451 Research® | PATHFINDER REPORT

Building a Scalable Budget for Security Analytics with Network Detection and Response

COMMISSIONED BY

ExtraHop

NOVEMBER 2019

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

ERIC HANSELMAN

CHIEF ANALYST

Eric Hanselman is the Chief Analyst at 451 Research. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of networks, virtualization, security and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines. The convergence of forces across the technology landscape is creating tectonic shifts in the industry, including SDN/NFV, hyperconvergence and the Internet of Things (IoT). Eric helps 451 Research's clients navigate these turbulent waters and determine their impacts and how they can best capitalize on them. Eric is also a member of 451 Research's Center of Excellence for Quantum Technologies.

Executive Summary

In the shifting landscape of security capabilities, it can be maddening to plan for investment. Throw in the constantly changing attack vectors that have to be mitigated, and this can seem like an impossible task. In the midst of this chaos, there are paths that can reduce the clutter in the decision-making process and build a foundation for capabilities that are nimble enough to handle whatever the future brings. Organizations have to take an objective assessment of their current posture and evaluate how they can raise their levels of operational maturity. The data to improve situational awareness through better network visibility may already be there, but it will take better tools and integration across hybrid domains, security, networking and operations teams to deliver its full power.

Key Findings

- Effective security capabilities require coordination and integration across teams.
- To get to DevSecOps, there has to be NetOps and SecOps collaboration.
- Organizations need common language to facilitate security decisions, and frameworks like NIST Cybersecurity Framework, CIS Top 20 Controls and MITRE ATT&CK can build solid bases.
- Network perspectives can build reliable sources of truth across hybrid environments.
- The adoption of TLS 1.3 will affect network-based analytics.

Complexities in Analytics

Budgeting for information security is a complex task. Being able to deliver sufficient detection and mitigation while keeping spending from reaching stratospheric levels is no mean feat. There are far too many options when it comes to tools, and the matrix of which tools address what capabilities and where they live is truly daunting. There's a way to consider the options that can help to focus on those aspects that can be of more value to the organizations implementing them.

When organizations consider what will allow them to integrate perspectives across security, operations and applications teams, there are two areas on which they should focus. The first is developing a common language to consider threats, protections and the goals of the business. The second is to establish solid sources of data to understand activity and develop deeper insights into the operation of their environments. This latter is a place where network-based visibility can form a foundation as a source of truth. At the same time, network data is less susceptible to the distortion that can be found in host-based techniques, and can provide faster time to value when a network tap infrastructure is in place.

With these benefits, network visibility has clear advantages, but there are many different implementations in the market with varying levels of capabilities and analytics. In this paper, we explore the various impacts of these differences and look at how enterprises can improve their security posture by putting them to work effectively.

Network Security Maturity

Enterprise security environments are dynamic, working to adapt to an evolving threat landscape. To make informed decisions about improvement, it's necessary to understand the current state of capabilities. As part of its 4SIGHT advisory program, 451 Research has built a maturity model that can be a useful guide in understanding where network security capabilities are today and how they can move forward. There is a progression from basic network monitoring to greater sophistication through network detection and response (NDR). Most organizations have made their way to greater levels of maturity, but that shift hasn't come without some pain.

For example, the move to intrusion detection systems (IDS), in its early phases, was characterized by significant alert density. New levels of visibility were valuable in understanding activity, but the manual task of sorting through the large volume of alerts placed a burden on security teams. Many moved to security information and event management (SIEM) systems to manage the volume of information, but maintenance of those systems to ensure that the perspectives they generated were valid also was a significant burden. Network behavior anomaly detection (NBAD) systems promised to reduce the amount of labor required in operation through a process of learning acceptable behavior. While they made significant progress, NBAD systems often had limited views or constraints in context that made it cumbersome to integrate with other IT management systems.

Each stage in maturity integrates the capabilities of the previous stages and layers on more sophisticated analysis and the ability to build in greater operational context. NDR approaches look to create operational integration across teams and environments to extend information flows. By collecting greater amounts of contextual data, NDR can function as a common platform through which IT teams can gain greater situational awareness and collaborate more effectively. Of course, there is always more that can be done to expand organizational effectiveness and progress, but NDR endeavors to more tightly bind protections and operational visibility directly to business processes.

Figure 1: The stages of enterprise network security environments

Source: 451 Research

	PRE-ENLIGHTENED	EXPERIMENTAL	MATURING	PROGRESSIVE	INTELLIGENT
HISTORIC STAGE	Pre-IDS era	IDS and initial SIEM	NBAD and behavioral analytics	NDR	Post-NDR
PEOPLE	Non-specialists	Nascent specialists, compliance-driven	Security operations with greater context	Integrated security, IT, cloud and networking operations	Applying intelligence to tackling business problems

	PRE-ENLIGHTENED	EXPERIMENTAL	MATURING	PROGRESSIVE	INTELLIGENT
PROCESS	Reactive	Beginning proactive stance; cautious network blocking	Higher-level analysis of activity, with trends and anomalies	Integrating operations for incident response and remediation; proactive tactics in use	Tight integration of teams and effective automation, reducing human intervention
TECHNOLOGY	Manual review	Initial investments in tools and automation	NBAD begins to optimize, and sufficient data exists for robust forensics	Machine learning benefits from greater data and can help automate investigation steps	Automated responses to detection and mitigation, guided by business logic
STRATEGY	Developing best practices	Meeting compliance requirements and developing triage capabilities	Opportunistic identification of anomalies for major use cases	Effective prioritization of responses	Blended responsibility for security across teams

Many enterprises have made it to the maturing stage. Operational security requirements and a need for greater staff effectiveness have been strong drivers, but their security teams often operate independently from other IT teams. Because of that separation, enterprises are missing an opportunity to take advantage of the benefits that linking the efforts of the full set of IT staff can bring. When an organization's IT teams can agree on labeling for assets, risks and remediation actions, the overall security posture improves, issues are addressed more rapidly, and errors are minimized.

To move forward, organizations need to invest wisely to create capabilities that will encourage teams to work across traditional boundaries. They need to ensure that there is analytic capability to lift the work required out of the doldrums of manual assessment and correlation. Prudent choices can take the visibility provided by network insights and turn it into a means to fuel operational change. NDR approaches can be the foundation to make this kind of transformation happen.

Technical Capabilities and Benefits

Many of the difficulties that organizations face in their information security environments come from teams operating in silos and the gaps in coverage that result. A natural effect of organizational growth, whether organic or inorganic (although the latter can be more problematic), is that more tools and systems are continually put in place for specific situations and for the use of just one team. Asset management systems for on-premises systems may not be extensible to new hosted or cloud providers. Log analyzers may only support certain classes of operating systems or applications. Endpoint protection may cover workstations, but not mobile or IoT devices. And for each of these classes of products, security and IT teams may be using different tools. All of this leads to a proliferation of tools, with none having a complete or shared picture of an organization's situation. Many organizations are turning to network visibility as the means to bridge those gaps and provide a more complete picture.

One of the important aspects of NDR systems is that network visibility completes the security picture in ways that are difficult for other approaches to address. The network is the means of moving information and, as a common medium, provides unique insight into an organization. It's also uniquely extensible to new environments, applications and devices. It provides a source for analytics that can more effectively correlate across the expanding world that enterprise infrastructure has become.

That benefit hasn't gone unnoticed in the marketplace, and the number of network-based security suppliers is growing. NDR requires capital investments for high-performance network monitoring sensors, cloud-based analytic datacenters, and marketing to educate decision-makers on the benefits of the approach. All of this makes entry into the market more complex; nevertheless, the opportunity is attracting new entrants and causing others to extend functionality to address portions of this need.

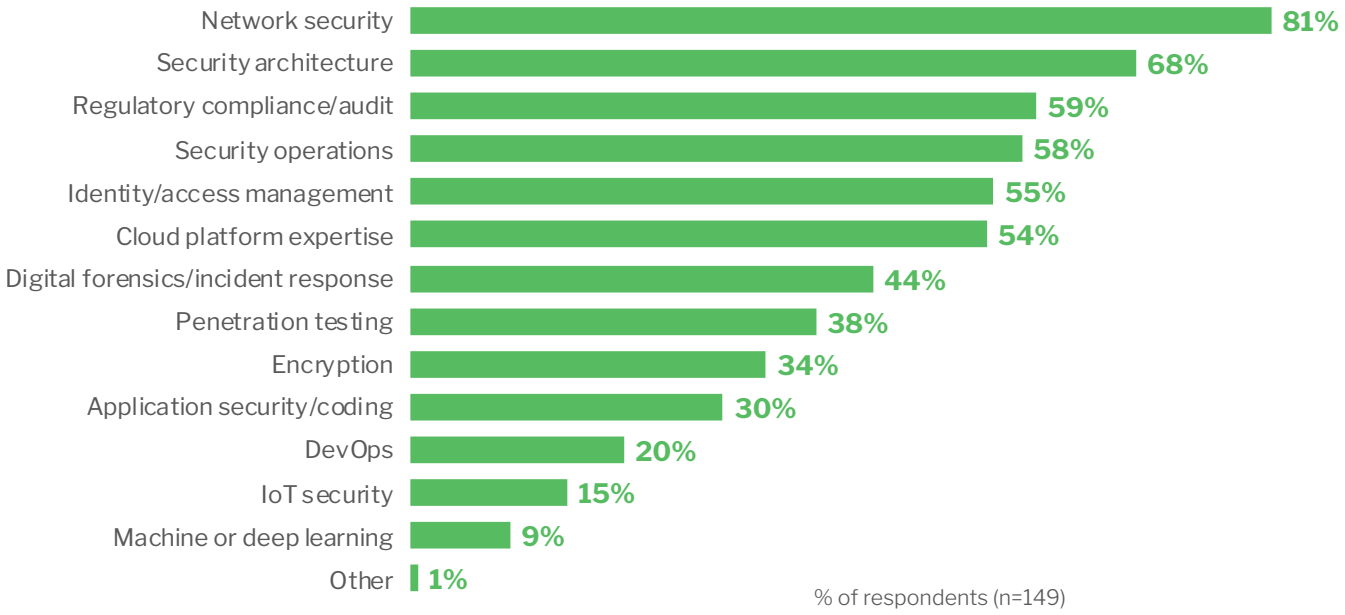
The growth in vendors has made it more difficult for organizations to identify offerings that will be the most effective in their environments. To differentiate among them, it can be useful to consider what has driven the return to network visibility as a valuable choice. The proliferation of physical locations in enterprises requires that NDR systems not only be able to handle the various location types (on-premises, colocation, hosted, cloud), but that they be able to scale to meet the volume of activity and entities that they will manage. That demands an architecture that is built to handle scale and diverse deployment needs.

A more subtle but just as important part of NDR systems is their ability to deliver on the needs of multiple IT teams. The financial reality of most organizations is that they can't support multiple toolsets and maintain budgets. Effective NDR systems will give organizations the ability to deliver perspectives to operations and security teams, with the added benefit of having them working from the same data, giving a common source of truth in identifying issues. This can lead to more effective operational integration, speeding fixes and reducing operational errors. Making teams more efficient can deal with one of the most persistent problems in IT – shortage of skilled staff.

Addressing the Skills Gap

Figure 2: Network security is the most desired skill set for security operations

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2019
Q: Which of the following skill sets are most important for security professionals to have today? Please select all that apply.



The network not only remains a primary source of security insight, but it is also the most sought-after skill among enterprise security teams. Eighty-one percent of respondents to 451 Research's Voice of the Enterprise (VotE): Information Security, Organizational Dynamics 2019 study identified network security as the most important skill set for security professionals, ahead of security architecture (68%), regulatory compliance/audit (59%) and operations (58%). Technology refresh is a significant driver in NVDR evaluation and adoption, with intrusion detection and prevention systems among the top targets.

Changes in Technology

Along with operational and infrastructure transitions, there are technology changes that are impacting the effectiveness of some security strategies. The evolution of application technologies to include greater levels of encryption for network data has been identified and addressed by many, but the greater prevalence of perfect forward secrecy (PFS) and the use of ephemeral keys mean that organizations have to consider how well any NDR system can support them. Legacy network visibility approaches have depended on the availability of static server keys and have architectures that depend on them, but PFS breaks this model. PFS is already in use in major application environments, driven by an awareness of the extent to which it's possible to abuse techniques that use longer lifetime keys. The news has been full of reports of the ease of breaking these older methods and the impacts of that vulnerability. Security analysts and application owners have moved aggressively to implement PFS in a range of applications because its use has been mandated in the TLS 1.3 specification. To maintain deep-level visibility,

NDR systems have to be able to address the more sophisticated techniques that are required to decrypt PFS traffic at high volumes and to securely manage the data that's derived. Without the ability to inspect payload, NDR systems have less detailed data to run through their machine learning algorithms and other detection techniques.

Frameworks for Alignment and Evaluation

Detection is the top requirement for NDR, but trusting vendor claims about the efficacy of their machine learning capabilities is a leap of faith for most security analysts. To address this, organizations should adopt a common vocabulary that they can use to describe what needs to be done and what a tool or procedure will accomplish. For example, organizations can align NDR findings and functionality to recognized efforts such as the MITRE ATT&CK framework, the Center for Internet Security (CIS) Top 20 Controls, or the National Institute of Standards and Technology (NIST) Cybersecurity Framework. ATT&CK offers detailed appeal to practitioners, while the CIS Controls will appeal to decision-makers and NIST for industry-specific prospects. NIST is frequently referenced at the executive level for its easy-to-understand five major categories (Identify, Protect, Detect, Respond, Recover). ATT&CK, meanwhile, has gained attention with operational teams for the framework it offers for systematically characterizing attack attributes and detail, with the goal in view of automating more machine-readable threat activity data and helping to alleviate complex security monitoring and response challenges.

The benefit of using frameworks is that they define terms and concepts objectively and allow teams to better understand roles and responsibilities. With this base, responsibilities can be delegated clearly and can be better understood. There are critical points of alignment for NDR with different frameworks, and understanding them can facilitate their use.

CIS CONTROLS

It can be useful to organizations that are working to assess their security posture to prioritize the steps needed to improve their situation. The CIS Top 20 controls are broken down into three groups: basic, foundational and organizational. An effective NDR implementation has a role to play in each and can be particularly important in addressing the first steps in completing the basic and foundational group actions.

- **Control 1 – Inventory and control of hardware assets:** The visibility that NDR provides can aid enterprises in understanding what's connected to their networks and what those devices are doing. It can enhance asset management systems by identifying devices that might have escaped normal provisioning processes.
- **Control 4 – Controlled use of administrative privileges:** Understanding context around connections to assets is critical to qualifying access events, and NDR provides the depth of information to better understand how they should be identified.
- **Control 9 – Limitation and control of network ports, protocols and services:** Being able to track network activity not only allows the understanding of current state but can also validate that controls are functioning as intended.

The CIS framework can be used in conjunction with other frameworks to create a plan of action that prioritizes next steps for implementation.

NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework is a comprehensive set of activities coupled with a risk identification and alignment methodology. Its five-element core activity structure (the Identify, Protect, Detect, Respond, Recover mentioned above) can provide clarity in setting roles for security activities. The capabilities of mature NDR systems can map to each of the NIST core activities. An important part of the NIST framework is that it offers a model, through its implementation tiers, for organizations to identify their expectations of business risk and appropriate levels of investment and integration to address them. This can be effective in performing gap analyses between current and desired states. The volume of the framework can be daunting, but it provides a useful mapping of high-level concepts to specific standards and recommendations (such as CIS, COBIT, ISO and NIST) that can aid organizations in better understanding the technical details of action classes.

MITRE ATT&CK

Understanding the nature of threats is a critical part of planning defenses, and the MITRE ATT&CK framework lays out a matrix of attack tactics and techniques to provide structure and a common vocabulary to them. Each element is defined with a tactic, technique or procedure (TTP) and organized by phase of action or effect. The ATT&CK framework can help organizations tie protections that they implement to specific attacks and evaluate the impacts. MITRE also defines a set of mitigations and aligns the mitigations with the TTPs that they address. The capabilities that NDR systems bring to an organization can be directly tied to many of the mitigations. The framework is a tool that organizations can leverage to understand how to integrate complementary technologies that are being deployed. For example, understanding what endpoint protection functionality requires network-based backup to be more effective.

Use Cases

There are a number of use cases that can illustrate the ideas presented above. Each identifies some of the key values that NDR can offer and how they're achieved.

BRINGING NETWORKING AND SECURITY TOGETHER

An area where effective NDR deployments can have significant impact is integrating operations across teams. Historically, security operations and network operations teams have operated independently, even though they are focused on the same network. Network teams were keeping it running, and security teams were keeping it safe. That often led to misalignment and sometimes even duplication of effort. If there wasn't a common source for the identification of assets and activity, there could be confusion and problems in prioritizing activity.

TEAM CHALLENGES	NDR BENEFIT
Misaligned information and asset data	Common base of information
Duplicated identification and remediation tasks	Alignment of workflows
Multiple analytics regions	Unified data for analytics
Independent tools	Common tool chain

APPROACHES TO HYBRID SECURITY

Most organizations are operating in multiple execution venues today. Whether cloud and on-premises or colocation, the dispersed nature of modern infrastructure requires the ability to operate effectively in any venue and be able to add new ones with a minimum of effort and disruption. While many cloud providers offer some level of operational analytics, they're not aligned with on-premises systems, which typically leads to isolated islands of data that are difficult to correlate.

HYBRID CHALLENGES	NDR BENEFIT
Different on- and off-premises toolsets	Unified toolset and capabilities
Onboarding learning curve	Common tools reduce onboarding effort
Multiple analytics regions	Unified data for analytics
Separate operational domains	Shared tool environment unites teams

MAINTAINING VISIBILITY WITH ENCRYPTION

Expanding security awareness and concerns have moved most organizations to greater use of encryption in the applications that they build and their network communications. Managing network visibility with encryption has often been labor-intensive and complicated, typically caused by the need to manage keys and the supporting infrastructure for passive monitoring. It's become mandatory to be able to decrypt traffic because attackers have become adept at using encryption to cloak their activities.

ENCRYPTION CHALLENGES	NDR BENEFIT
Static key use declining	PFS-capable decryption expands visibility
Attackers cloaking traffic	Capable decryption exposes attacks
Decryption impacts application performance	Scalable tap-style decryption doesn't impact performance
Integration with endpoint and network protection	API integration capabilities

Conclusions

Organizations face many challenges in securing their IT infrastructure. The combination of complex environments, constrained budgets and a shifting threat environment make it difficult to settle spending priorities. The visibility that network-based approaches present and the capabilities that effective NDR deployments can yield build a strong case for their use. A capable NDR system can serve the needs of operational and security teams. It can facilitate the creation of SecOps processes by being a single source of truth that integrated teams can put to work, and it can offer a common language that can make team interactions more efficient. Having a common operation platform brings information together to fuel better analytical performance. It can also unite operational teams that address different parts of hybrid environments by offering a common set of tools to address infrastructure in different forms and locations. The ability to increase operational efficiency by bringing teams together and the gains that powerful analytics can deliver can give security spending its greatest impact.

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
Chrysler Building
405 Lexington Avenue,
9th Floor
New York, NY 10174
+1 212 505 3030

SAN FRANCISCO
505 Montgomery Street,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®