# VORHERSAGEN.
# VORBEUGEN.
# DURCHSETZEN.

GEGEN AUSGEKLÜGELTE UND
KI-GESTÜTZTE ANGRIFFE MIT
DER POWER VON DNS

infoblox®

# INHALTSVERZEICHNIS

# DAS PROBLEM MIT EINEM REAKTIVEN „ERKENNEN UND REAGIEREN“-ANSATZ

## Traditionelle Methoden werden zu langsam, riskant und ineffektiv.

Der herkömmliche Kill-Chain-Ansatz hat ausgedient. Er beruht auf einer „Patient Null-Infektion“-Strategie, bei der eine andere Organisation als erstes Ziel dient, auch bekannt als „Patient Null“. So kann man mehr über das Verhalten dieser Malware lernen und diese Erkenntnisse dann auf die eigene Organisation anwenden.

Aber dieses Modell funktioniert nicht mehr. Die Bedrohungsakteure von heute entwickeln Malware, die auf Ihre Branche, Ihr Unternehmen und sogar Ihre Mitarbeiter zugeschnitten ist – und machen es damit exponentiell wahrscheinlicher, dass Sie der Patient Null sind.

**Die durchschnittliche Ausbruchszeit von Bedrohungsakteuren (also die Zeit, die ein Angreifer benötigt, um sich nach dem ersten Zugriff lateral durch ein Netzwerk zu bewegen) liegt bei 48 Minuten.**[1] Das bedeutet, dass Unternehmen nur ein sehr kurzes Zeitfenster haben, um einen Angriff zu erkennen, zu untersuchen und zu unterbinden, bevor er sich weiter im Netzwerk ausbreitet.

# DURCHSCHNITTLICHE AUSBRUCHSZEIT VON BEDROHUNGSAKTEUREN

### Erster Zugriff

Ein Bedrohungsakteur verschafft sich Zugang zum Netzwerk


### 48 Minuten

Wie lange es im Durchschnitt dauert, bis eine laterale Bewegung im Netzwerk stattfindet

### Auswirkungen von Bedrohungsakteuren

# BEDROHUNGSAKTEURE VERSCHAFFEN SICH EINEN UNFAIREN VORTEIL

**Obwohl Organisationen jährlich über 200 Milliarden US-Dollar für Cybersicherheitslösungen ausgeben,[2] sind Angriffe wie Ransomware weiterhin erfolgreich. Dies ist ein Indikator für kritische Lücken in aktuellen Ansätzen.**

Da Bedrohungsakteure neue Werkzeuge verwenden, um häufiger, ausgefeilter und unauffälliger anzugreifen, sind reaktive Sicherheitslösungen nicht mehr ausreichend. KI-generierte, einmalig einsetzbare Malware ist mittlerweile so einzigartig, dass jeder Angriff zu einem „Zero-Day" wird. Hierbei existiert weder eine Signatur noch ein bekanntes Verhalten, um sie zu erkennen.

## WIE BEDROHUNGSAKTOREN KI EINSETZEN

Die Fähigkeit der KI, große Datenmengen zu verarbeiten und aus Mustern zu lernen, ermöglicht es Cyberkriminellen, fortschrittlichere und gezieltere Angriffsstrategien zu entwickeln.

**KI-gestütztes Social Engineering**
Eine prominente Methode ist das KI-gestützte Social Engineering, bei dem Angreifer äußerst überzeugende Phishing-E-Mails und Voice-Phishing-Anrufe (Vishing) erstellen, die oft so klingen, als kämen sie von vertrauenswürdigen Personen. Dies macht es einfacher, die Opfer dazu zu verleiten, sensible Informationen preiszugeben oder Zugang zu sicheren Systemen zu gewähren.

**KI-gestützte Malware-Entwicklung**
Darüber hinaus beschleunigt KI die Entwicklung von bösartigem Code und verkürzt so die Zeit, die für die Entwicklung ausgefeilter Ransomware benötigt wird, die herkömmliche Sicherheitsmaßnahmen umgehen kann. Diese Fähigkeit senkt die Einstiegshürde und ermöglicht es auch weniger erfahrenen Hackern, effektive Ransomware-Angriffe durchzuführen.

**Senkung der Einstiegshürden für Cyberkriminalität**
Und schließlich macht KI die Cyberkriminalität leichter zugänglich. Mit KI-gestützten Tools, die alles von der Erstellung von Phishing-Kits bis hin zur Verbreitung von Malware automatisieren, können nun auch weniger qualifizierte Angreifer glaubwürdige und schädliche Kampagnen durchführen. Diese Zunahme von Cyberkriminalität „als Service", möglich gemacht durch die KI, bedeutet häufigere, vielfältigere und schwerer vorhersehbare Angriffe in allen Branchen.

# WICHTIGE TRENDS IN DER CYBERANGRIFFSLANDSCHAFT

Tools wie ChatGPT und FraudGPT ermöglichen es unerfahrenen Angreifern, fortschrittliche Phishing-E-Mails und ausgeklügelte, gezielte Malware zu erstellen, die herkömmliche Abwehrmaßnahmen umgehen.

Im ersten Quartal 2025 stieg die Zahl der Ransomware-Angriffe im Vergleich zum vierten Quartal 2024 um 132 %, unterstützt durch KI-gestütztes, täuschungsbasiertes Social Engineering, um sich zunächst Zugang zu Netzwerken zu verschaffen.[3]

Jede Sekunde gibt es weltweit 11 Opfer von Malware-Angriffen. Das sind 340 Millionen Opfer jährlich, und die Zahl wird exponentiell weiter wachsen.[4]

Die Ausnutzung von Schwachstellen verzeichnete aufgrund von KI-gesteuerten Bedrohungen einen Anstieg von 34 %.[5]

78 % der befragten Chief Information Security Officers berichteten, dass KI-gestützte Bedrohungen erhebliche Auswirkungen auf ihre Organisationen haben.[6]

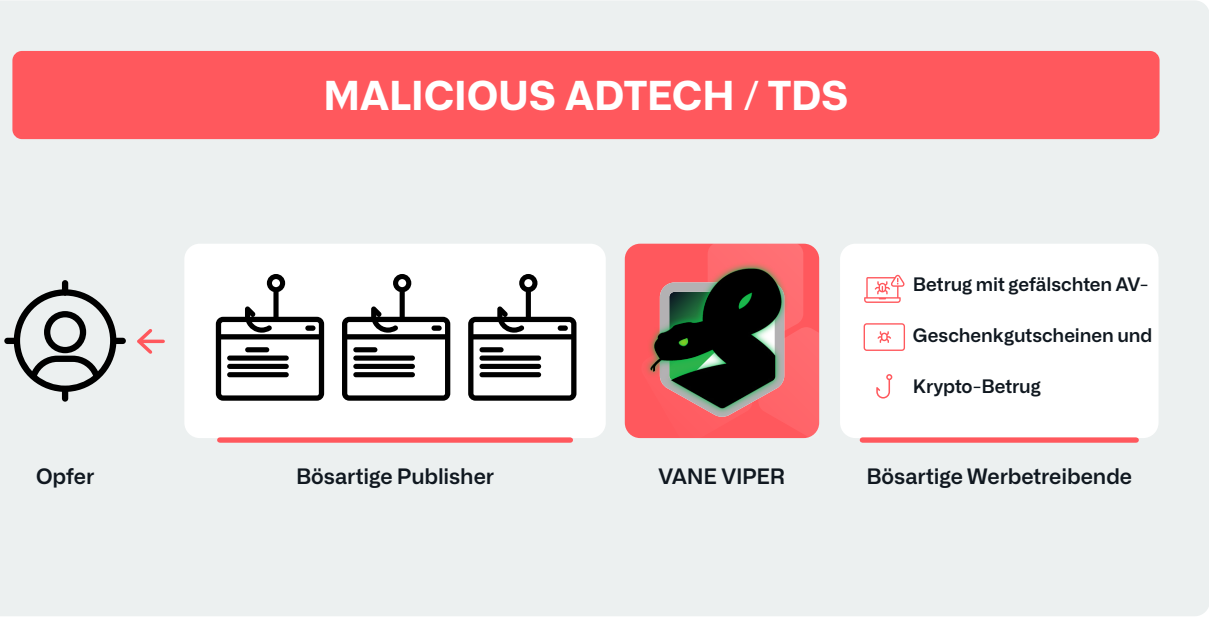
61 % der Organisationen verzeichneten im Jahr 2024 einen Anstieg bei Deepfake-Angriffen.[7]

Die Anzahl der Top-Level-Domains (TLDs) hat sich vervielfacht (vor 30 Jahren waren es sieben, heute sind es über 1.500). Das wiederum macht es Cyberkriminellen leicht, mithilfe von KI Lookalike-Domains zu erstellen.[8]

# DIE ROLLE VON TRAFFIC DISTRIBUTION SYSTEMS BEI MODERNEN ANGRIFFEN

Traffic Distribution Systems (TDS) wurden von Bedrohungsakteuren übernommen, um ihre böswilligen Aktivitäten zu verstärken. Genauso wie Google AdSense Websites bei der Monetarisierung hilft, indem es Nutzer zu relevanten Anzeigen leitet, nutzen Cyberkriminelle bösartige TDS, um Nutzer auf bösartige Websites zu leiten, oft über gekaperte Websites oder irreführende Anzeigen. Die Umleitungsketten sind so aufgebaut, dass sie die Infrastruktur des Angreifers verbergen und für herkömmliche Sicherheitstools nahezu unsichtbar machen. Sie sind heimtückisch, skalierbar und leider auch sehr profitabel für die Angreifer.

- Bösartige Adtech-Anwendungen nutzen TDSs und verbreiten vor allem Infostealer-Malware, die im Zentrum von Datenverstößen in Unternehmen stehen.
- Vane Viper, eine groß angelegte getürkte CAPTCHA-Kampagne, die TDS zur Verbreitung von Lumma Stealer nutzt, verfügt über eine massive Infrastruktur mit mehr als 10.000 Domains. Sie lieferte im 4. Quartal CY2024 täglich 1 Million Werbeeinblendungen über mehr als 3.000 Websites von Werbetreibenden.




# PRÄVENTIVE SICHERUNG IHRES UNTERNEHMENS MIT PROTECTIVE DNS

**Präventive Sicherheit ist ein fortschrittlicher Ansatz, der sich darauf konzentriert, Cyber-Bedrohungen zu antizipieren, vorherzusehen und zu stoppen, bevor sie Schaden anrichten können.**

Gartner definiert präventive Cybersicherheit als: „Ein proaktiver Ansatz, der darauf abzielt, Cyberangriffe zu verhindern, zu stören oder von der Erreichung ihrer Ziele abzuhalten. Da Bedrohungsakteure bei Cyberangriffen zunehmend auf generative KI zurückgreifen, spielen präventive Cybersecurity-Technologien eine entscheidende Rolle bei der Verbesserung der Verteidigung von Unternehmen gegen KI-gestützte Malware, Zero-Day-Schwachstellen, Ransomware und andere damit verbundene Bedrohungen. Diese Bedrohungen können oft nicht allein durch herkömmliche ‚Erkennungs- und Reaktions'-Tools und -Ansätze wirksam eingedämmt werden."

**Organisationen können DNS verwenden, um ihre gesamte Umgebung – On-Premises-Infrastruktur, Cloud-Workloads, Remote-Benutzer und IoT/OT-Geräte – vor ausgeklügelten und modernen Angriffen zu schützen.**

Ein „Protective DNS"-Ansatz ist präventiv, weil er sich nicht auf den Patienten Null verlässt. Er nutzt eine Kombination aus prädiktiver Bedrohungsanalyse, die die Infrastruktur von Bedrohungsakteuren blockiert, bevor diese als Waffe eingesetzt werden, und einer algorithmischen/ML-basierten Analyse von DNS-Anfragen in Kundennetzwerken, um Schutz zu bieten, bevor der Angriff Wirkung zeigt.

# PRÄDIKTIVE THREAT INTELLIGENCE:

Verfolgt Aktivitäten vor einem Angriff und identifiziert die Infrastruktur von Bedrohungsakteuren, bevor sie für Angriffe genutzt wird, anstatt Malware-Varianten und einzelne Domains zu verfolgen.

Verwendet DNS-Telemetrie und maschinelles Lernen, um hochriskante Domains zu identifizieren und Bedrohungen zu blockieren, bevor sie in Netzwerken ankommen.

Erkennt und blockiert TDSs, die dazu verwendet werden, Benutzer dynamisch auf Phishing-Websites, Exploit-Kits oder Malware-Payloads umzuleiten.

---

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

Das National Institute of Standards and Technology (NIST) hat die Bedeutung von DNS für die Cybersicherheit erkannt und Richtlinien für Protective DNS in sein maßgebliches Dokument, NIST SP 800-81, aufgenommen. Der Leitfaden unterstreicht die Rolle von DNS als grundlegende Ebene der Cyberabwehr und erklärt, dass Unternehmen durch die Integration von Protective DNS in bestehende Sicherheitsinfrastrukturen ihre Fähigkeit verbessern können, Bedrohungen früher als herkömmliche Sicherheitssysteme zu erkennen und zu blockieren.

> DNS-Server können bedeutende Einblicke in die Verbindungen und Datenflüsse von Endpunkten gewähren und Sicherheitsvorfälle oft früher als andere Systeme verhindern“.
>
> –**NIST**

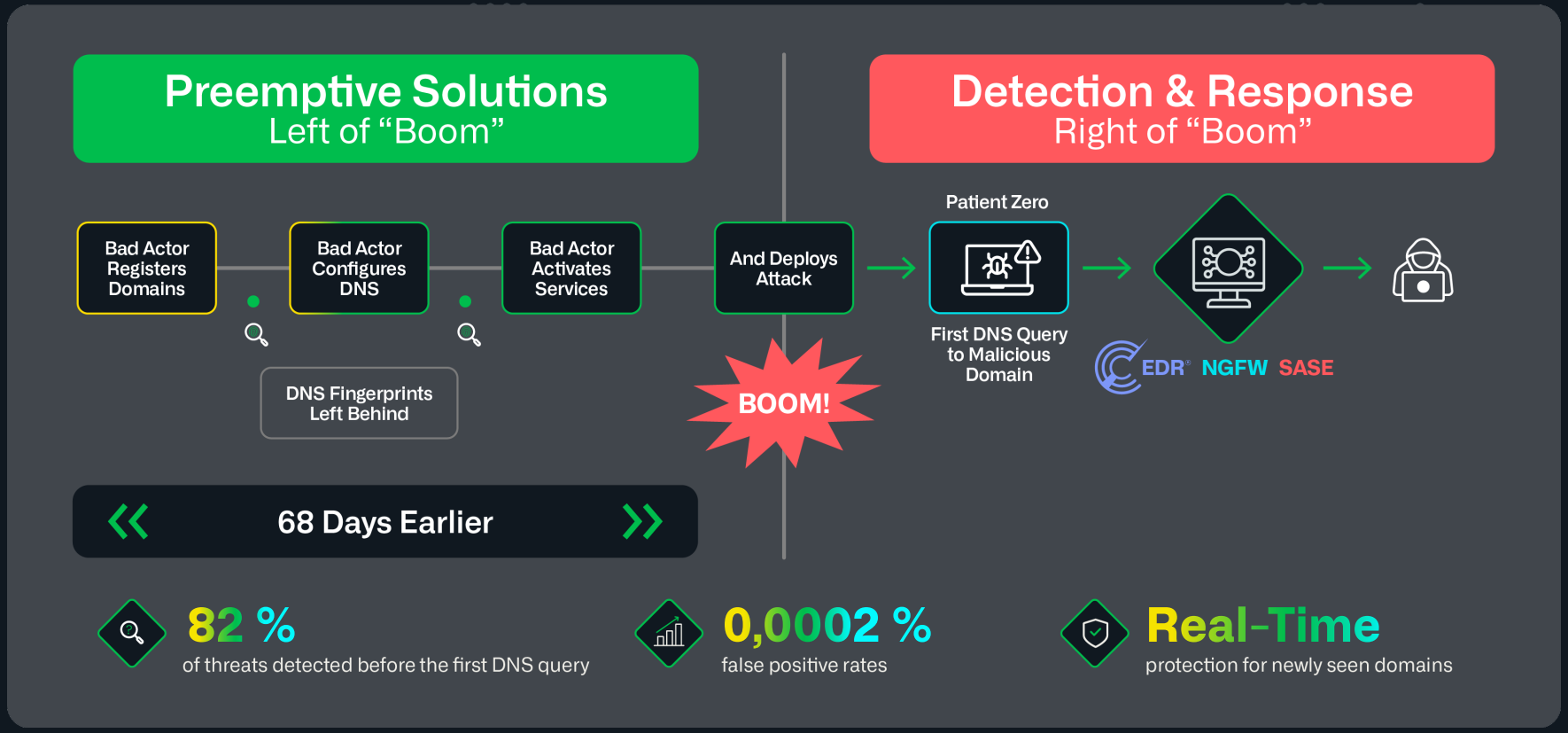
## Das branchenführende Protective DNS-Angebot von Infoblox, Infoblox Threat Defense™, bietet viele Vorteile gegenüber reaktiven Sicherheitsmaßnahmen:

- Bietet Schutz **vor dem Eintreten von Auswirkungen** und bei der Absicht zu kommunizieren.
- Als **DNS-Resolver** (d. h. ein Server oder eine Software, die von Menschen lesbare Domainnamen in maschinenlesbare IP-Adressen umwandelt) **sieht Infoblox jede DNS-Verbindung** von jedem Gerät (einschließlich Endbenutzergeräten, IoT/OT), unabhängig davon, ob sie sich hinter einer Firewall befinden oder nicht, ob es einen **SASE-Agenten gibt oder nicht.**
- Überwacht **204.000** Bedrohungsakteur-Cluster oder Gruppen verwandter Cyberangriffsaktivitäten in Echtzeit.
- **Blockiert 5-mal mehr hochriskante/mittelriskante Domains** im Vergleich zu anderen Sicherheitstools, die nach bekanntem bösartigem Verhalten suchen.
- Blockiert im Durchschnitt **68,4 Tage früher** als der Rest der Branche.
- **Erkennt 82 % der domainbasierten Bedrohungen** vor der ersten DNS-Abfrage.
- Hat eine **Falsch-Positiv-Rate von 0,0002 %**.
- Identifiziert und blockiert **nicht genehmigte KI-Nutzung** basierend auf DNS-Aktivität.
- Hilft, die Gefährdung durch **verwaiste DNS-Einträge** und ähnliche Domains zu reduzieren.
- Reduziert die Belastung anderer Sicherheitstools wie Firewalls und SIEM-Systeme (Security Information and Event Management) **um 50 %**, indem **bösartiger Datenverkehr herausgefiltert** wird, bevor er diese Systeme erreicht.
- Einfache **Zuordnung von Benutzern und Geräten** und Priorisierung von Bedrohungen mit Asset-Einblicken.

# INFOBLOX THREAT DEFENSE

## 204K (Tendenz steigend) nahezu in Echtzeit entdeckte und überwachte Cluster/Kartelle

## ÜBER 100 Profile von benannten Bedrohungsakteuren



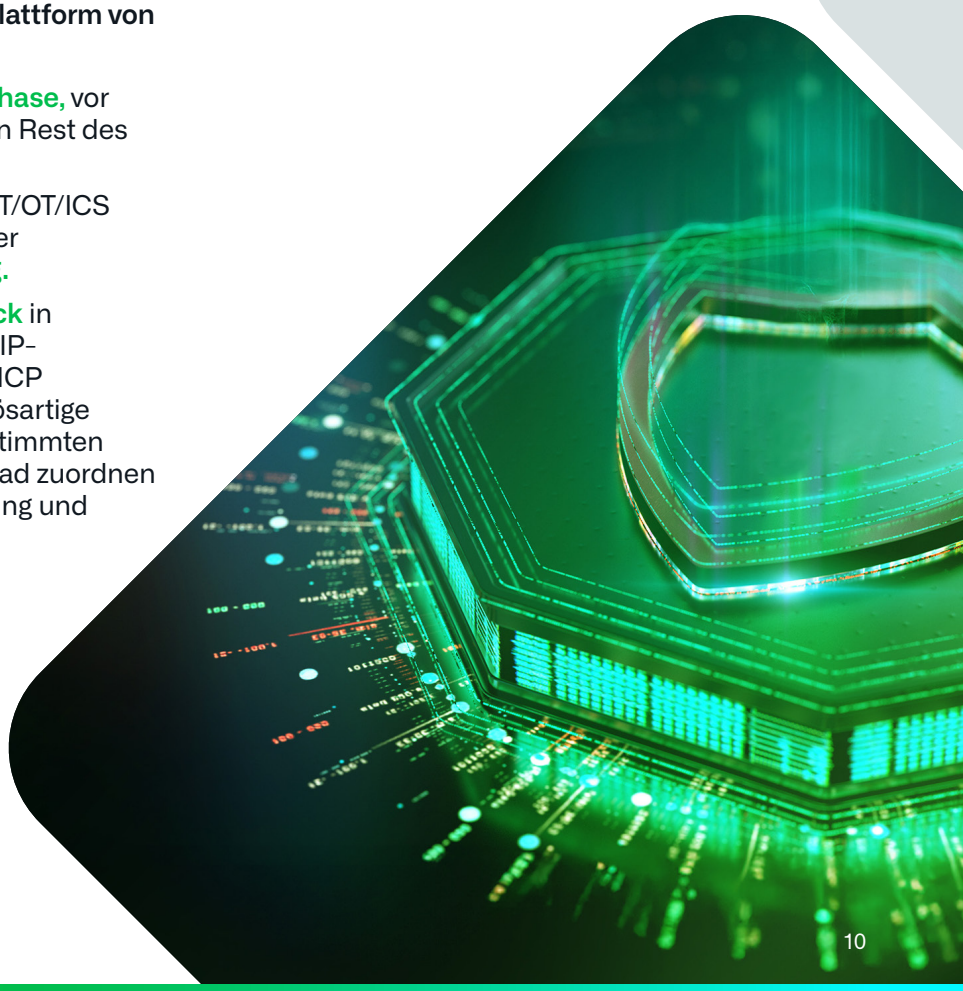
# DIE STÄRKE EINER PROTECTIVE DDI-PLATTFORM

**Protective DNS funktioniert am besten dort, wo DNS bereits verwaltet wird – auf einer DDI-Plattform. Infoblox ist der einzige Anbieter, der eine integrierte Protective DDI-Plattform anbietet, die die Aktivierung eines Schutzes erleichtert, der von einem einzigen Team verwaltet wird, das für alle DNS-bezogenen Probleme verantwortlich ist.**

Dies vereinfacht den Betrieb und die Fehlerbehebung im Vergleich zur Aktivierung von Protective DNS in Next-Generation Firewalls (NGFWs) oder Secure Access Service Edge (SASE) Lösungen erheblich. Mit Infoblox als DNS-Resolver profitieren Unternehmen von einer einzigen, einheitlichen Plattform, die die DNS-Abfragedaten des Unternehmens auf Bedrohungen hin überwacht, das Risiko bewertet, wenn eine neue Domain in die Infoblox-Resolver gelangt, und bei Bedarf proaktiv blockiert, so dass Vorfälle gar nicht erst auftreten.

**Weitere Gründe, warum die Verwendung von Protective DNS auf einer DDI-Plattform von Vorteil ist:**

- **Blockiert in der frühesten Phase,** vor der Verbindung, bevor es den Rest des Sicherheitsstacks erreicht.
- Schützt Benutzer, Geräte/IOT/OT/ICS und Cloud-Workloads mit der **umfassendsten Abdeckung.**
- **Echtzeit- und nativer Einblick** in DNS-Abfragen, die mit dem IP-Adressmanagement und DHCP korreliert sind, sodass Sie bösartige Aktivitäten sofort einem bestimmten Benutzer, Gerät oder Workload zuordnen können, was die Untersuchung und Remediation beschleunigt.



# GESCHÄFTLICHE VORTEILE

- Reduziertes Risiko durch Datenverletzungen.
- Einsparungen von durchschnittlich 500 SOC-Analystenstunden pro Monat und 400.000 USD an Produktivitätssteigerung pro Jahr.
- Ein ROI von 243 % mit einer Amortisationszeit von weniger als sechs Monaten.
- Reduzierung der Anzahl der durch andere Sicherheitswerkzeuge generierten Warnmeldungen um 50 %, wodurch die Betriebskosten gesenkt werden.

# ANWENDUNGSFÄLLE VON KUNDEN

**Infoblox-Kunden haben Infoblox-Lösungen erfolgreich für verschiedene Anwendungsfälle implementiert:**

### Proaktiver Schutz vor Ransomware

Eine Fast-Casual-Restaurantkette entschied sich nach einigen aufsehenerregenden Ransomware-Ereignissen für einen proaktiveren Ansatz zur Verbesserung der allgemeinen Sicherheitslage durch die Implementierung von Protective DNS. Das Unternehmen wollte außerdem eine 100%ige Transparenz des DNS-Traffics zur Überwachung von Bedrohungen.

### Verhinderung von Datenexfiltration über DNS

Eine große Krankenversicherung schloss Lücken im Bereich DNS-Tunneling, die während eines internen Pen-Tests durch ihr Red-Team festgestellt wurden und die mit den bestehenden NGFW- und SASE-Lösungen nicht blockiert werden konnte.

### Zero Trust

Ein Transportunternehmen nutzte eine Kombination aus DNS-gestütztem Fernzugriff und Bedrohungserkennung zusammen mit Endpunktlösungen wie Endpoint Detection and Response (EDR) und Mobile Device Management (MDM), um eine Zero-Trust-Benutzer- und -Gerätestrategie zu entwickeln, die „alle, überall und gleichzeitig“ schützt.

# DURCHBRECHEN SIE DIE KILL CHAIN, BEVOR SIE BEGINNT. SEIEN SIE NICHT PATIENT NULL. WERDEN SIE EIN CYBERHERO.

Weitere Informationen finden Sie auf der Infoblox Threat Defense Seite unter www.infoblox.com/de/products/threat-defense/.


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