USE CASE BRIEF | SECURITY

infoblox

Preempt Ransomware and Other Advanced Threats

Reduce Breach Risk with Proactive Protection and Mitigation

IMPACT SUMMARY

Keeps Businesses Ahead of Attackers: Uses predictive intelligence to stop threats before they land on networks, unlike traditional tools that detect and respond to threats after a patient zero infection.

Blocks DNS-Based Exfiltration: Protects data internally and externally by blocking DNS-based exfiltration missed by firewalls and SASE.

Safeguards Continuity: Prevents ransomware before it disrupts operations, protecting customer trust and avoiding costly downtime.

Strengthens Board-Level Confidence: Provides clear visibility and metrics that demonstrate threats blocked before they impact the organization.

82% of threats blocked before the first query

5X more high-/medium-risk domains blocked preemptively

0.0002% false positive rate

68.4 days of protection delivered on average before an attack

INTRODUCTION

Cybercrime is rising fast, with global costs expected to hit $23 trillion by 2027.[1] Breaches like ransomware continue to succeed, highlighting critical gaps in current approaches.

One major reason? The attackers have evolved. Threat actors are increasingly using AI to launch more prolific, sophisticated and stealthy campaigns. AI accelerates the development of malicious code, reducing the time required to create sophisticated ransomware that can evade traditional detect and respond security measures. This capability lowers the barrier for entry, enabling less experienced hackers to deploy effective ransomware attacks.

CHALLENGE

The technology that has enabled unprecedented connectivity and innovation has also created vast attack surfaces, which threat actors exploit with increasing speed and sophistication. As organizations become more dependent on digital infrastructure, the stakes continue to rise—making modern, proactive cybersecurity imperative for organizational survival.

The Accelerated Ransomware Epidemic

According to Forbes, ransomware attacks surged by 132 percent in the first quarter of 2025 compared to the last quarter of 2024,[2] aided by AI deception-based social engineering to gain initial access to networks.

The ITRC Annual Data Breach Report found that there are as many as 11 victims of malware attacks per second worldwide.[3] This translates to 340 million victims annually, which will continue to grow exponentially as AI-driven malware attacks become more prevalent. In another recent report, 87 percent of surveyed security professionals indicated that their organizations have already experienced AI-driven cyberattacks.

Phishing's Role in Ransomware

Phishing emails are the source of 41 percent of ransomware attacks. When a user clicks a malicious link in a phishing email, malware is downloaded and executed on their device. Once inside the organization's network, the ransomware initiates its attack by using command-and-control (C2) communications to retrieve an encryption key. The ransomware then encrypts files on the infected system.

After encryption, users are each presented with a ransom request from the attacker. As the attack unfolds, the ransomware may also exfiltrate sensitive data. Attackers often use this stolen data to pressure victims into paying the ransom—threatening to leak the information if demands are not met.

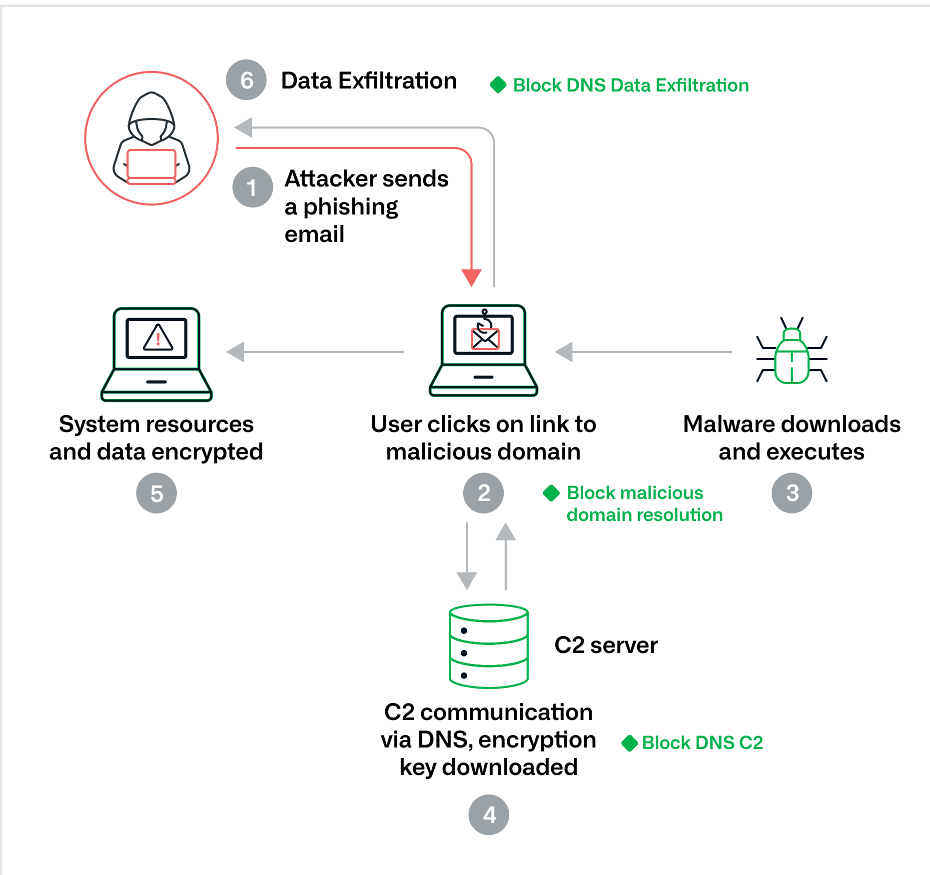

Figure 1. The typical ransomware lifecycle, beginning with a phishing email

Traditional "Detect and Respond" Approaches Fall Short

Ransomware and other sophisticated attacks such as data exfiltration/infiltration and domain generation algorithms DGAs/registered DGAs (RDGAs) are constantly evolving. Malware families are discovered annually and new variants detected daily. Threat actors are generating uniquely crafted, single-use malware that renders traditional, reactive tools—those waiting for a "patient zero" infection—ineffective. Every attack turns into a "patient zero" scenario—where no signature or known behavior exists to detect it.

Most security tools are reactive and focus on detecting and responding to threats after they have already been activated. This approach is insufficient to protect against threats. The average threat actor breakout time (how long it takes to spread after landing on a network) is a speedy 48 minutes. This means that organizations have a very short window to detect, investigate and remediate an attack before it spreads further within the network. This challenge exists for commonly used security tools such as next-generation firewalls (NGFWs), secure access service edge (SASE), endpoint detection and response (EDR) and network detection and response (NDR), which cannot catch the threat before it impacts the network.

SOLUTION

The market is looking for new innovative ways to counter AI-driven and sophisticated attacks, and is moving toward a more preemptive solution—one that stops threats before they enter the environment or move laterally. This approach not only blocks attacks earlier but also reduces the load on traditional “detect and respond” tools.

Protective DNS: Stopping Ransomware Before It Starts

Infoblox places DNS at the core of protecting an organization’s entire infrastructure—on-premises, in the cloud, across remote users and within IoT/OT—against advanced and AI-driven threats like ransomware, data exfiltration, C2 and DGAs.

Protective DNS safeguards businesses before impact with:

- Predictive, original and hunted threat intelligence that blocks threat actor infrastructure before it is weaponized
- Algorithmic/ML-based analysis of DNS queries in each network
- Detection of DNS tunneling for exfiltration

Organizations can now proactively stop connections to malicious and high-risk domains before any attack is launched, keeping harmful and unwanted traffic off the network.

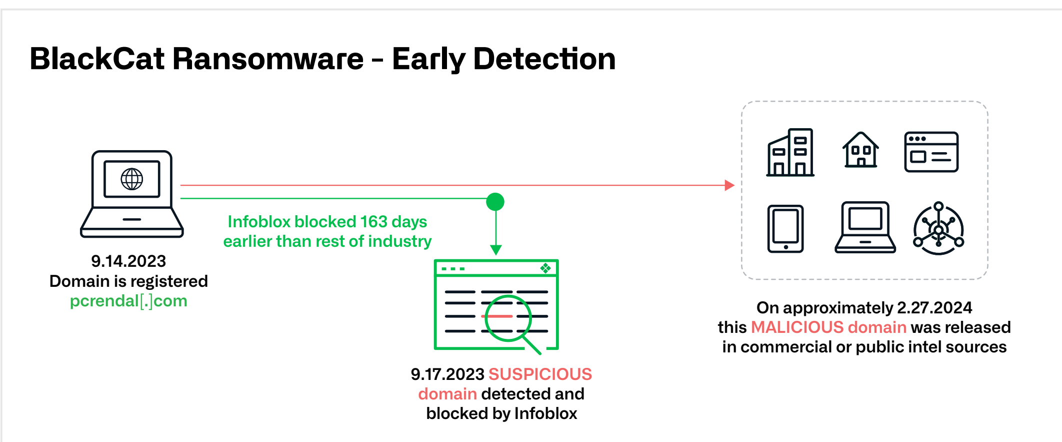

Figure 2. BlackCat Ransomware’s domain blocked by Infoblox 163 days before commercial and public intel sources

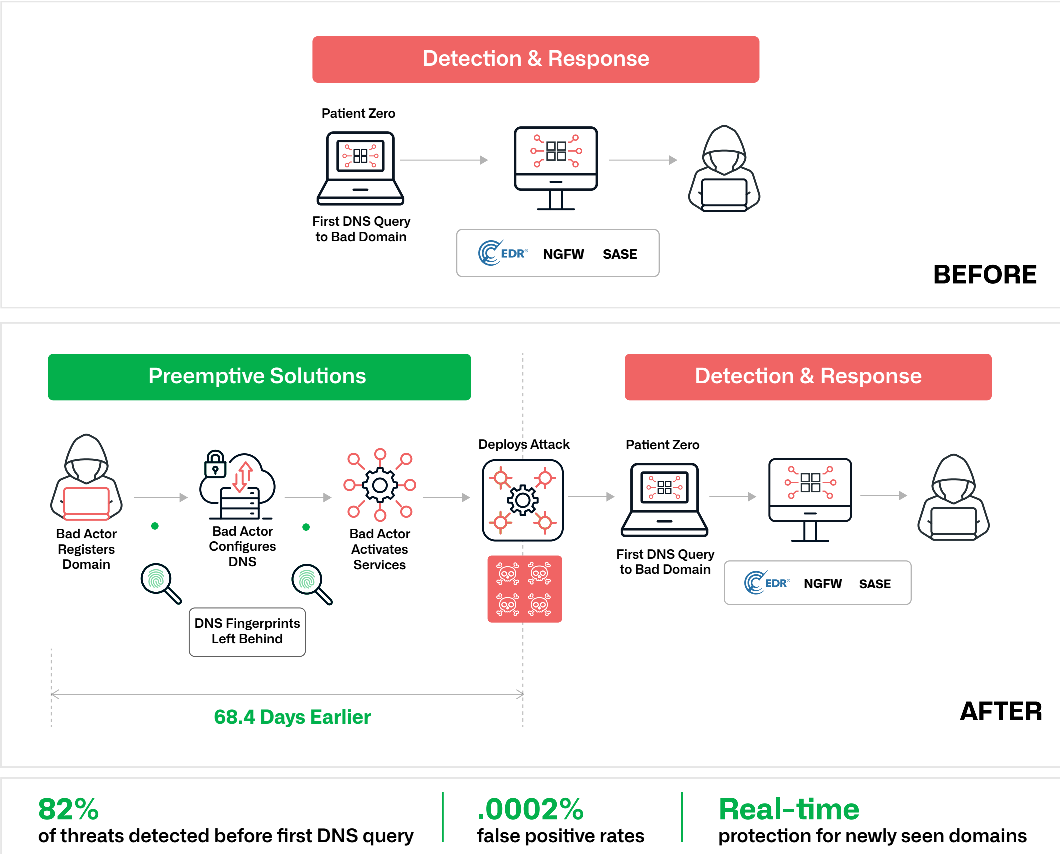

Figure 3. Traditional solutions versus Infoblox

Visibility: Offering Insights—and Reducing Risks—across Complex Environments

To lower the likelihood of lateral spread and potential impact, Infoblox provides rapid identification of assets involved in security incidents.

Organizations achieve this cross-domain visibility using Infoblox's automated near-real-time discovery to uncover all networks and assets across their complex hybrid and multi-cloud environments, including those with diverse devices (i.e., IoT and OT).

When enterprises can see what was safeguarded by Protective DNS, they gain:

- Faster investigation into threats
- Enhanced ability to track malicious activity back to a specific user, device or cloud workload
- Clear communication about the potential business impacts that were avoided

A Unified Point of Control: Simplifying Protection and Performance

With Infoblox, organizations get the benefit of a single control point that leverages existing infrastructure and protects at the earliest stage of the chain, prior to compromise. Rather than struggling with fragmented security tools, they can use DNS to secure their entire infrastructure—on-premises, cloud workloads, remote users, and IoT/OT devices—from sophisticated and modern attacks.

This unique, DNS-based approach delivers:

- Unified protection with consistent policies across IoT/OT, workloads and endpoints DNS-layer blocking, which decreases traffic on routers and firewalls—and lowers costs
- Agentless access for employees, devices, IoT and other infrastructure elements
- Reduction of 50 percent in the number of alerts generated by other security tools, lowering operational costs and letting SOC teams focus on alerts that matter

HOW INFOBLOX CAN HELP PREEMPT RANSOMWARE AND OTHER ADVANCED THREATS BEFORE IMPACT

Organizations implementing Infoblox security solutions gain a proactive security posture that stops threats before they can impact business operations. By leveraging predictive threat intelligence and advanced DNS analytics, businesses can move from reactive incident response to preemptive threat prevention, significantly reducing their attack surface and security operational burden.

Success across Real Customer Implementations

- After several high-profile ransomware events, a fast casual restaurant chain needed a more proactive approach to improve overall security posture. With Protective DNS from Infoblox, they were able to significantly reduce ransomware risk while getting 100 percent visibility of their DNS traffic for monitoring threats.
- A large health insurance company addressed vulnerabilities related to DNS tunneling found during initial penetration testing by its red team. Infoblox effectively mitigated these gaps, which had gone unnoticed by the company's NGFW and SASE solutions.
- A transportation company integrated DNS-powered remote access and threat detection with endpoint solutions (such as EDR). This Zero Trust approach helped secure devices and users across the organization.

KEY CAPABILITIES

Predictive Threat Intelligence: Blocks threat actor infrastructure to proactively protect against emerging ransomware and other attacks

AI Analysis: Evaluates DNS queries in customer networks using algorithmic and machine learning techniques that can recognize evolving ransomware and advanced threats, including data exfiltration and DGAs

"Protection Before Impact" Monitor: Enables CISOs and security teams to showcase to the board how early the Infoblox solution blocked threats before users accessed them

Asset Discovery and Inventory Integration: Identifies assets involved in ransomware and other cybersecurity incidents to accelerate assessment and response

1. *Key Cyber Security Statistics for 2025*, Sentinel One, July 30, 2025.
2. *Massive Surge In Ransomware Attacks—AI And 2FA Bypass In Crosshairs*, Winder, Davey, Forbes, March 25, 2025.
3. *ITRC 2024 Annual Data Breach Report*, Identity Theft Resource Center, January 2025.

infoblox

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

Version: 20251020v1