infoblox.

Präemptive Netzwerksicherheit für das Zeitalter der künstlichen Intelligenz

Stephan Fritsche, Security Lead Central Europe, Infoblox

18.03.2026, Stuttgart

infoblox®

Stephan Fritsche

Security Lead

Central Europe

MARKET TRENDS

Threat Actors Have Unfair Advantage

Easy for threat actors to register domains at scale, leverage AI for targeted attacks. **Adtech**, and **cloaking techniques** evade detection

Expanded Attack Surface

An organization's attack surface keeps expanding, which includes hybrid users, cloud workloads, IoT/OT and other assets; 91% of organizations have **2+** cloud providers[1]

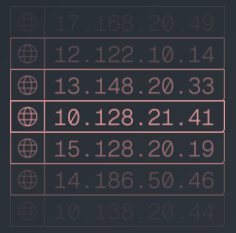
Preemptive Security

Given threat actors' increasing use of GenAI in cyberattacks, **preemptive cybersecurity** technologies play a crucial role in enhancing organizations' defense against AI-enabled malware[2]

1. https://cloud-computing.tmcnet.com/breaking-news/articles/460855-infoblox-simplifies-multi-cloud-complexity-with-ddi-solution.htm#:~:text=A%20TechTarget%20report%2C%20commissioned%20by%20Infoblox%2C%20has,numerous%20benefits%2C%20it%20also%20introduces%20new%20challenges.
2. Gartner – Emerging Tech Radar: Preemptive Cybersecurity, 25 November 2024

infoblox.

AI AND AUTOMATION LOWERING BARRIER FOR THREAT ACTORS



AI-Powered Sophistication

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

Increased Volume

AI-powered scripts generates thousands of fake domains. AI can make domain generation algorithms more evasive and legitimate.

Smarter Traffic Distribution

AI optimizes malicious traffic flow and adapts attack patterns in real time for effectiveness.

infoblox.

LIMITATIONS WITH “REACTIVE SECURITY”

THE PATIENT ZERO PROBLEM

Patient zero infected

Detect in	Respond in	Investigate In
1 min	60 min	10 min

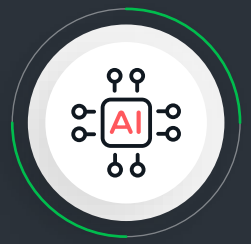
AI coding tools make it easier to create sophisticated and targeted malware

Challenging to detect and response before threat actor breakout time **(48 minutes)**

450,000 new malware samples detected everyday and will increase with AI

THE PATIENT ZERO TRAP

ATTACK LAUNCHED



Threat actor launches attack designed for victim.

SOMEONE ELSE IS HIT FIRST

Someone becomes Patient Zero. No signature. No Alert.

DAMAGE DONE

Patient Zero pays the price: Ransom, downtime, & breach impacts.

DETECTION SHARED

Patient Zero's data trains everyone else's defenses.

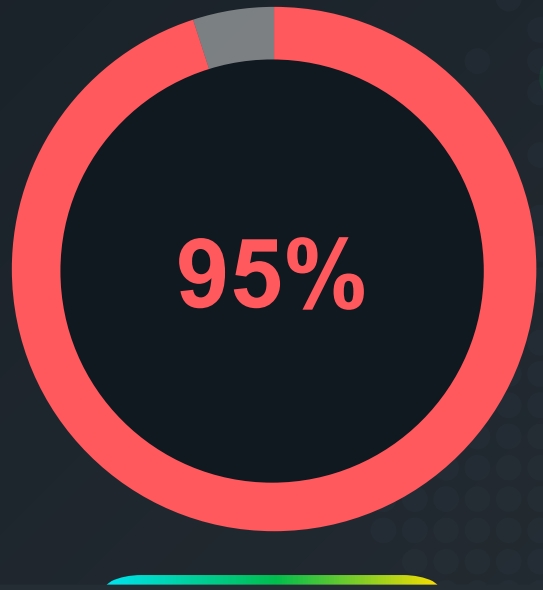
EVERYONE IS PROTECTED

Other orgs benefit. Except Patient Zero.

AI accelerates and scales these attacks significantly.

infoblox

THE REALITY:
EVERYONE IS A PATIENT ZERO NOW
BECAUSE OF AI-DRIVEN ATTACKS



of threat-related
domains target only
one victim

Source: Infoblox Threat Landscape Report

A DIFFERENT APPROACH IS NEEDED

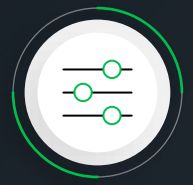
A reactive response-based approach is *no longer enough* to keep networks safe

DNS IS THE FIRST POINT OF DETECTION FOR CYBERATTACKS

Adversary Toehold

An ever-expanding attack surface gives attackers a plethora of hooks – phishing, vishing, prompt injection, vulnerability exploit

Makes a DNS query to resolve a malicious domain



Command and Control

When an attacker exploits a vulnerability or convinces a user to visit a hostile URL, their toehold escalates by visiting a C2 system to download malware/ ransomware or communicate with the adversary.

Makes a DNS query to C2 server

Data Exfiltration

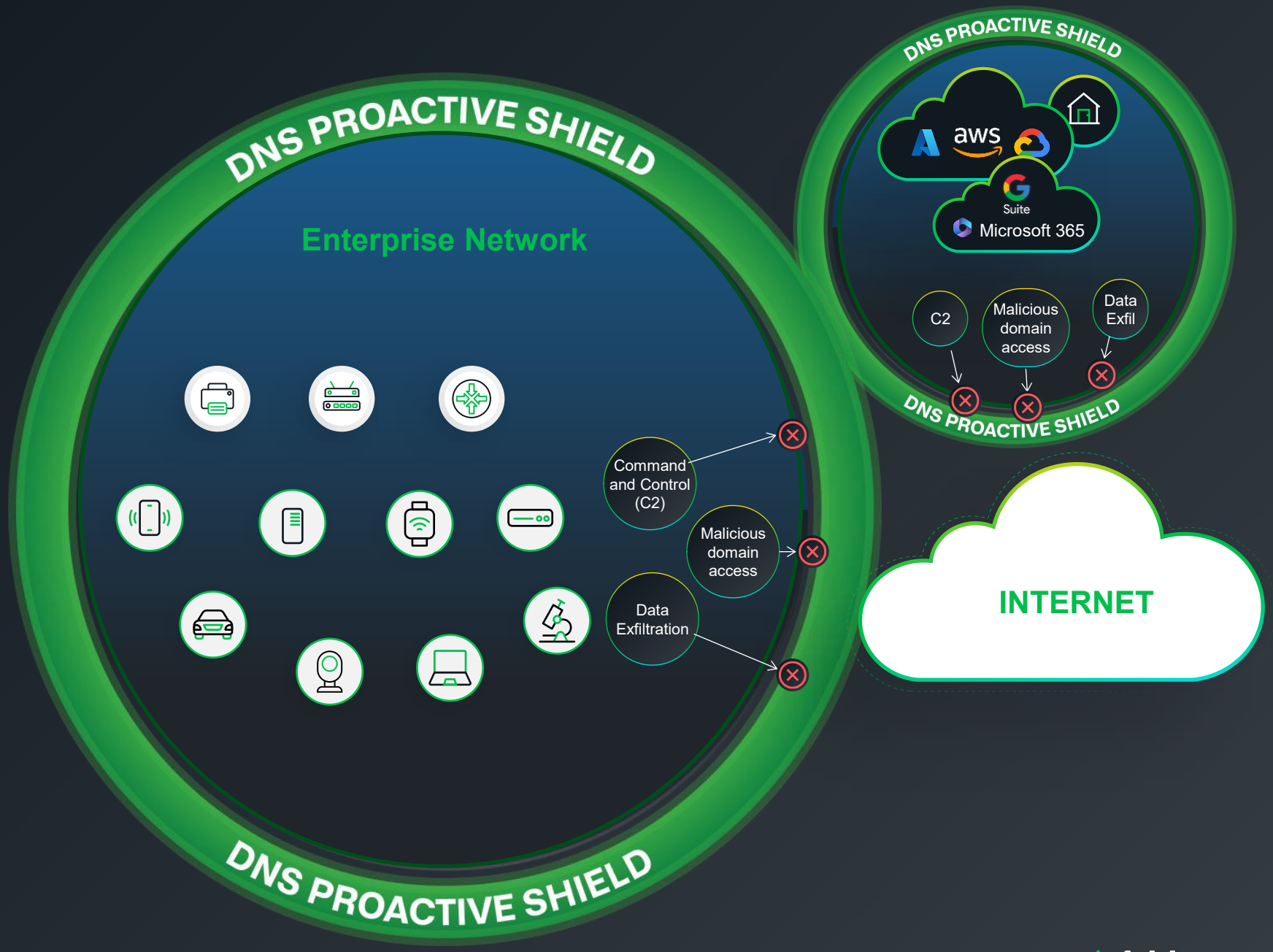
Data is extracted to a malicious server

Makes a DNS query to malicious server

Varied attack chains all have one common thread: Using your existing network infrastructure to make a DNS query

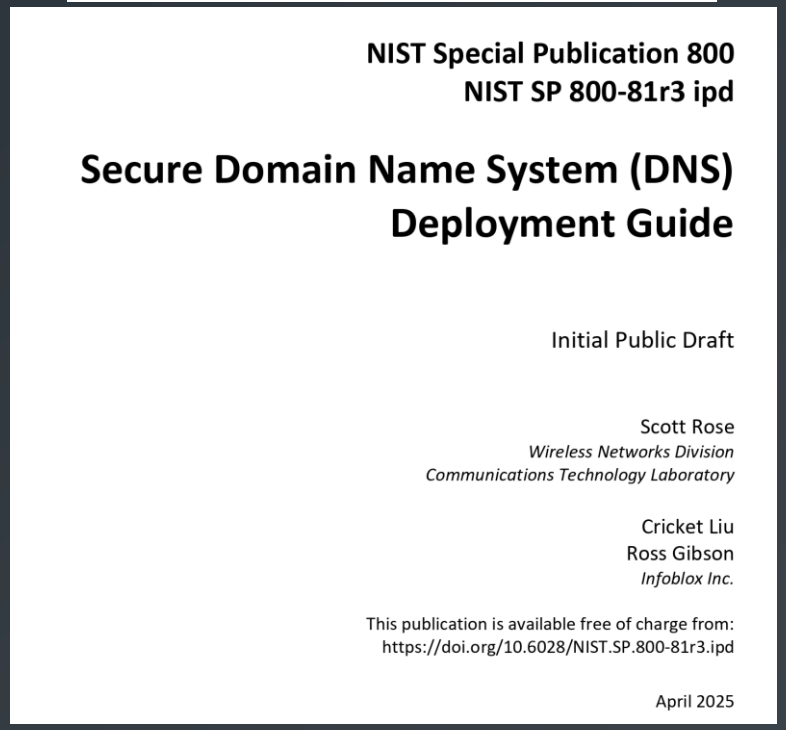
DNS AS A UNIVERSAL, PROACTIVE SHIELD

DNS can block attacks early and reduce load on all security tools



NIST INCLUDES PROTECTIVE DNS IN NEW GUIDE IN 2025

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



NIST Special Publication 800
NIST SP 800-81r3 ipd

Secure Domain Name System (DNS) Deployment Guide

Initial Public Draft

Scott Rose
Wireless Networks Division
Communications Technology Laboratory

Cricket Liu
Ross Gibson
Infoblox Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-81r3.ipd

April 2025

Three Pillars for Best Practices

- Employing Protective DNS
- Protecting DNS Protocol
- Protecting DNS Service and Infrastructure

> “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.

TWO APPROACHES TO SOLVING A DRUG PROBLEM

Going after individual dealers – quick, easy but less impactful

Going after the drug cartel – harder but more strategic and impactful

EXAMPLE – PROLIFIC PUMA

Legitimate Link Shortening Service

bitly

Illegitimate Link Shortening Service – Prolific Puma

Attackers can't use Bitly to shorten their links

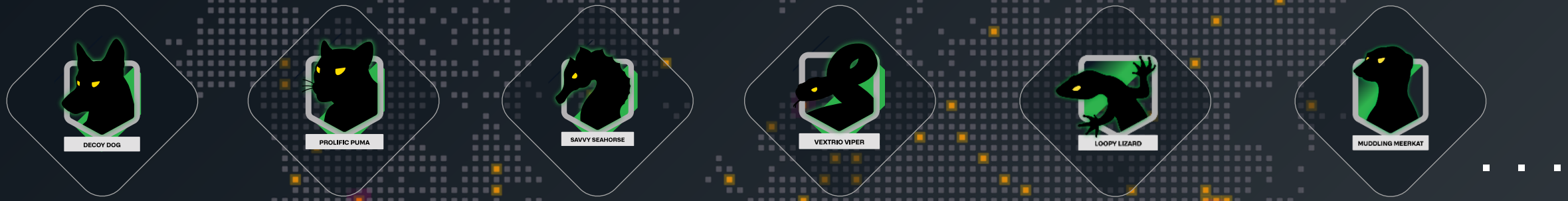
So they use Prolific Puma malicious link shortening service

Since April 2022, Prolific Puma has registered up to **75K** unique domains

Since May 2023, Prolific Puma has used .US for 55% of total domains created; significant numbers of .US domains have been used to attack prominent companies such as BoA, Amazon, AT&T and others

If you block the "drug cartel" Prolific Puma, you can block attackers' supply chain

INFOBLOX TRACKS 204,000 THREAT ACTOR GROUPS



. . .

204,000

near real-time infrastructure clusters discovered and monitored

100+

named threat actor profiles

infoblox

RECENTLY IDENTIFIED BY INFOBLOX

Domain is Registered

*e.g., Rasapool[.]net**

May 4th

High Risk Domain Detected & Blocked by Infoblox

May 6th

Infoblox Blocks on an Average 68.4 Days Earlier than Rest of Industry/Before Attack

First Query Seen

May 9th

MALICIOUS Domain Released in Commercial or Public Intel sources

May 10th

82% of threats detected before the first DNS query, **0.0002%** false positive rate

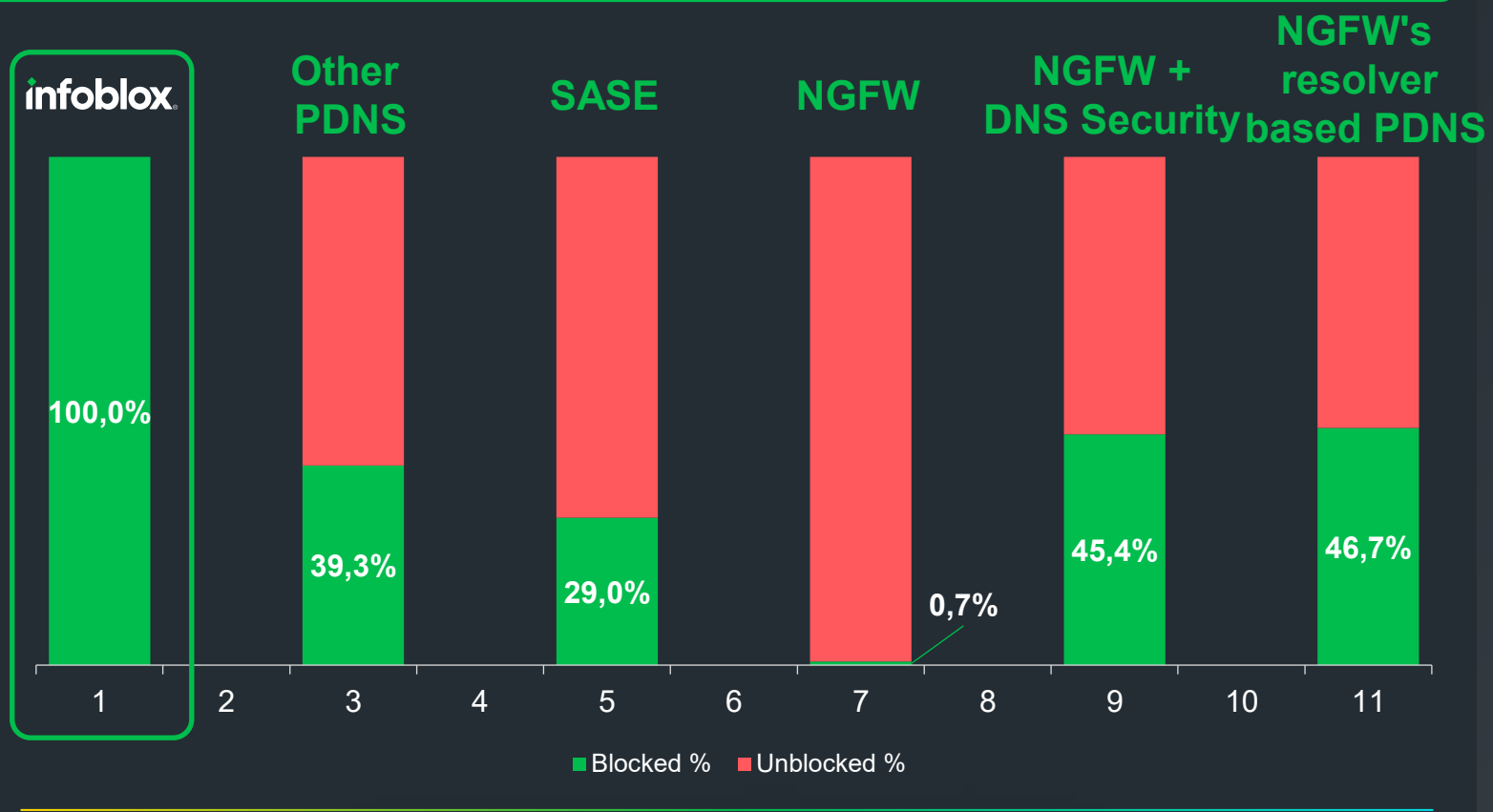
*used in BlackBasta ransomware campaign

INFOBLOX THREAT INTEL BLOCKS MORE DOMAINS OTHERS DON'T

Other tools block a fraction of threats that Infoblox blocks in real customer environments

DNS Threat Intel is Unique

- Malicious Lookalikes
- DNS Tunneling Detection
- DNS Threat Actors
- Blockable New Emergent Domains
- Malicious Domains
- Traffic Distribution Systems
- Encrypted DNS (DoH)
- DGA and RDGA Domains
- New Emerging Phishing Domains
- Command and Control Domains
- Infoblox Preemptive Blocking Domains



Comparison Test of DNS-based Threats

INFOBLOX POWERS GOOGLE CLOUD'S DNS ARMOR

Public preview available in August 2025

Preemptive security for cloud workloads

Leverages market leading DNS threat intelligence and algorithmic/ML based analysis on DNS queries to preemptively detect threats

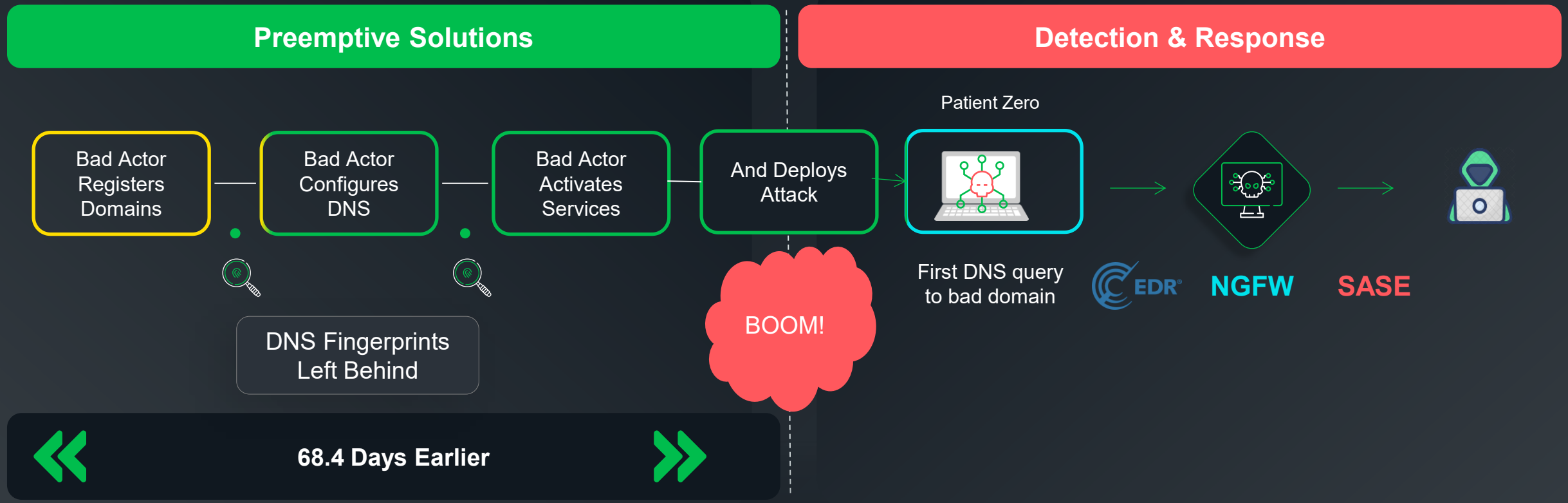
Cloud-native scalability

Designed to grow with workloads, offering unmatched performance and reliability, even during peak demands

Integrated management

Natively integrated into Google Cloud console for seamless monitoring, logging, and analytics without leaving the Google Cloud ecosystem

BUILD PREEMPTIVE SECURITY SOLUTIONS TO IMPROVE THREAT DETECTION



82%
of threats detected before first DNS query

.0002%
false positive rates

Real-time
protection for newly seen domains

infoblox

GARTNER IDENTIFIED INFOBLOX

As Predictive Threat Intelligence Sample Vendor

Range
- Now (0 to 1 year)
- 1 to 3 years
- 3 to 6 years
- 6 to 8 years

Mass
- Low
- Medium
- High
- Very High

Gartner

Emerging Tech Impact Radar: Preemptive Cybersecurity

7 October 2025 - ID G00830315 - 46 min read

By: Emerging Tech and Trends Security Research Team

Initiatives: Emerging Technologies and Trends Impact on Products and Services

> Traditional cybersecurity based on a reactive detection and response approach is struggling against emerging AI threats and failing to keep pace in many cases. C-level executives must embrace a new preemptive strategy to neutralize threats before they can cause harm.

Overview

Key Findings

- Preemptive cybersecurity is the future of business resilience. Instead of just reacting to threats, C-level executives must evolve their security operations into a proactive, living defense system that actively anticipates and prevents attacks. This strategic shift is no longer just about protecting against loss — it's about building a foundation for future growth and innovation.
- The emerging AI-enabled threat landscape demands more than just faster detection and response; it requires predictive threat intelligence combined with AI-driven analytics and preemptive action. AI and machine learning (ML) technologies must be used to anticipate attack paths and predict where an adversary is likely to strike to more effectively neutralize potential attacks before they begin.
- The future of cybersecurity is defined not by static defenses, but by dynamic infrastructure. This preemptive approach fundamentally shifts the focus from building walls and reacting to breaches to actively securing the underlying systems and networks. By implementing continuous, adaptive changes, organizations can make their infrastructure inherently more resilient and unpredictable, effectively neutralizing threats by denying attackers a stable target.

Recommendations

C-level executives must:

Gartner

Hype Cycle for Security Operations, 2025

Quick Answer: How Does Exposure Management Support Preemptive Cybersecurity?

Predictive Threat Intelligence

Analysis By: Elizabeth Kim

Definition:

The goal of predictive threat intelligence (PTI) technology solutions is to forecast the likelihood of future cyberattacks and provide early insights on emerging threats so security teams can proactively strengthen and prepare their defenses. PTI platforms combine AI with advanced analytics and predictive modeling to collect and analyze large amounts of cybersecurity data. PTI platforms are the evolution of traditional threat intelligence solutions. However, unlike traditional threat intelligence platforms, PTI solutions are focused less on what has happened in the past and more on enabling security teams to explore and understand what could happen in the near future. When combined with intelligent simulation and scenario testing, PTI can enable cybersecurity teams to move from theoretical models toward empirical validation. PTI is a critical emerging technology that is foundational to preemptive cybersecurity strategies.

Sample Vendors

Anomali; Augur Security; BforeAI; CrowdSec; Haruspex; Infoblox; Orpheus Cyber; Silent Push

Range

The range for predictive threat intelligence is one to three years because of the rapid advancements around AI, which is the underlying technology fueling PTI.

GETTING STARTED

01

Learn:

Attend the **Hands-on lab** or a **Security Workshop**

02

Evaluate:

Sign up for a **Security Assessment**

03

Try:

Take a test drive with a **POC** or use the **Infoblox Inspect Tool**

04

Justify:

Get a **Business Value Assessment** done

infoblox.

IT-Security
Roadshow 2026

controlware

Danke für Ihre Aufmerksamkeit.