PREDICT. PREEMPT. PREVAIL.

AGAINST SOPHISTICATED AND AI-POWERED ATTACKS WITH THE POWER OF DNS

infoblox®

TABLE OF CONTENTS

THE PROBLEM WITH A REACTIVE “DETECT AND RESPOND” APPROACH

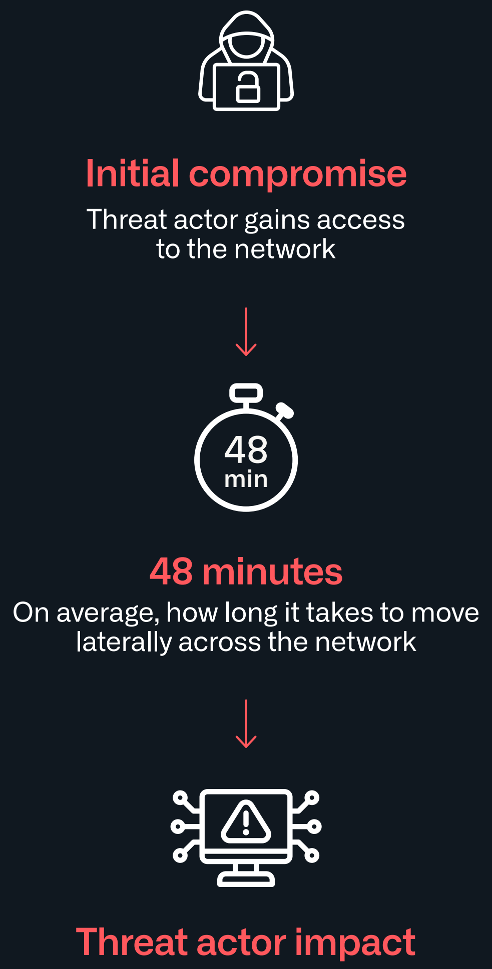
Traditional methods are becoming too slow, risky and ineffective.

The legacy kill chain approach is dying. It has relied on a “patient zero infection” strategy whereby another organization serves as the first target, also known as “patient zero,” so that more can be learned about how that malware behaves—and then applying those insights to your own organization.

But that model no longer holds. Today’s threat actors are crafting malware tailored to your vertical, your company, even your employees—making it exponentially more likely that you will be patient zero.

The average threat actor breakout time—how long it takes an adversary to move laterally across a network after gaining initial access—has reached a speedy 48 minutes.[1] This means that organizations have a very short window to detect, investigate and remediate an attack before it spreads further within your network.

AVERAGE THREAT ACTOR BREAKOUT TIME



Initial compromise

Threat actor gains access to the network

48 minutes

On average, how long it takes to move laterally across the network

Threat actor impact

THREAT ACTORS ARE GAINING AN UNFAIR ADVANTAGE

Despite organizations spending over $200 billion annually on cybersecurity solutions,[2] breaches like ransomware continue to succeed—highlighting critical gaps in current approaches.

As threat actors use new tools to launch more frequent, sophisticated and stealthy attacks, reactive security solutions are no longer sufficient. AI-generated, single-use malware is now so uniquely crafted that every attack becomes a "zero day"—and no signature or known behavior exists to detect it.

HOW THREAT ACTORS ARE USING AI

AI's ability to process vast amounts of data and learn from patterns enables cybercriminals to develop more advanced and targeted attack strategies.

AI-Powered Social Engineering

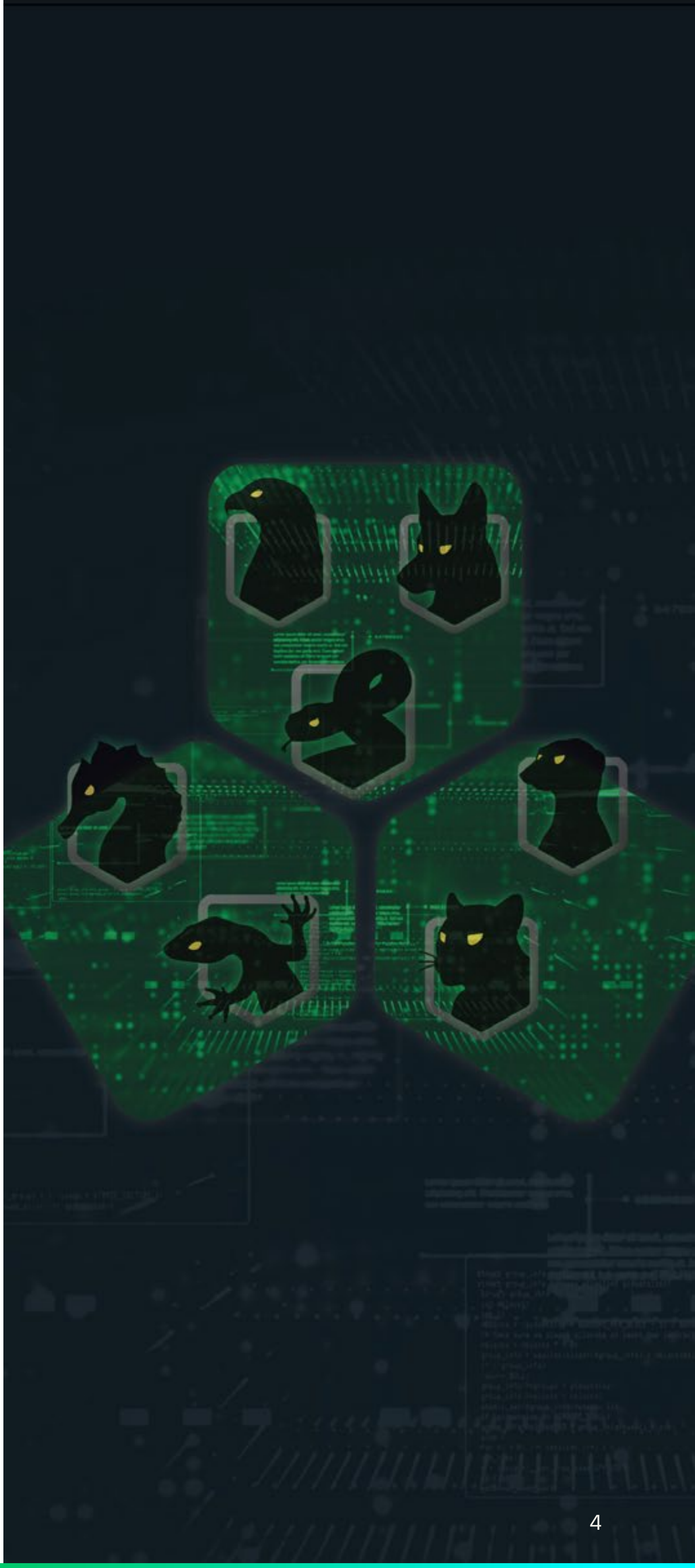
One prominent method is AI-powered social engineering, where attackers create highly convincing phishing emails and voice phishing (vishing) calls, which often sound like they are coming from trusted individuals, making it easier to deceive victims into revealing sensitive information or granting access to secure systems.

AI-Driven Malware Development

Additionally, AI accelerates the development of malicious code, reducing the time required to create sophisticated ransomware that can evade traditional security measures. This capability lowers the barrier for entry, enabling less experienced hackers to deploy effective ransomware attacks.

Lowering the Barrier to Entry for Cybercrime

Finally, AI is making cybercrime more accessible. With AI-powered tools automating everything from phishing kit generation to malware delivery, even low-skilled attackers can now launch credible and damaging campaigns. This rise in "as-a-service" cybercrime—powered by AI—means more frequent, more varied and more difficult-to-predict attacks across industries.



KEY TRENDS IN THE CYBERATTACK LANDSCAPE

Tools like ChatGPT and FraudGPT allow novice attackers to create advanced phishing emails and sophisticated, targeted malware that bypass traditional defenses.

Ransomware attacks surged by 132% in Q1 2025 compared to Q4 2024, aided by AI deception-based social engineering to gain initial access to networks.[3]

Every second, there are 11 victims of malware attacks worldwide. That’s 340 million victims annually, which will continue to grow exponentially.[4]

Vulnerability exploitation saw a 34% increase due to AI-driven threats.[5]

78% of chief information security officers surveyed reported that AI-powered threats are having a significant impact on their organizations.[6]

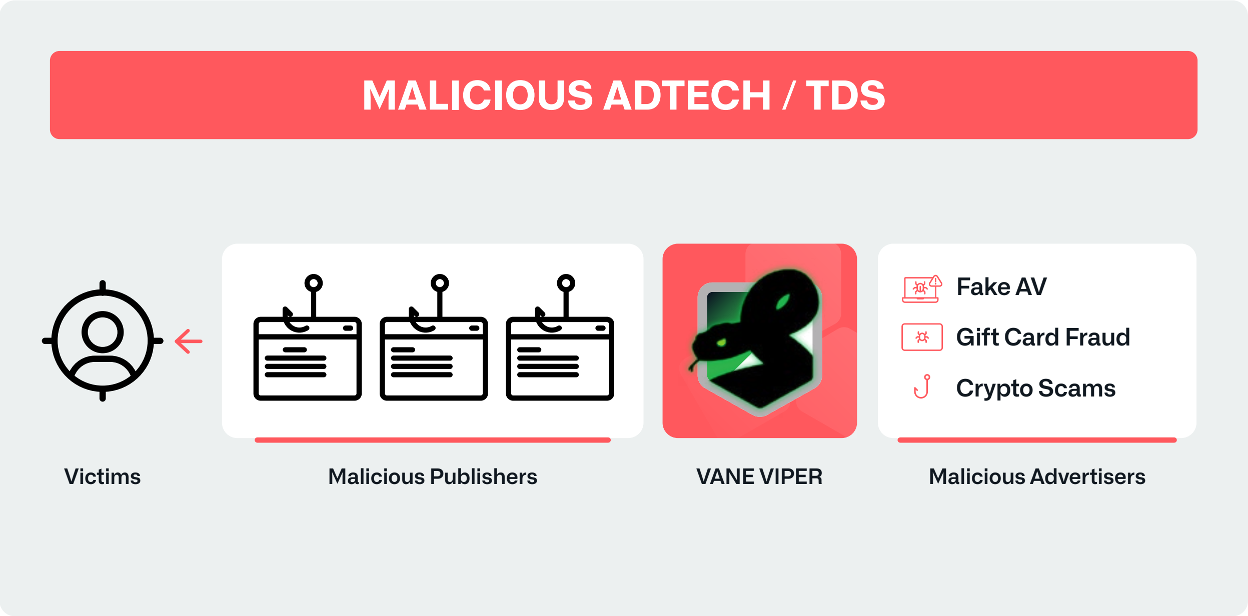
61% of organizations saw an increase in deepfake attacks in 2024.[7]

The number of top-level domains (TLDs) have increased manyfold (30 years ago there were seven, now there are 1,500+), making it easy for actors to create lookalike domains using AI.[8]

THE ROLE OF TRAFFIC DISTRIBUTION SYSTEMS IN MODERN ATTACKS

Traffic distribution systems (TDSs) have been adopted by threat actors to enhance their malicious activities. Just like Google AdSense helps websites monetize by directing users to relevant ads, cybercriminals are using malicious TDS to funnel users to malicious sites, often through hijacked websites or deceptive ads. The redirection chains are built to hide the attacker's infrastructure, making it nearly invisible to traditional security tools. It's stealthy, scalable and, sadly, very profitable for threat actors.

- Malicious adtech use TDSs and mostly deliver infostealer malware which are at the heart of enterprise data breaches.
- Vane Viper, a large-scale fake CAPTCHA campaign that uses TDS to distribute Lumma Stealer, has a massive infrastructure with more than 10,000 domains. It delivered 1 million ad impressions per day in Q4 CY2024 through 3,000+ advertiser sites.



MALICIOUS ADTECH / TDS

PREEMPTIVELY SECURE YOUR ORGANIZATION WITH PROTECTIVE DNS

Preemptive security is an advanced approach that focuses on anticipating, predicting and stopping cyberthreats before they can cause harm.

Gartner defines preemptive cybersecurity as: "A proactive approach aimed at preventing, disrupting or deterring cyberattacks from achieving their objectives. Given threat actors' increasing use of generative AI in cyberattacks, preemptive cybersecurity technologies play a crucial role in enhancing organizations' defense against AI-enabled malware, zero-day vulnerabilities, ransomware and other associated threats. These threats often cannot be effectively mitigated solely through traditional 'detection and response' tools and approaches."

Organizations can use DNS to protect their entire environment—infrastructure on-premises, cloud workloads, remote users, and IoT/OT devices—from sophisticated and modern attacks.

A Protective DNS approach is preemptive because it doesn't rely on patient zero. It uses a combination of predictive threat intelligence that blocks threat actor infrastructure before they are weaponized, and algorithmic/ML-based analysis of DNS queries in customer networks to provide protection before impact.

PREDICTIVE THREAT INTELLIGENCE:

Tracks pre-attack activities and identifies threat actor infrastructure before it's weaponized—instead of chasing malware variants and individual domains.

Leverages DNS telemetry and machine learning to identify high-risk domains and block threats before they land on networks.

Detects and blocks TDSs—used to dynamically redirect users to phishing sites, exploit kits or malware payloads.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

The National Institute of Standards and Technology (NIST) has recognized the importance of DNS in cybersecurity and included Protective DNS guidelines in its authoritative document, NIST SP 800-81. The guide emphasizes the role of DNS as a foundational layer of cyberdefense and states that by integrating Protective DNS into existing security infrastructures, organizations can enhance their ability to detect and block threats earlier than traditional security systems.

> “DNS servers can provide significant insight into the connections and dataflows of endpoints and can often prevent security incidents earlier than other systems.”
>
> **-NIST**

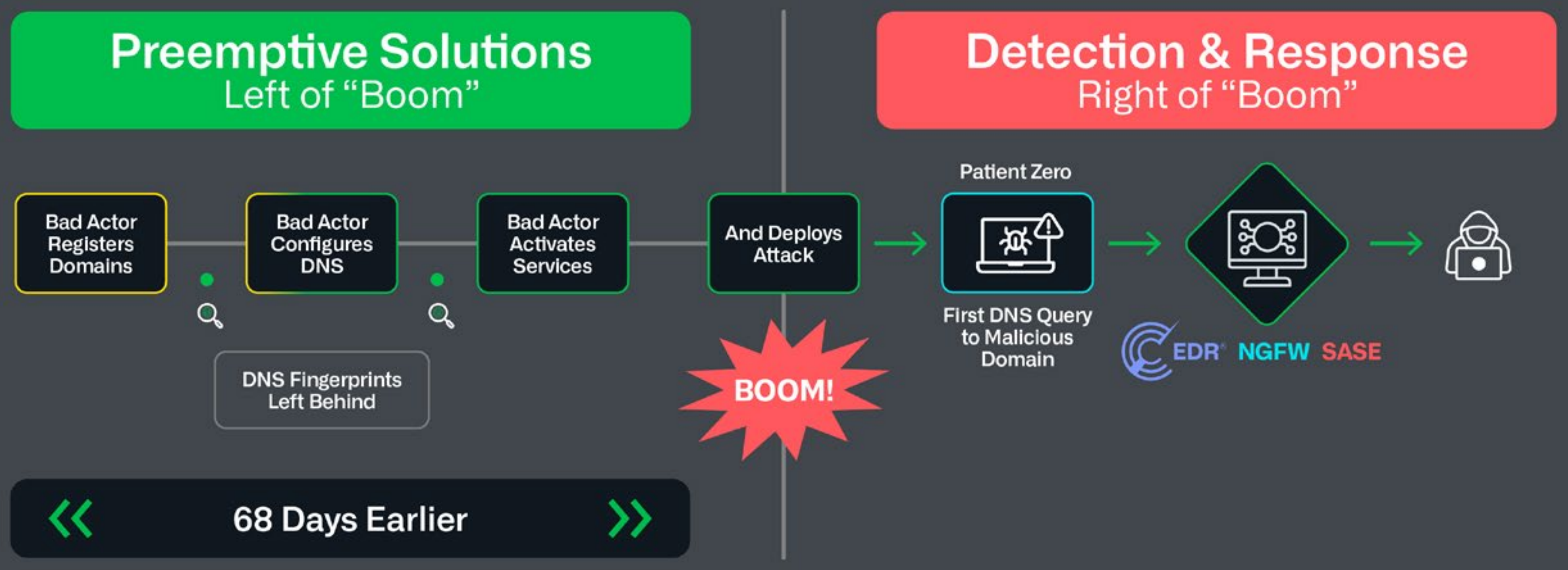
Infoblox's industry-leading Protective DNS offering, Infoblox Threat Defense™, offers many advantages over reactive security measures:

- Provides protection **before impact** and at the intent to communicate.
- As a **DNS resolver**—meaning a server or software that converts human-readable domain names into machine-readable IP addresses—Infoblox **sees every DNS connection** from every device (including end-user devices, IoT/OT) whether they sit behind a firewall or not, whether there is a **SASE agent or not.**
- Monitors **204K real-time** threat actor clusters or groups of related cyberattack activities.
- **Blocks 5X more high-risk/medium-risk** domains vs. other security tools that look for known malicious behavior.
- Blocks on average **68.4 days earlier** than the rest of the industry.
- **Detects 82% of domain-based threats** before the first DNS query.
- Has a **0.0002% false positive** rate.
- Identifies and blocks **unsanctioned AI usage** based on DNS activity.
- Helps reduce exposure from **dangling DNS records** and lookalike domains.
- **Reduces the load by 50%** on other security tools, such as firewalls and security information and event management (SIEM) systems, by **filtering out malicious traffic** before it reaches these systems.
- Easy **user and device attribution** and threat prioritization with asset insights.

INFOBLOX THREAT DEFENSE

204K (and counting) near–real-time clusters/cartels discovered and monitored

100+ named threat actor profiles



82% of threats detected before the first DNS query

0.0002% false positive rates

Real–time protection for newly seen domains

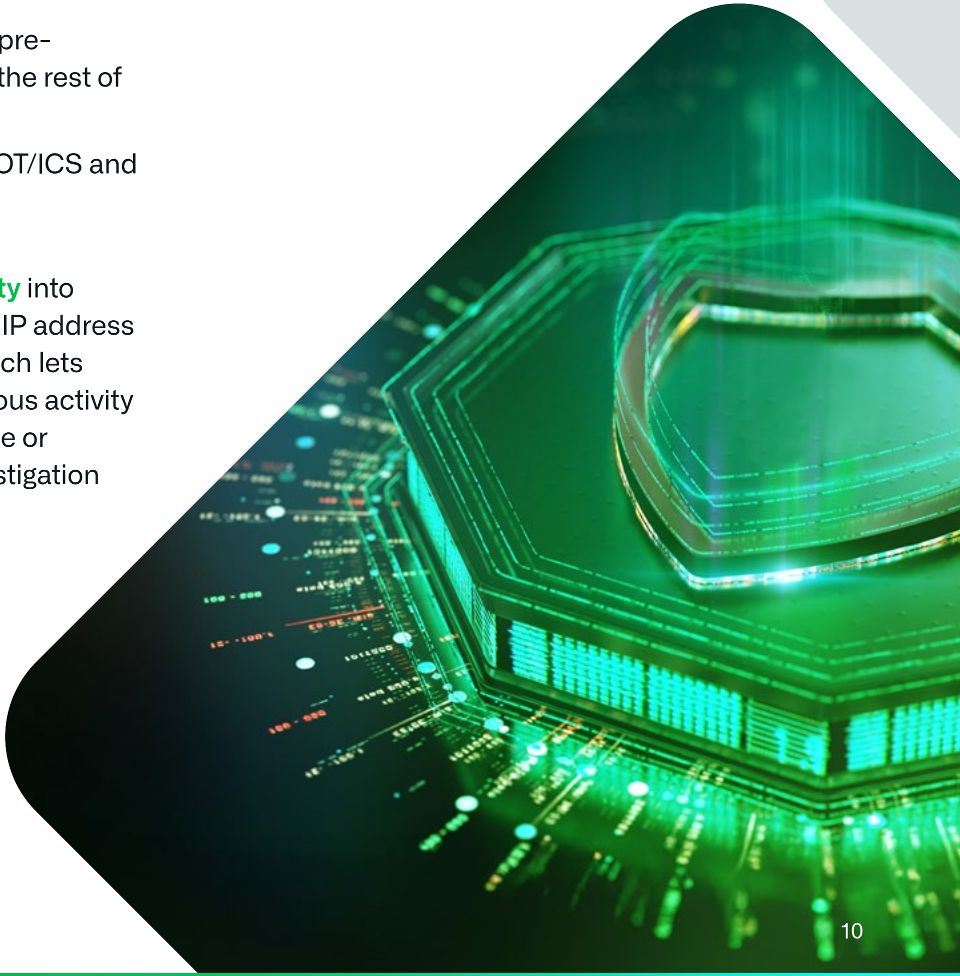
THE POWER OF A PROTECTIVE DDI PLATFORM

Protective DNS works best where DNS is already managed—on a DDI platform. Infoblox is the only vendor that offers an integrated protective DDI platform, making it easier to turn on protection that's managed by a single team responsible and accountable for all DNS-related issues.

This vastly simplifies operations and troubleshooting versus enabling Protective DNS in next-generation firewalls (NGFWs) or Secure Access Service Edge (SASE) solutions. With Infoblox as the DNS resolver, organizations benefit from a single unified platform that monitors enterprise DNS query data for threats, assesses risk when a new domain enters Infoblox resolvers and proactively blocks in-line as needed, preventing incidents from ever occurring.

Other reasons why using Protective DNS on a DDI platform is advantageous:

- **Blocks at the earliest stage,** pre-connection, before it gets to the rest of the security stack.
- Protects users, devices/IOT/OT/ICS and cloud workloads via the **broadest coverage.**
- **Real-time and native visibility** into DNS queries correlated with IP address management and DHCP which lets you immediately map malicious activity back to a specific user, device or workload—speeding up investigation and remediation.



BUSINESS BENEFITS

Reduced risk from data breaches.

Savings on an average of 500 SOC analyst hours per month and $400K in productivity savings per year.

A 243% ROI with a payback period of less than six months.

Reduction of 50% in the number of alerts generated by other security tools, lowering operational costs.

CUSTOMER USE CASES

Infoblox customers have successfully implemented Infoblox solutions for various use cases:

Proactive Protection against Ransomware

A fast casual restaurant chain decided to take a more proactive approach to improve overall security posture by implementing Protective DNS after a couple of high-profile ransomware events. They also wanted 100% visibility of DNS traffic for monitoring threats.

Prevent Data Exfiltration over DNS

A large health insurance company plugged gaps around DNS tunneling identified during an internal pen testing by their red team, which they were not able to block using their existing NGFW and SASE solutions.

Zero Trust

A transportation company used a combination of DNS-powered remote access and threat detection along with endpoint solutions, like endpoint detection and response (EDR) and mobile device management (MDM), to form a Zero Trust user and device strategy to protect “everyone, everywhere, all at once.”

BREAK THE KILL CHAIN BEFORE IT STARTS.
DON'T BE PATIENT ZERO. BE A CYBERHERO.

For more information, please visit the Infoblox Threat Defense page at www.infoblox.com/threat-defense.

[1] *CrowdStrike 2025 Global Threat Report: Beware the Enterprising Adversary*, Myers, Adam, CrowdStrike Blog, February 27, 2025.
[2] *Day 19: Analyzing DNS Logs — Detection Use Cases and How to Spot Malicious Activity*, Infosec Ninja, May 7, 2025
[3] *Massive Surge In Ransomware Attacks—AI And 2FA Bypass In Crosshairs*, Winder, Davey, Forbes, March 25, 2025.
[4] *ITRC Annual Data Breach Report*, Identity Theft Resource Center, January 2025.
[5] *Verizon 2025 DBIR Report*
[6] *Top 40 AI Cybersecurity Statistics*, Fox, Jacob, Cobalt, October 10, 2024.
[7] *Speedy threat actors improving their lateral movement*, Hurley, Billy, IT Brew, March 4, 2025.
[8] ICANN—In 2012, ICANN (the Internet Corporation for Assigned Names and Numbers) launched a top-level domain expansi
program, allowing organizations to apply for custom top-level domains.