

Supercharge Your Vulnerability Management Approach with Infoblox



Table of Contents

Why Read This?	03
The Reality of Cybersecurity Today	04
The Visibility and Context Gap	05
Same Security Ecosystem, Whole New Ball Game: Supercharging Vulnerability Management through Integration.....	06
01 Identify, prioritize and remediate vulnerabilities fast, wherever and however they arise	
02 Reduce security ecosystem complexity and ease management of vulnerabilities and threats across hybrid or multi-cloud environments	
03 Improve your security posture and amplify the ROI of your current security ecosystem	
Customer Stories	10
Infoblox: Making Invisible Risks Visible and Actionable.....	11





Why Read This?

Today's IT environments are complex with the rapid growth of cloud services, IoT devices and hybrid infrastructures. This complexity creates fragmented and dynamic networks that are challenging to manage and secure. Organizations face numerous challenges in managing vulnerabilities, which can leave them open to undetected vulnerabilities and increased security risks. Adopting the same strategies as in the past or purchasing yet more security tools is not going to deliver the outcomes needed. Maintaining comprehensive visibility and context is more critical than ever.

USD 4.44M

The global average cost of a data breach in 2025.

1 in 5

Number of organizations that suffered a breach due to security incidents involving shadow AI.

USD 1.9M

The average cost savings for organizations that used security AI and automation extensively in prevention versus those that did not.

Source: IBM Cost of a Data Breach Report 2025

In this e-book, we will show you how Infoblox uses DNS to supercharge your vulnerability management by providing real-time, actionable insights and integrating seamlessly with your existing security ecosystem. Discover how Infoblox improves asset discovery, leverages preemptive and predictive threat intelligence to strengthen threat protection and reduces costs, enabling more efficient security management and a stronger overall security posture.



The Reality of Cybersecurity Today

It is complicated—and getting more so.

Technology environments have undergone extensive transformation and digitalization over the past decade. Adoption of cloud, containers, virtualization, the explosion in devices thanks to IoT, the flood of data, the rise of hybrid working and applications at the edge are just a few of these seismic changes. And cybersecurity has had to constantly shift, evolve and scale to try and keep pace.

Clear IT environment perimeters have evaporated. The attack surface available to bad actors has expanded exponentially and AI-generated attacks are giving adversaries an unfair advantage, making more organizations “patient zero” before traditional tools can react. The risk of falling victim to ransomware, data loss or theft, or of critical IT systems being taken out of action, are also very real and growing. And that is before we get into any financial penalties or reputational damage you may incur from a security incident, or the cost of your business insurance.

Cybersecurity Snapshot

- 26,447 vulnerabilities were disclosed in 2023, **25%** of which were immediately targeted for exploitation.¹
- 95% of organizations surveyed experienced a cloud-related breach with **92%** reporting exposure of sensitive data.²
- **107%** year-over-year rise in IoT malware attacks.³
- **59%** of organizations were hit by ransomware.⁴
- **61%** of hackers plan to use generative AI for hacking tools and to find more vulnerabilities.⁵

However, the issue is not a lack of well-designed, highly effective security platforms, solutions and tools that can combat these challenges head on. Which begs the question: “What are we all missing?”

¹ 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is, Abbasi, Saeed, Qualys, May 14, 2025.

<https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one>

² IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs, IBM, July 24, 2023.

<https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs>

³ SonicWall 2024 Mid-Year Cyber Threat Report: IoT Madness, PowerShell Problems and More, Riddles, Jordan, SonicWall, 2024.

<https://www.sonicwall.com/blog/sonicwall-2024-mid-year-cyber-threat-report-iot-madness-powershell-problems-and-more>

⁴ The State of Ransomware 2024, Adam, Sally, Sophos, April 30, 2024. <https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/>

⁵ Hacker-Powered Security Report 2025: The Rise of the Bionic Hacker, HackerOne, 2025. <https://www.hackerone.com/report/hacker-powered-security>



The Visibility and Context Gap

What you do not know, can hurt you. Cybersecurity solutions have been designed to fulfill specific security functions, and the majority do that very well. But what cybersecurity solutions cannot “see,” they cannot monitor, scan, report on, remediate or block. As IT environments have become more complex, the blind spots have become a lot bigger.

It is like doing an obstacle course blindfolded, with no idea how big or small the course is or what the obstacles are. It is inevitable that at some point you are going to miss something and trip up.

Today, visibility into what is happening across your IT environment—when and what is affected—has greatly reduced due to the growing complexity of modern infrastructures. The shift to cloud, combined with hybrid environments and a myriad of interconnected systems, has introduced layers of complexity that make it increasingly difficult to monitor and manage your IT landscape effectively.

There is also less contextual data, which makes it very challenging for security solutions and security teams to understand, assess and prioritize vulnerabilities. Is this a “shut that device down and remediate now” issue, or a “schedule it for some time this month” task? When context is limited, SecOps teams must manually gather data across systems, which slows down investigation and delays remediation. This increases the risk of a critical vulnerability being missed or not resolved in time.

The mean time to remediate (MTTR) a critical severity web application vulnerability is 35 days. Internet-facing host/cloud-critical severity vulnerability MTTR is 61 days.⁶

Greater adoption of cloud, increased use of virtualization and containers, and more complex networks mean your environment is broader but also more fluid. This adds to your visibility challenges, making it hard to assess when and how often to scan for vulnerabilities. **Continuous scanning can consume significant network bandwidth and resources. But a “scan on schedule” approach means anything that happens between scans may be missed,** whether it is visible to your vulnerability management solution or not.

Vulnerability management solutions identify, assess and report on vulnerable assets to help IT teams prioritize remediation. But how can you take your protection a step further to stay ahead of sophisticated attacks and preemptively reduce your risk profile?

That is where Infoblox comes in with Protective DNS and predictive intelligence to spot risky infrastructure before attacks land.

⁶ 2024 Vulnerability Statistics Report (9th Edition), Edgescan, 2024. <https://www.edgescan.com/wp-content/uploads/2025/04/2024-Vulnerability-Statistics-Report.pdf>

Same Security Ecosystem, Whole New Ball Game: Supercharging Vulnerability Management through Integration

What if rather than replace your perfectly functional vulnerability management solution, you could turbocharge its capabilities and add preemptive protection by giving it the end-to-end, multi-cloud visibility and early indicators of attacker activity it has been missing? By leveraging the foundation of how your IT environments fundamentally operate—DNS, DHCP and IP address management—Infoblox does just that, turning previously invisible risk into actionable signals.

Quick Glossary Guide

- **DNS:** The Domain Name System is the address system and database. Without it, no device, service or resource can connect to the internet or a private network. Nor can any other devices and networks be located without DNS.
- **DHCP:** A Dynamic Host Configuration Protocol server automatically assigns IP addresses, default gateways and other network parameters to devices. Without these a device or service cannot connect to or function on a network.
- **IPAM:** IP address management ensures the administration of DNS and DHCP is centralized, streamlined and automated. This enables efficient allocation, tracking and management of IP resources across complex networks.

Anything that wants to use or connect to your infrastructure must engage with these critical functions to be able to do so. The servers on which these services reside therefore have visibility and data on every single thing that happens on your infrastructure, every function and device, and can serve up that data to any vulnerability management solution seamlessly. Thanks to a high degree of ecosystem integration and an expansive range of APIs, suddenly the invisible is made visible—and actionable in three critical ways, discussed next.





Identify, prioritize and remediate vulnerabilities fast, wherever and however they arise

Stay operational and secure as threats, vulnerabilities and your infrastructure evolve with smarter, more effective cybersecurity using the platforms and tools you already have today. Infoblox unifies and simplifies network security management, reducing risk by giving on-premises, hybrid and cloud visibility across vulnerability management platforms, including IoT devices, the OT environment and more. No more gaps in visibility, no more limitations on reach for optimal protection, without increasing cost.

A Tolly Group test shows Infoblox's platform **“outperforms other DNS security solutions by detecting a fuller range of threats more accurately.”⁷**

Infoblox does not replace the security ecosystem, but improves visibility and contextual network data across your entire IT environment. This removes any gaps in visibility and adds layers of protection by closing the door on connections of concern, preventing unauthorized access to your networks and systems.

Infoblox provides contextual real-time insights into all devices accessing the network into your vulnerability management platform, enabling real-time, end-to-end, total visibility. This integration of Infoblox and your vulnerability management platform massively enhances selective scanning capabilities, reduces risk and helps minimize costs while supercharging the security solutions you have in place today.

All of this can help you activate a reduction in insurance premiums, and reassure investors and stakeholders with accurate Common Vulnerability Scoring System (CVSS) scores that demonstrate a reduced risk posture.

Infoblox together with vulnerability management gives you:

- Real-time scanning and accurate identification of assets
- More visibility of assets with contextual device information
- Location tracing of assets with extensible attributes
- Reduction of false positives, backed by highly accurate DNS-based intelligence that filters out noise
- Protection from malicious and suspicious DNS activity by blocking risky domains and infrastructure before users, devices or workloads are impacted
- Vulnerability management solution alerts to scan suspect hosts
- Automatic isolation of infected hosts when leveraged with network access control (NAC), quarantining them until remediated

⁷ Infoblox's BloxOne Threat Defense Outperforms the Competition in DNS Security (Press Release), Infoblox, February 1, 2022. <https://www.infoblox.com/news/news-events/press-releases/infobloxs-bloxone-threat-defense-outperforms-the-competition-in-dns-security/>

02

Reduce security ecosystem complexity and ease management of vulnerabilities and threats across hybrid or multi-cloud environments

Infoblox offers the industry's most comprehensive hybrid, multi-cloud DNS, DHCP and IPAM solution, enabling you to supercharge security tools like vulnerability management by embedding preemptive, DNS-layer security. This proactive approach allows you to go from being the hunted to the hunter by using DNS-level insight to shut down attacker infrastructure before it can be weaponized. It offers fast, seamless integration with your current ecosystem and unifies network and security visibility and management, giving you greater protection and cost-effectiveness.

Get clarity through visibility and context related to everything happening on your infrastructure, including vulnerabilities arising in your hybrid or multi-cloud environments for true end-to-end security coverage. This minimizes any risk to business continuity and reduces mean time to detect (MTTD) and MTTR to lessen the business impact of any vulnerabilities.

Infoblox simplifies migrations and streamlines hybrid cloud operations, centralizes DNS management, automates provisioning, strengthens security and unifies asset visibility. Infoblox allows you to scale quickly, whether it is adding new domains, platforms, networks or devices as your demands increase. This is all done with reduced administration and the simplified and automated management of network security.

Infoblox together with your vulnerability management platform provide you with your digital fingerprint so you can:

- Centralize control over DNS, DHCP and IPAM to simplify management and ensure comprehensive visibility across multi-cloud environments.
- Ensure accurate asset tracking and correlation of network activity by leveraging DNS, DHCP and IPAM data.
- Enhance incident response by quickly identifying network activity sources tied to security events.
- Improve threat detection and response using actionable insights tied to network identity and infrastructure.
- Speed up vulnerability detection and remediation with seamless automation and real-time data from Infoblox.
- Increase accuracy in identifying vulnerable assets and associated risks with integrated network services data.



03

Improve your security posture and amplify the ROI of your current security ecosystem

Infoblox can provide a return on investment (ROI) of 243 percent over three years, while paying for itself in less than six months, according to a Forrester Total Economic Impact Study.⁸

Infoblox enhances operational efficiency, delivering cost and time savings across all integrations. Customers leveraging Infoblox and ecosystem integrations have reported significant improvements in several key areas:

- **Improved operational efficiency**, including a remarkable 70 percent time reduction through automation of manual tasks.
- **Reduced investigation time** such as expedited breach investigations with a 67 percent decrease in time spent.
- **Streamlined, reduced inventory collection time** by over 90 percent.
- **Significantly lower operational costs** (79 percent) through improved operational efficiency.

With better, more accurate data, vulnerability management and other security solutions and tools gain the required visibility and information in real time to then maximize ROI across your ecosystem. Our platform can run on-premises, across hybrid and multi-cloud, as part of a ready unified solution.

More detailed reporting and real-time scanning can help reduce both risk and the number of scans required, and therefore the cost where a “pay by scan” model is in place. It aids compliance and further reduces vulnerability by maintaining network integrity and regulatory adherence, and offers unique DNS-based threat intelligence to provide insight into weaknesses and how to improve security behavior.

And, as the leading providers of DNS, DHCP and IPAM, you may already be an Infoblox customer, meaning you will not even have to purchase our platform.

Infoblox together with vulnerability management enables:

- **Continuous Asset Discovery:** Real-time updates on new and existing devices ensure an accurate, up-to-date asset inventory for comprehensive visibility.
- **Selective Scanning:** Contextual asset information helps prioritize high-risk assets, optimizing resource usage and reducing licensing costs.
- **Preemptive Threat Detection:** DNS-based threat intelligence and AI/ML analytics predict and identify risky domains and attacker infrastructure before they're confirmed as malicious, complementing vulnerability management with earlier, more decisive responses.

⁸ Forrester Study: The Total Economic Impact™ Of Infoblox DDI, Forrester, October 2023.
<https://info.infoblox.com/resources-analyst-reports-2023-the-total-economic-impact-of-infoblox-ddi>

Customer Stories



Large North American Bank

From low visibility and compliance concerns to almost 100 percent scanning coverage and regulatory reporting.

The bank required vulnerability scanning to comply with stringent regulations, but it took eight hours to scan only 60 percent of the network. By optimizing their security ecosystem, Infoblox enabled scan on demand, which now scans all people and devices as they connect, minimizing risk and shutting the door on security incidents before they arise.



Global Energy and Automation Solutions Company

From high risk and high premiums to saving \$1.2 million in cyber-insurance fees in three years.

This organization had a poor cybersecurity risk score leading to a high cost of insurance. Bringing in Infoblox improved their rating within months from intermediate to advanced, and propelled them into the top percentile in both vertical and national ratings for cybersecurity risk score.



Infoblox: Making Invisible Risks Visible and Actionable

Infoblox makes the invisible visible in real time, using DNS-first visibility and Protective DNS to surface risky activity and then sharing that context with all major cybersecurity solutions to amplify your security ecosystem.

The only unified DNS, DHCP, IP address management (DDI) plus preemptive, DNS-layer threat protection solution available.

Other vendors offer IPAM, some promise DNS-based security. Only Infoblox delivers unified DNS, DHCP and IPAM, with predictive threat intelligence and DNS-layer protection in one, while supercharging your current cybersecurity ecosystem with contextual insights and data on everything that happens on your network and cloud platforms.



Hybrid and Multi-Cloud Focus

Infoblox accelerates cloud migration and ensures reliable, secure IT services in hybrid, multi-cloud environments. **Over 165 new features** enhance management, visibility, deployment and security.⁹ Our platform is the world's first 100 percent cloud-native critical network and security services architecture.



Designed from the Network Up

Infoblox unifies critical network services, simplifying complex networking, with cloud-managed DDI that streamlines DNS, DHCP and IPAM. Offering seamless data management, it is simple to scale as you add new domains, platforms or networks.



Advanced Security Features

Infoblox integrates preemptive threat intelligence and DNS-layer security. It proactively disrupts threats by leveraging AI-driven analytics that track how adversaries build and use infrastructure, enabling earlier detection of malicious domains with exceptionally low false-positive rates. It is the only protective DDI platform that can provide contextual insights (from DHCP) to identify threats by individual user or device versus IP address, supporting real-time mitigation of threat/security events.

Infoblox platforms can be integrated quickly and simply with all major security vendor, network automation and cloud solutions, including Tenable, Qualys and Rapid7, for vulnerability management through 80 integrations and over 120 APIs. Today, we already help protect and enable more than 13,000 customers worldwide, including 75 percent of Fortune 500 companies.

⁹ 165 Reasons to Choose Infoblox: A Year of Innovation in Network and Security Solutions for the Modern Enterprise, Gupta, Mukesh, Infoblox, May 17, 2024. <https://blogs.infoblox.com/company/165-reasons-to-choose-infoblox-a-year-of-innovation-in-network-and-security-solutions-for-the-modern-enterprise/>



Supercharge Your Security Ecosystem Today



A New Approach Is Key

The sheer volume of live vulnerabilities and threats is unlikely to reduce anytime soon. Organizations must innovate to protect their data, systems and people from bad actors and the threats they unleash.



See Everything

You cannot defend against what you cannot see. Without visibility, your security ecosystem is blind to threats.



Contextual Information Adds Value

Understanding and acting on detected threats is essential. Context helps reduce investigation time by providing critical detail.



Supercharge Your Security

Infoblox provides the comprehensive solution you need to enhance visibility and context. It boosts the effectiveness of your existing security solutions and seamlessly integrates new platforms and solutions you may adopt in the future.

Looking to supercharge your vulnerability management?

Contact your Infoblox representative to discover how we can protect your business and get started today.



Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

