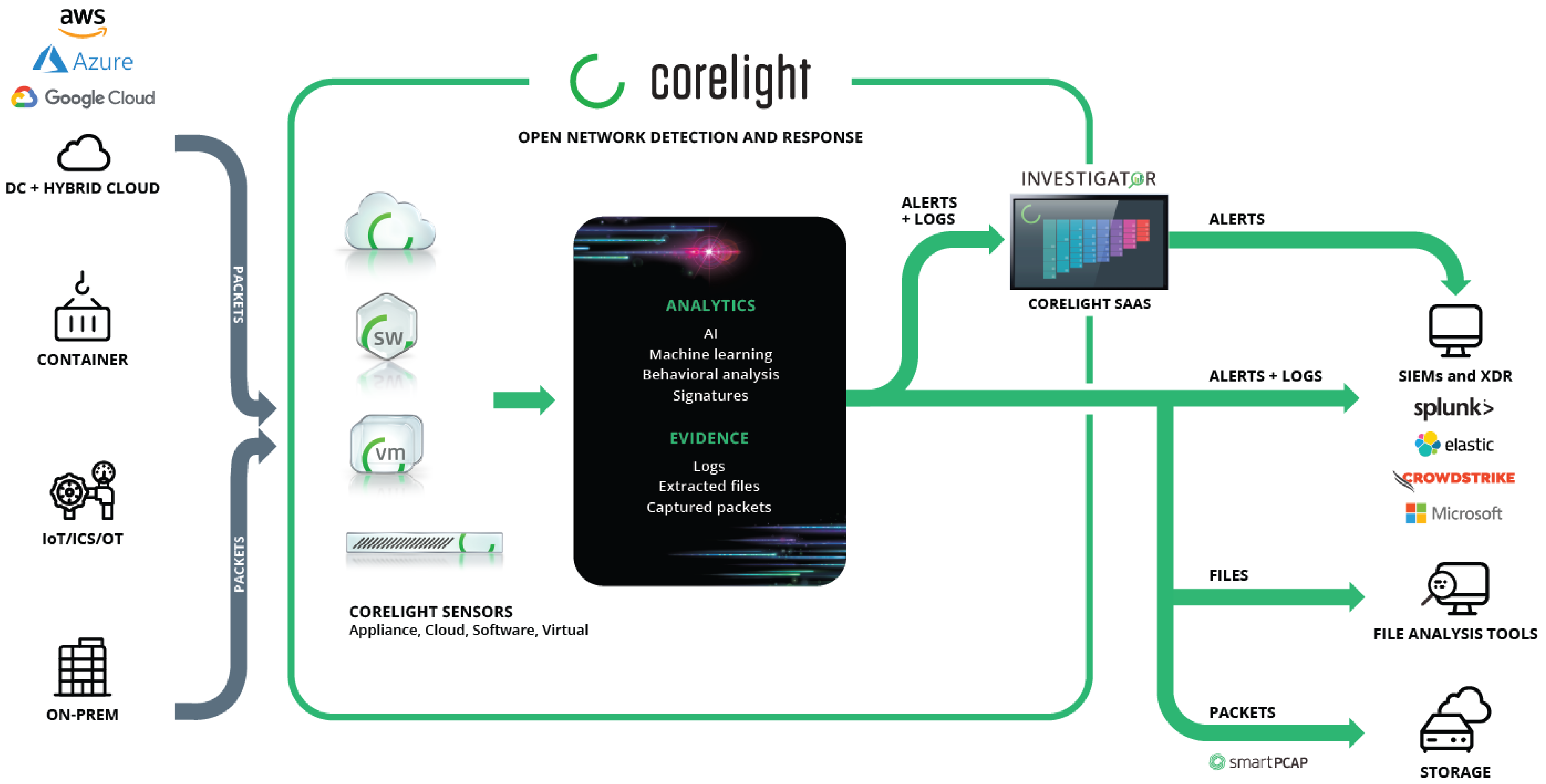
Corelight's Open NDR platform provides comprehensive network visibility across on-prem, hybrid, and multi-cloud environments. It combines the open source network security monitoring tool, Zeek, Suricata IDS, and Corelight's proprietary analytics and Smart PCAP to transform network data into high-fidelity detections and evidence to enable teams to quickly investigate and respond to an event. Corelight Open NDR enables customers to consume rich network data in the manner best for them by enabling export to any SIEM or extended detection and response (XDR) solution and access from any SOC architecture. Its open core, open data, and open platform design delivers the key requirements for open NDR, as previously discussed. Specifically:

- **Open core.** Corelight is the corporate steward of Zeek, which has over 20 years of federally funded research and development, over 10,000 deployments worldwide, and a robust community constantly contributing findings and detections. Zeek analyzes network traffic and runs complex behavioral detections, creating compact, high-fidelity transaction logs in a fully customized output. The Corelight Open NDR platform natively integrates the Suricata IDS engine to broaden detection and provides custom Suricata rules in addition to licensed third-party content to enable customers to run the most relevant rule sets to meet their needs. The combination of these detection methods helps organizations uncover stealthy zero-day threats more effectively.

- **Open data.** The Zeek foundation of Corelight's Open NDR enables organizations to consume the data the platform collects wherever they need, including SIEMs and XDR tools. Because analysts have access to the raw data, they can build their own enrichment rules or leverage those of the broader community. Corelight offers five collections, which are turnkey packages delivering proprietary detections and insights along with curated insights from the Zeek community. Further, the open data standard better supports generative AI applications because they are already public and crawled by the large language model providers, meaning customers don't need to train AI on proprietary vendor data sets.

- **Open platform.** The ability to leverage the wealth of data Corelight collects, where and how security analysts want, cannot be overstated. Organizational needs change over time, and the flexibility to send raw data elsewhere in the stack or leverage curated detections and insights natively in the Corelight console provides investment protection over the long term. Corelight Investigator enables investigations directly in the console.

Figure 8. Corelight Open NDR



Corelight Open NDR Benefits

Through its focus on open core, open data, and open platform, Corelight Open NDR helps organizations improve security effectiveness and efficiency.

Specifically, organizations are able to:

Achieve complete, hybrid cloud visibility.
Corelight's out-of-band sensors parse all network traffic across on-premises, hybrid, or multi-cloud environments, replacing multiple data sources such as Netflow or logs with a single, comprehensive source of telemetry. This reduces blind spots across cloud, shadow IT, and rogue access points; increases confidence in existing controls; and accelerates risk assessments and audits. Additionally, Corelight's encrypted traffic analysis capabilities not only support Zeek's native capabilities, but also extend these with proprietary insights. Corelight provides detections for encrypted threats without decryption, leveraging the observable elements of encrypted connections.

Improve detection coverage and accuracy.
Corelight's powerful combination of open source security capabilities in Zeek and Suricata IDS, with proprietary machine learning, behavioral analysis, on-premises and cloud-specific detections, and signatures augmented by community-developed detection engineering, helps improve both detection coverage and accuracy. This includes increased detection and tactics, techniques, and procedures (TTP) coverage for known attacks, reduced dwell time, and, ultimately, lower risk of reputational and financial loss. Rather than providing just an alert, Corelight offers machine learning detections that are transparent and reveal the feature-level scores of the model so analysts can more easily and quickly validate and triage ML alerts.

Accelerate incident response.
By aggregating rich network data and insights from across the environment, and by supporting analysts with AI-assisted investigation workflows, Corelight helps accelerate incident response. Corelight's AI-accelerated investigation workflows are GPT-explained alerts and next steps for investigations, provided as plain English. Whereas reading rules and understanding IDS alerts typically require technical expertise, by using natural language, Corelight helps analysts more easily understand what the alert is and what steps to take to further investigate or address it. This improves time to case resolution as well as mean time to respond; empowers analysts to accomplish more, reducing the need to engage outside incident response firms; and limits the scope of defensible disclosure via breach notification.

Increase operational efficiency.
Ultimately, the consolidation of NDR, IDS, and PCAP functionality in a single sensor deployment architecture, coupled with the high level of visibility and detections and accelerated incident response, helps improve operational efficiency. Compared to solutions that require separate sensors for different capabilities, scalability is increased, and management overhead and costs are reduced. Additionally, there is no need to retrain or upskill the team to learn cloud-specific threat detection tools. A more efficient and capable SOC then has the ability and bandwidth to innovate rather than simply react. This, in turn, helps minimize data loss and stop future attacks, which improves the confidence in security team abilities and can improve employee retention.

BACK TO CONTENTS

Key Corelight Open NDR Alliance Partners

Integrations with ecosystem partners provides flexibility to leverage the rich data collected by Corelight elsewhere in the stack. Technical partnerships with a variety of vendors ensure security teams don't have to rip and replace tools to derive value from Corelight Open NDR. Some of Corelight's key alliance partners include:

- **Crowdstrike**
  Corelight seamlessly integrates with a range of CrowdStrike products, including CrowdStrike Falcon XDR and CrowdStrike Falcon LogScale, so analysts can view consolidated EDR and NDR alerts and gain context across both attack surfaces for incident response investigations. Corelight also provides NDR solutions for CrowdStrike Services in customer engagements when delivering incident response, compromise assessment, and network security monitoring services.

- **Google/Mandiant**
  As a strategic Google Cloud security partner, Corelight's Open NDR Platform integrates across the Google Cloud Security Operations Suite to deliver a superior level of attack visibility, response, and threat-hunting capabilities. Organizations can use Mandiant Threat Intelligence to enrich Corelight high-fidelity logs and prioritize Suricata alerts that can be consumed into Chronicle and analyzed by its Breach Analytics module for faster, more effective investigations.

- **Microsoft**
  By providing correlated log data from over 50 protocols through passive network monitoring, Corelight provides SIEM analysts using Sentinel a clear picture of all the activity across their global networks. Additionally, the Corelight App for Microsoft Sentinel helps resource-constrained SOC teams simplify deployment and alert triage by ingesting pre-formatted, correlated network evidence directly into Sentinel dashboards and data repositories. This helps provide a holistic view of the environment, including context for device inventory and the ability to quickly respond to alerts to mitigate advanced threats from a single pane of glass.

- **Splunk**
  Corelight data integrates natively into Splunk data models and dashboards to simplify threat detection and response, while Corelight Sensors can use the Splunk Universal Forwarder to optimize data ingestion into the enhanced data models of Splunk Enterprise Security. Additionally, Corelight network evidence can be used to inform Splunk SOAR playbooks, optimizing response activities.

Conclusion

> “The metadata-based approach of Corelight’s Open NDR, coupled with Corelight’s machine learning analytics and the Suricata IDS engine as well as PCAP, **provides a singular repository of every level of network detection and data an analyst could need to investigate and validate alerts.**”

Conclusion

NDR is clearly critical for security programs, especially to round out the SOC visibility triad and efficiently unify threat detection and response across on-premises and cloud environments. However, the specifics matter immensely. Alert fatigue is real, and solutions that do not provide access to the underlying data prevent analysts from fully unpacking the “what” and “how.” An open NDR foundation offers security teams greater flexibility to consume network data natively, through a SIEM, or in an XDR. The metadata-based approach of Corelight’s Open NDR, coupled with Corelight’s machine learning analytics and the Suricata IDS engine as well as PCAP, provides a singular repository of every level of network detection and data an analyst could need to investigate and validate alerts. Further, the community-based foundation of Zeek, coupled with Corelight’s custom detections, puts this data to good use through evidence-based detections of truly malicious activity rather than simple alerting on anomalous behavior. With those using open source NDR already seeing tangible security and operational benefits, security teams exploring NDR should assess Corelight’s OpenNDR and how it can help their SOC teams become more efficient and effective.

corelight

ABOUT

Corelight transforms network and cloud activity into evidence that security teams use to proactively hunt for threats, accelerate response to incidents, gain complete network visibility, and create powerful analytics. Corelight's global customers include Fortune 500 companies, major government agencies, and large universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology. For more information, visit https://corelight.com or follow @corelight_inc.

LEARN MORE

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.