ExtraHop

Public Sector Edition

WHY THE TIME IS RIGHT

For Network and Security Collaboration

eBOOK

Table of Contents

Introduction

The transition to a more distributed workforce and the acceleration of cloud adoption as a result of the pandemic have placed additional strain on already strapped network operations (NetOps) and cyber protection (SecOps) teams. Fragmented tools and environments make every incident and troubleshooting effort consume more time and energy than your teams have to spare.

When the SolarWinds SUNBURST attack hit in late 2020, thrusting advanced threats in the spotlight, it became even more clear that any friction in the detection and investigation flow would delay a response.

The time is now for truly collaborative NetSecOps. This ebook will explore:

- How current circumstances have introduced new friction and challenges into SecOps, Net Ops, and incident response
- How increasing collaboration and data and tool sharing between these teams can improve each team's separate outcomes, as well as the shared mission objectives
- How to take the first steps toward greater NetSecOps collaboration or fortify your existing processes for better outcomes

What is NetSecOps?

We believe it is a commitment to collaborate rather than a transition to an official team called “NetSecOps” on the org chart. For the purposes of this eBook, NetSecOps is the collaboration between the Network, Cybersecurity and Cloud teams to reduce the friction that can delay a response to either a security incident or an application outage—which potentially risks the institutional mission or causes monetary damage. Whether you merge network and security teams completely, or just commit to greater collaboration and shared network data sources and tooling, a NetSecOps approach can yield major operational and organizational benefits.

How Remote Work Impacts Network and Cyber Operations

More than half (53%) of Public Sector IT leaders have had their priorities impacted by the pandemic and transitioning to remote workforces.

Almost overnight, public sector institutions and operations were decentralized by work-from-home (WFH) mandates, flinging assets, data, and people all over the country. VPN usage and remote access tools ballooned to accommodate new connections from anywhere. With this newly distributed access came an abundance of unknown, unmanaged devices that were connecting to organizational resources. As staff and contractors used personal devices for both work and home lives, visibility decreased and the potential window for attackers to compromise those devices increased exponentially.

88% of respondents rely on VPN tunneling for their work.	How are VPN tunnels secured at scale?
30% rely on RDP, a protocol notorious for being abused by attackers.	How do you assure RDP sessions are legitimate and used securely?
Only 13% of respondents indicated that their organization fully manages webcams in their environment.	How do you ensure that sensitive, connected devices (IoT) in workers' homes aren't a vector for stealthy attackers?

Shadow IT has only grown more pervasive during the pandemic.

The fundamental connective tissue between distributed workforces and the resources they need to do their jobs well is the network. These shifts toward permanently decentralized workforces and organizations make it all the more important to be closely monitoring network traffic, both to understand user experience and to detect, investigate, and respond to security threats.

71% of IT departments reporting that every week, they were finding IT assets they didn't know of in their inventories.

Accelerating Cloud Migration

Supporting this newly altered reality for many public sector organizations meant accelerating their migration to the cloud, and expanded organizations' digital presence far beyond the internal network, exposing the weaknesses of siloed IT and disparate toolsets. While cloud technology, or cloud migration, has been a major initiative or on the horizon for many organizations over the years, the fast decision making required for daily operations forced security considerations onto the backburner.

Over 90% of federal, state, and local agencies have already moved at least some of their systems and solutions to the cloud.

Even at pre-pandemic speed, cloud migrations tend to have unintended consequences for both cyber and network operations, not to mention unforeseen costs. In April of 2020, still comparatively early in the pandemic, Microsoft CEO Satya Nadella said at a quarterly earnings report: "We've seen two years of digital transformation in two months."

Assuring that workloads newly migrated to the cloud are still secure and performant is a challenge many organizations were already facing. Feeling pressure to hurry the process along only to support mission objectives increases the chance of misconfigurations or security degradations resulting from a rushed cloud migration.

How can network data be the key to cloud migration and security?

Over the past several years, all the major public cloud providers (AWS, GCP, and Microsoft Azure) have either released or announced virtual traffic mirroring in their environments, opening up access to raw packet streams for monitoring and analysis. They did this because they acknowledge network data's criticality for security and operational use cases. Cloud workloads spin up and down on demand. Applications are fragmented, containerized, and amalgamated from microservices. Workloads are split across cloud and on-premises environments, yielding complex, hybrid environments. Agent-based monitoring solutions, and even the built-in offerings from the CSPs, have a hard time maintaining an unbroken view of what is happening.

But the network is always on, and if you're watching it, you've got the most complete, ground-truth view of what's happening in your organization.

A September 2020 survey found that nearly half of organizations (48%) had accelerated their cloud migration as well as their overall IT modernization initiatives due to pressures caused by the pandemic.

Advanced Threats, Supply Chain Attacks, and Ballooning Attack Surfaces

According to the 2020 Verizon Data Breach Incident Report, **over a quarter of breaches still take months to be discovered.** This dwell time translates directly to more profits for attackers and more damage to breached institutions. Advanced threat actors have time and patience to wait without being detected until they can execute their mission.

SolarWinds SUNBURST backdoor was in action for nearly a year, possibly more by some estimates, before it was widely reported.

Another 2020 survey found a 430% increase in "next-generation" supply chain attacks using targeting Open Source Software (OSS) as the vector for transmitting malicious code.

Organizations that assume they will be compromised, are in a better position to respond quickly to prevent catastrophic damage. That response requires network and security teams to work in unison to detect threats before they breach the network.

SolarWinds SUNBURST provides motivation to invest in fast, efficient incident response capabilities, which ultimately requires collaboration between NetOps and SecOps.

What's Different in This New Era? A Razor Thin Margin for Error

The unfavorable reality is that IT teams are siloed—functioning as separate entities and only collaborating when necessary. Years ago, network operations and cybersecurity needs were handled by a singular IT Operations team. As infrastructures grew in complexity, organizations splintered the groups into specialized NetOps, SecOps, and now CloudOps teams. This change bred inefficiencies—security, network, database, cloud, and application teams now use different tools, access different data, and don't communicate effectively.

"No matter how much technology is used, and no matter how well-documented security processes and playbooks are, security teamwork is needed to work across the business to avoid vulnerabilities, to quickly react to new threats and to develop new techniques and processes."

- SANS Analyst Report: Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs)

Visibility, Access, and Accountability Are The Keys to NetSecOps

War rooms, as time-honored as they may be, are a stale paradigm for incident response, whether the incident is security or performance-centric. When operations teams are siloed and speak a "different language" (read: use different processes and data sources), performance and operational challenges can lead to unhelpful finger pointing, and delayed responses. An adversarial mood may arise between teams, further complicating the incident or downtime resolution.

The success of NetSecOps depends on mutual accountability. If everyone speaks the same language and uses the same format, it becomes much easier to identify root cause and fix the issue rather than playing hot potato.

The technical foundation of successful NetSecOps is built on two things:

Broad, deep visibility into what is happening in the IT environment
Access to this visibility for members of every team that may potentially be involved in a war room or incident response activity.

All network communications and activity—benign or malicious— cross the network. Network data provides the connective tissue for NetSecOps collaboration, enabling each team to resolve their own issues more quickly and independently, while accelerating and reducing friction in truly collaborative actions such as incident response.

Closing The Gap: Why Network Data Holds The Key

NetSecOps benefits from sharing data sources, increased visibility, and improved workflows, that provides the resources to collaborate more efficiently across infrastructure, network management & monitoring, and incident response.

The most successful collaboration happens when both NetOps and SecOps have access to the same broad, deep visibility into activity throughout the entire environment, rather than relying on ad hoc processes and data sources that must be manually gathered and correlated before a clear picture can emerge. Benefits of this include:

- Improved network and end-user performance
- Visibility over an expanding and permeable environment (cloud, applications, and network)
- Shortened remediation times and reduced reactive troubleshooting
- Faster mean time to detection (MTTD) and risk reduction
- Lower operational costs
- Skills gap coverage

Benefits like these are only achievable if NetSecOps has full visibility through the cloud, to ensure security and network performance are effectively managed. And sharing a toolset that facilitates real-time access to packet-level data in on-premises, cloud, and hybrid environments.

Minimize spending on technologies with overlapping functionality

Simplify technology adoption

Reduce mean time to resolution (MTTR)

Automate routine activities to overcome staffing gaps

Achieving the Results of Network Data Sharing

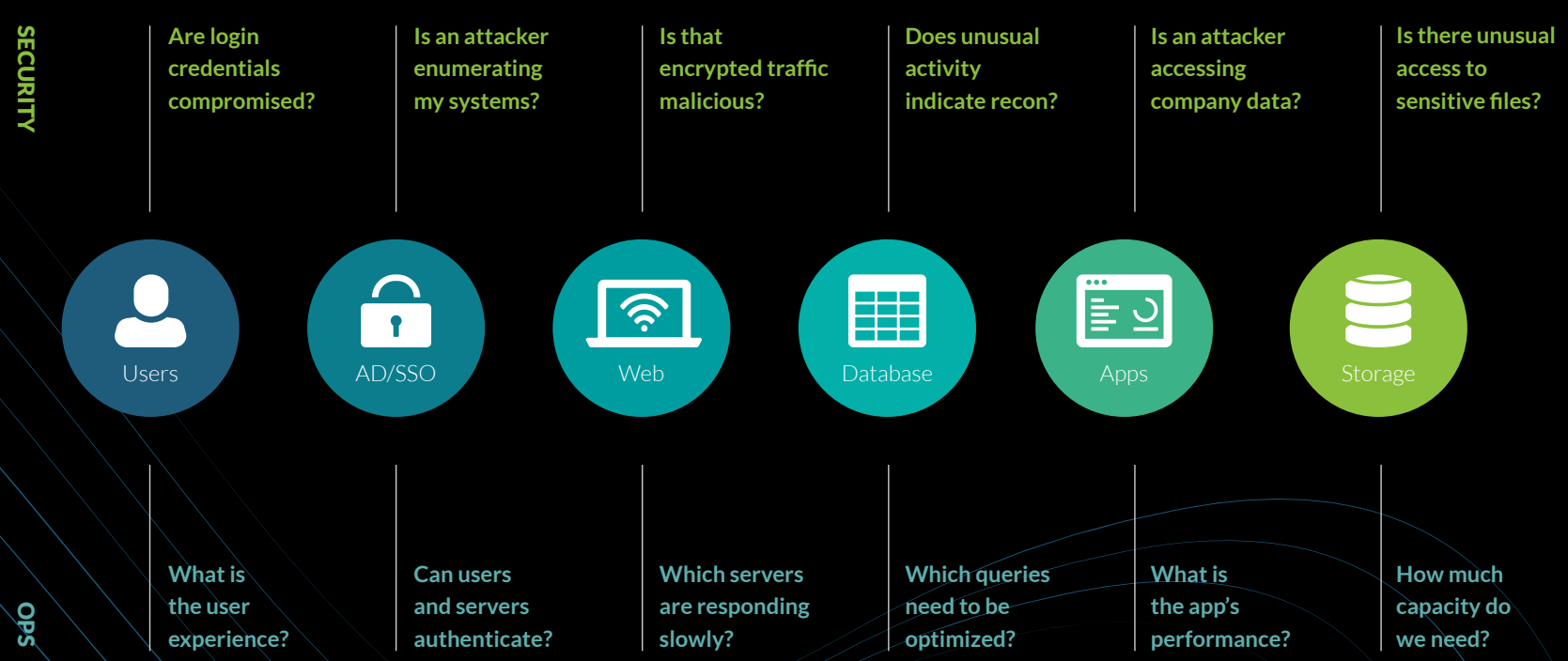
With network data as the fundamental data source fueling security and IT operations team and requirements, organizations are able to:

- Accelerate incident response and reduce attack dwell time
- Manage and monitor cloud applications to catch misconfigurations and assure secure, performant deployments across cloud, on premises, and remote environments
- Create real organizational change that feeds future innovation

Research has shown that collaboration between NetOps and SecOps teams can result in 37% reduction in risk and 31% increase in responsiveness to changes in the business, which is exactly what organizations need in the face of the uncertainties facing them in 2021 and beyond.

You don't need to merge NetOps and SecOps on the org chart or do a big organizational overhaul to reap the benefits of NetSecOps. The teams just need to share data, tools, and a mindset a little more than they might right now. IT leaders and organizations have an opportunity to up the ante to deliver a fast and secure user experience while enabling institutional agility.

Questions Network Data Can Answer for Security and Network Operations Teams



Making NetSecOps a Reality with ExtraHop Reveal(x)

1. Examine all the tools you have that are separately capturing packets, analyzing separate areas of the network, detecting CVEs, or enabling forensics based on network observation, and think about how much money and effort you could save if those capabilities were consolidated into a single tool.

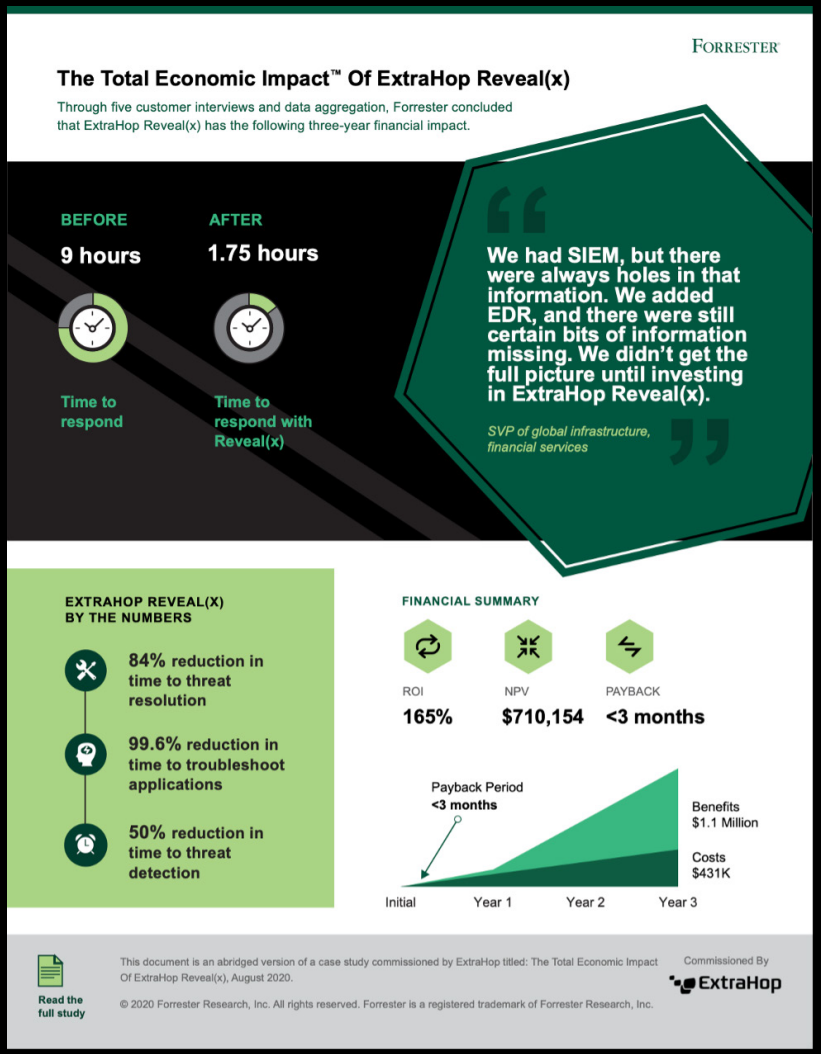
2. Give every security and operational team access to fully analyzed network data, the foundational data source for both security operations and network operations.

3. Assure that each person or team who would potentially be called on for a war room or incident response action is able to fluently navigate and interpret analyzed network traffic and identify the relevant traffic to investigate an incident.

4. Reap the rewards of faster incident response.

5. If the above steps made sense to you, check out the free online demo of Reveal(x) and see what your NetOps and SecOps teams have been missing out on.

START DEMO



About ExtraHop Networks

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

info@extrahop.com
www.extrahop.com