Enterprise Strategy Group by TechTarget

SHOWCASE

OCTOBER 2024

The Infoblox Ecosystem: Powerful Integrations To Simplify NetOps and SecOps in Hybrid, Multi-Cloud Environments

John Grady, Principal Analyst

Abstract: Fragmentation across the numerous security and network tools and processes enterprises have in place today has increased complexity, created gaps in visibility, limited efficiency, and reduced security efficacy. Technical partnerships that provide integrations across a variety of tools and vendors can help both network and security teams improve efficiency and effectiveness by breaking down these silos. The Infoblox Ecosystem offers this by utilizing certified prebuilt integrations across leading technology partners, providing more comprehensive visibility, automation of manual tasks, more efficient investigations, and, ultimately, a stronger security posture.

Security and Network Teams Struggle to Overcome Disjointed Tools and Processes

Enterprise environments continue to become more distributed and complex. The continued migration to the cloud and adoption of IoT means IT teams have to connect and secure more devices and locations than ever before, and do so with a variety of siloed tools. Collecting and distributing the data required to maintain visibility, efficiently configure infrastructure, and effectively investigate and respond to incidents is incredibly difficult with these silos in place.

Cybersecurity in particular is top of mind for nearly all organizations. Threat actors have more resources at their disposal than ever to compromise enterprise systems and access sensitive data. Successful, high-profile attacks have highlighted how significant the business impacts from such events can be. These factors have raised cybersecurity to an executive- and board-level issue. Yet, for all this focus, many organizations continue to struggle with cybersecurity, especially when it comes to security operations.

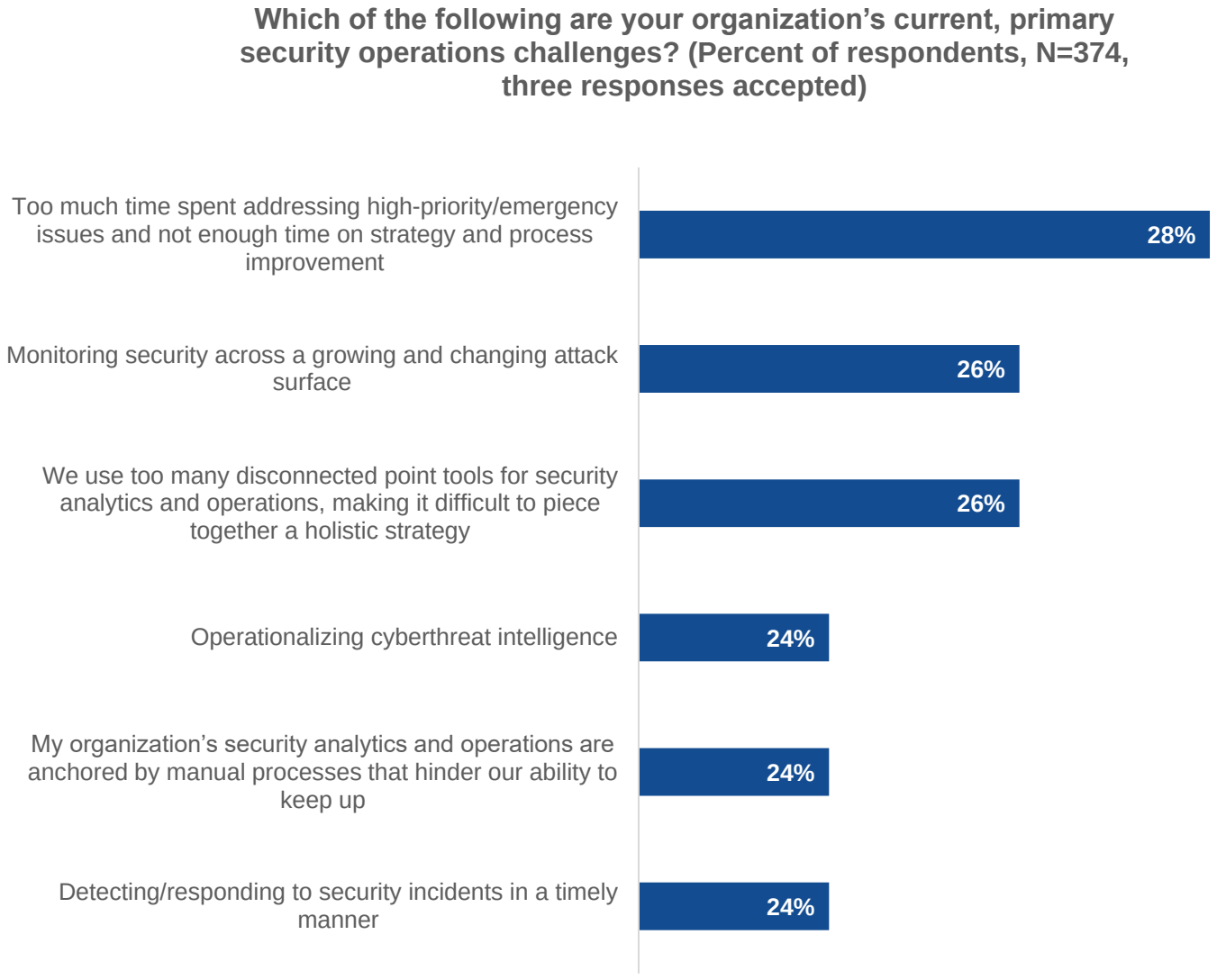
Research from TechTarget's Enterprise Strategy Group has identified the top challenges organizations cited with regard to security operations (see Figure 1).[1] These can also be viewed as a proxy for network operations challenges and loosely grouped as issues around efficiency and effectiveness:

- **Lack of efficiency.** Organizations indicated that their dependence on manual processes, capacity to respond to incidents in a timely manner, and ability to spend enough time on strategy and process improvements were all challenges. The inability to efficiently manage security operations and respond to incidents leads to a cycle of reaction rather than proactive improvement. The dependence on manual processes and lack of automation is relevant on the network side as well. NetOps teams must support cloud and developer teams that want to deploy infrastructure and applications as quickly as possible, but they are often forced to choose between moving quickly without all the information they need or manually aggregating the data they need, which takes time and slows the process down. There are also costs associated with these challenges, as operations teams are forced to spend cycles trying to stitch together views from disjointed tools.

[1] Source: Enterprise Strategy Group Complete Survey Results, *2024 XDR and SOC Modernization Trends*, May 2024.

- **Difficulty remaining effective.** On the effectiveness side, respondents pointed to the use of too many disconnected point tools, difficulty monitoring security across a growing attack surface, and struggle to operationalize cyberthreat intelligence. In fact, 37% of respondents indicated that they use at least 26 tools for security operations.[2] Attackers do not think in silos; rather, they leverage multivector attacks to compromise target organizations. As enterprise environments have become more complex and distributed, attackers have learned to use this to their advantage. Siloed network and security tools make it difficult to tie indicators together across the attack surface and effectively detect and respond to threats. Jumping from tool to tool and console to console to identify malicious activity, determine the extent of the incident, and begin to implement network policies to quarantine the attack takes too much time and gives attackers a greater chance to locate and exfiltrate sensitive data.

Figure 1. Top Security Operations Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[2] Ibid.

Vendors Should Take the Lead on Ensuring Networking and Security Tools Work Together Across Providers

The general solution to these issues is better integration across both security and networking tools. On the cybersecurity side, in particular, there is strong agreement on this fact, with Enterprise Strategy Group research finding that 84% agreed that a cybersecurity product's integration capability is an important consideration of the security product procurement criteria.[3] The more robust these integrations are, the easier it is for organizations to effectively apply a defense-in-depth cybersecurity approach to their environment.

But while nearly all organizations prefer stronger integrations, there are differing approaches on how to achieve that. One strategy is consolidation through the shift toward platforms. While this can help simplify some processes, there are downsides as well. Standardizing on a single or reduced number of vendors can increase risk when things do go wrong. There is no backup when attacks occur that bypass that vendor's detections. The chance for catastrophic outages is higher with a single point of failure. There is also the likelihood that, while some of a platform's capabilities will be best-of-breed, others will be simply good enough.

The alternative is technology alliances that provide prebuilt integrations between different vendors' tools. This type of approach helps IT teams break down the silos between tools, while still enabling them to choose different solutions that best meet their needs and address their priority use cases. Technology alliances can help security and network teams improve efficiency by automating manual tasks, especially around data aggregation and sharing. This can lower operational costs and help analysts focus on more proactive and strategic activities. Further, these integrations often lead to better effectiveness. The data and telemetry shared between tools can improve efficacy, limiting the number of unnecessary alerts and false positives, as well as aid in investigations, reducing mean time to detection and mean time to response.

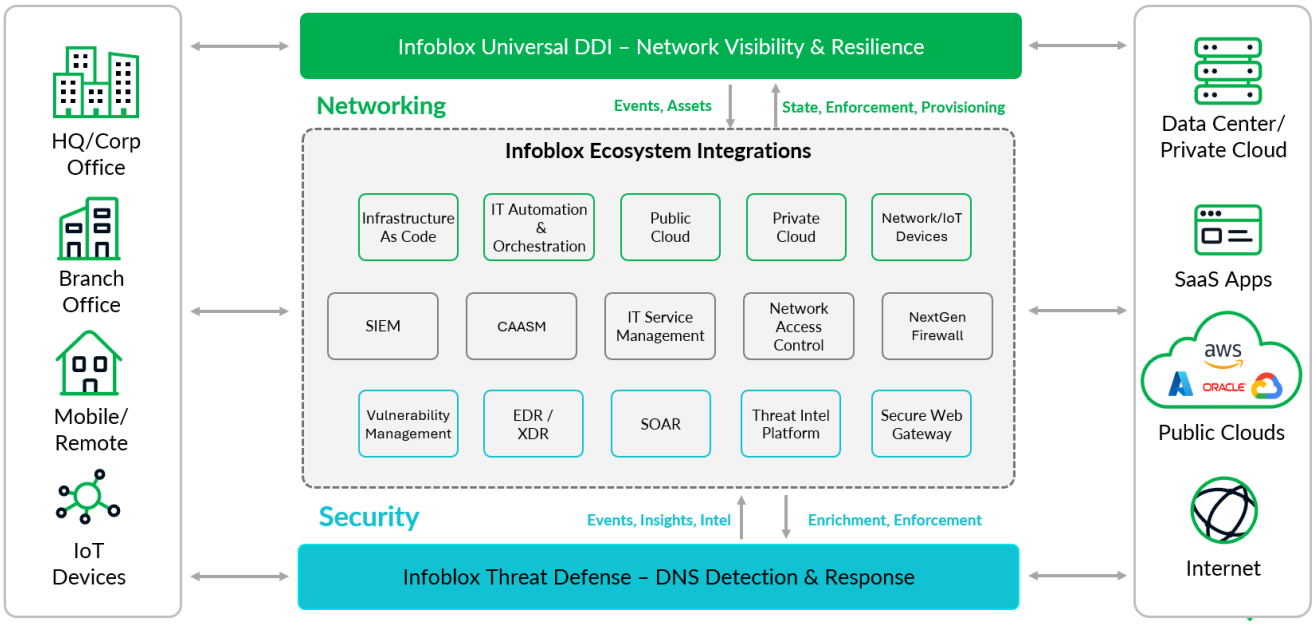
How Infoblox Ecosystem Helps Network and Security Teams Streamline Operations and Strengthen Security

Infoblox is well known as a leading provider of Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM) solutions—the combination of which is known as DDI—to enable robust network infrastructures that extend into hybrid, multi-cloud networking. Over the years, the company has expanded into security through its Infoblox Threat Defense offering that leverages DNS to detect and block a wide variety of attacks, including malware, phishing, ransomware, and other modern tactics.

The Infoblox Ecosystem Program is focused on enabling seamless integration with security and network partner solutions, enhancing visibility, automation, and threat intelligence sharing to improve operational efficiency and strengthen security across enterprise networks. The idea of technical partnerships is not new, but two aspects stand out in Infoblox's approach. The Infoblox Ecosystem features a broad range of integrations across different categories of IT and security tools (see Figure 2). The Infoblox Ecosystem Portal features numerous prebuilt, certified integrations at launch with leading technology partners like Microsoft, Splunk, Terraform, and many more. The comprehensive certification and support process ensures high-quality, effective integrations. Infoblox not only builds these integrations, but provides direct support, issue handling, and escalations to partner development teams when necessary.

[3] Source: Enterprise Strategy Group Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

Figure 2. Infoblox Ecosystem Architecture



Source: Infoblox

The advantages of this approach are better visibility and predictability, as well as enhanced investigations. Infoblox is uniquely positioned to see network activities and threats ahead of other networking and security tools by using DNS. This visibility gives customers predictability over what comes onto the network. Further, the authoritative IP information, contextual device information, and DNS threat intelligence Infoblox collects provides actionable network insights. Through the ecosystem, this visibility can be shared with other tools such as vulnerability management, security information and event management (SIEM), firewalls, etc. The ecosystem integration of Infoblox SOC insights with SIEM systems delivers curated alerts, minimizing data ingestion, reducing costs, alleviating alert fatigue for SecOps teams, and helping them complete investigations faster. In fact, a recent report from Enterprise Strategy Group validated through custom research and interviews with Infoblox customers that Infoblox networking and security products could help teams achieve a 79% reduction in operational costs, with one customer able to recognize a 70% reduction in time spent on incident management.[4]

Key Use Cases Organizations Can Support With the Infoblox Ecosystem

Infoblox is constantly building its Ecosystem and expanding its partnerships to address new use cases. Among the current use cases the Infoblox Ecosystem supports, four stand out in particular:

- **Vulnerability management.** While these tools are invaluable to identify vulnerabilities across the environment, there are drawbacks. They often lack a comprehensive view of all the assets on the network, run scans on a fixed schedule that could be as infrequent as weekly or monthly, and don't directly address vulnerability remediation. Through integrations with vulnerability management tools from vendors such as Tenable, Qualys, and Rapid7, Infoblox can help provide accurate asset discovery by identifying devices as soon as they join the network. The DNS visibility of Infoblox can help identify potential threats targeting devices earlier, helping security teams more accurately focus their vulnerability scans through selective scanning, and respond to potential threats more effectively. Finally, when critical vulnerabilities or threats are detected, security teams can immediately isolate compromised devices.

[4] Source: Enterprise Strategy Group Economic Validation, *Analyzing the Economic Benefits of Infoblox Networking and Security Management in a Multi-cloud Environment*, March 2024.

- **SIEM.** Two of the most common challenges with SIEM are cost and complexity. SIEMs have the ability to consume a massive amount of data, but the storage required to do that is expensive. Further, this model can result in data and alert overload and fatigue, which leads to diminishing returns. Infoblox addresses these challenges by only sending high-fidelity, actionable alerts to SIEMs such as Microsoft Sentinel, Splunk, and IBM QRadar, reducing the volume of data and alerts. The contextual network data Infoblox provides includes the IP address, DHCP fingerprint, and more, which helps security teams move through the investigative process faster.
- **Multi-cloud.** Multi-cloud strategies help organizations increase resilience and take advantage of different cloud service provider (CSP) core competencies. However, using CSP tools only increases tool sprawl and complexity. Infoblox integrates with all major CSPs including AWS, Azure, Google, and OCI, providing an integrated solution to help organizations achieve greater automation, a single DNS naming convention, and visibility across on-premises and cloud networks. By automating at the DDI layer once and distributing across all clouds, security and IT teams save time and resources.
- **Infrastructure as code (IaC).** IaC platforms help IT teams navigate the more dynamic nature of cloud by automating infrastructure provisioning. The lack of visibility into IP address usage and availability, coupled with the manual management of DNS provisioning, can counteract the benefits of IaC. The Infoblox Provider Plug-In for IaC platforms such as HashiCorp Terraform, and Ansible enables IT teams to allocate IP addresses and DNS records for endpoints and services as part of IaC deployments. When an endpoint or service is no longer needed and deprovisioned from the cloud platform, the Infoblox Provider will automatically remove the IP address or DNS record, ensuring things are always up to date.

Conclusion

Digital transformation and cloud migration initiatives are being prioritized because they can help the business become more agile and better succeed in the market. Yet network and security resources are finite, and many teams struggle to keep pace with the rate of change common in today's enterprise. Even still, they cannot be perceived as slowing the business down, so they must find ways to improve their level of efficiency. This pressure is compounded with global regulations that emphasize DNS data in cybersecurity. Australia's Security of Critical Infrastructure Act, Europe's NIS2 Directive, and the U.S. Executive Order 14028 all require stronger network visibility, including monitoring of DNS traffic, to protect critical infrastructure. These regulations highlight DNS as a key component in defending against cyber threats.

While some attempt to power through by stitching together the different tools in their environment, the better approach is selecting providers that understand the broader problems their customers face and seek to help address use cases outside their core areas of focus through technical partnerships with a variety of technology vendors. Through its certified prebuilt integrations across leading technology providers, the Infoblox Ecosystem helps organizations improve the efficiency and effectiveness of both their security and network operations teams.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com