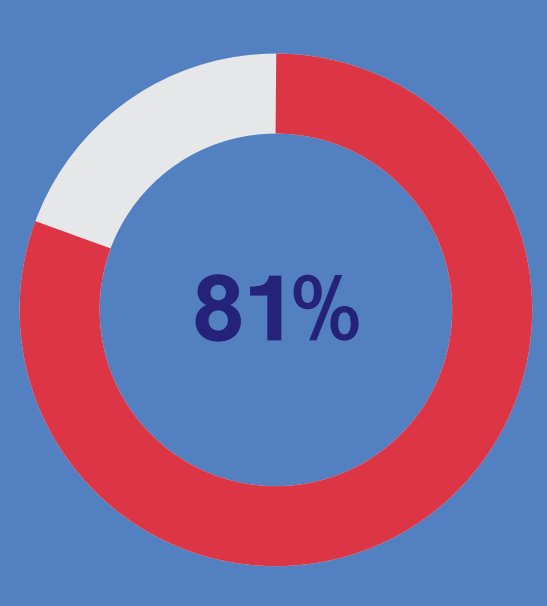
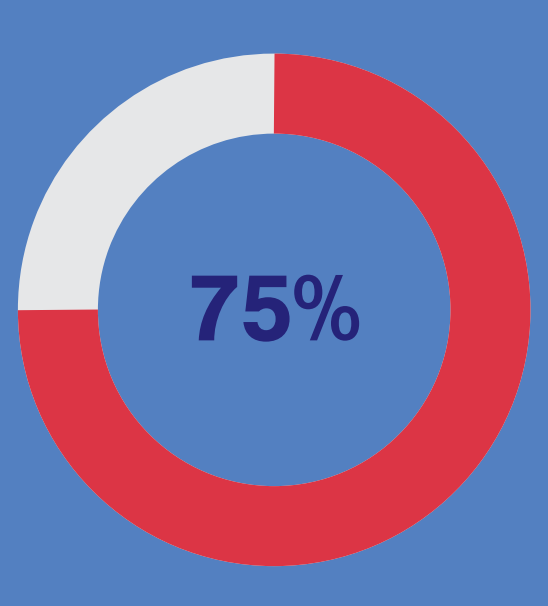
DARKREADING infoblox

Leveling Up Cyber-Threat Intelligence Maturity

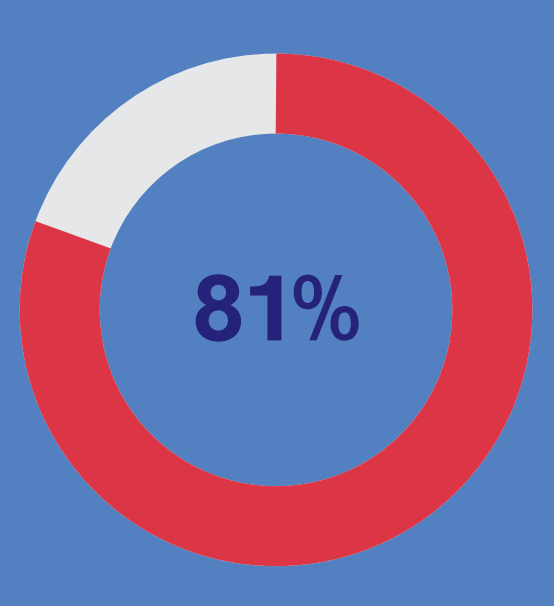
The threat landscape continues to evolve at a faster pace than existing defenses.



of organizations encountered one or more phishing attacks (up from 58% in 2022).[1]

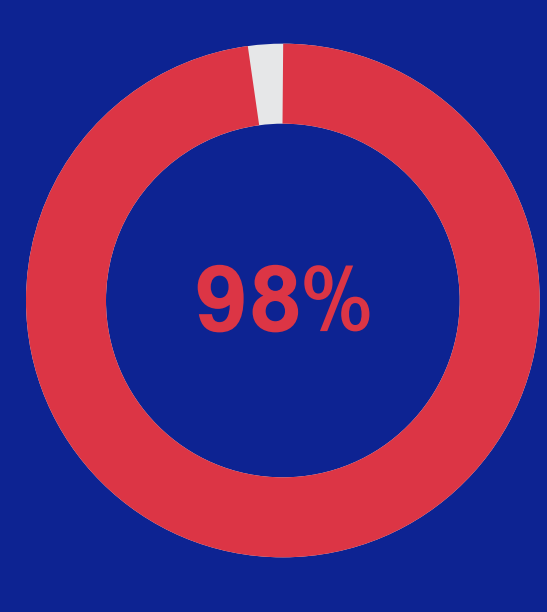


of organizations have faced smishing (SMS phishing) attacks.[2]

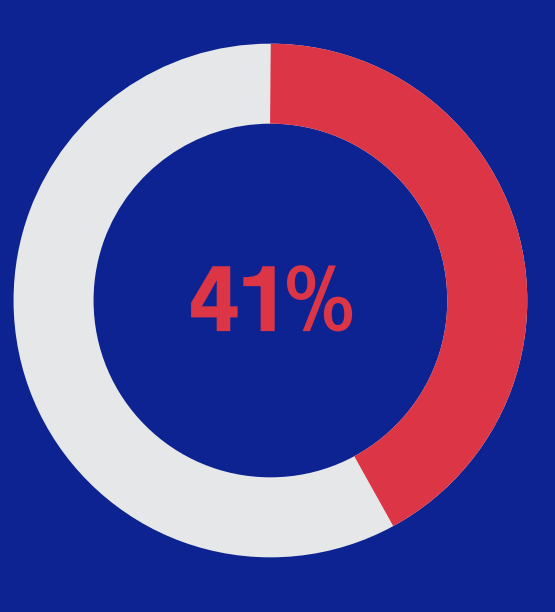


of zero-day attacks were generated by commercial spyware vendors targeting specific victims in 2023.[3]

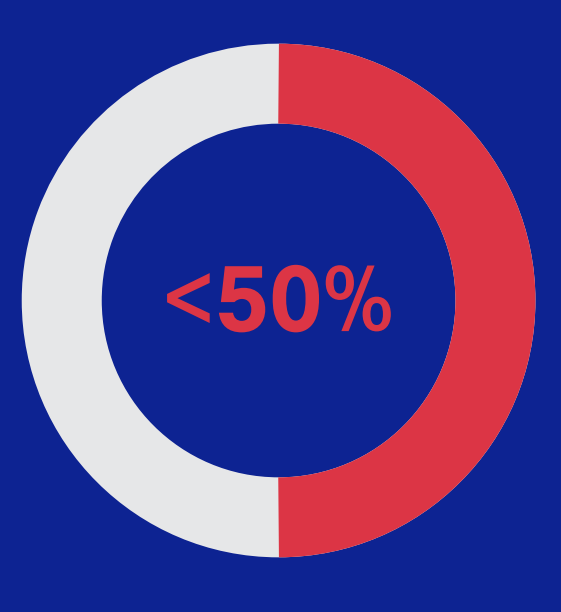
Cyber-threat intelligence (CTI) is now a vital discipline of enterprise cybersecurity programs but the practice is not consistently or effectively applied across the board.



of security managers and practitioners agree that comprehensive threat intelligence is essential for an effective cybersecurity program.[4]



of organizations rate themselves as advanced in threat intelligence practices.[5]



of security organizations today have a dedicated CTI team.[6]

Mature CTI (cyber-threat intelligence) strategies must deliver strategic, operational and tactical insights tailored to stakeholders across the business.

THREE KEY PILLARS OF ACTIONABLE THREAT INTELLIGENCE:

Strategic

WHAT IT IS

Big picture intelligence about what's going on in the cyber-threat landscape, including contextual intelligence about relevant geopolitical happenings, regional or industry vertical concerns and economic motivations that will drive how and why threat actors perform as they do in different scenarios.

WHY IT'S IMPORTANT

Feeds into senior decision-makers to help make better risk management decisions.

Operational

WHAT IT IS

Information obtained by looking closely at TTPs and examining the behavioral patterns of threat groups and ongoing attacks.

WHY IT MATTERS

Help incident responders prep for faster response times and establish high-value preventative measures.

Tactical

WHAT IT IS

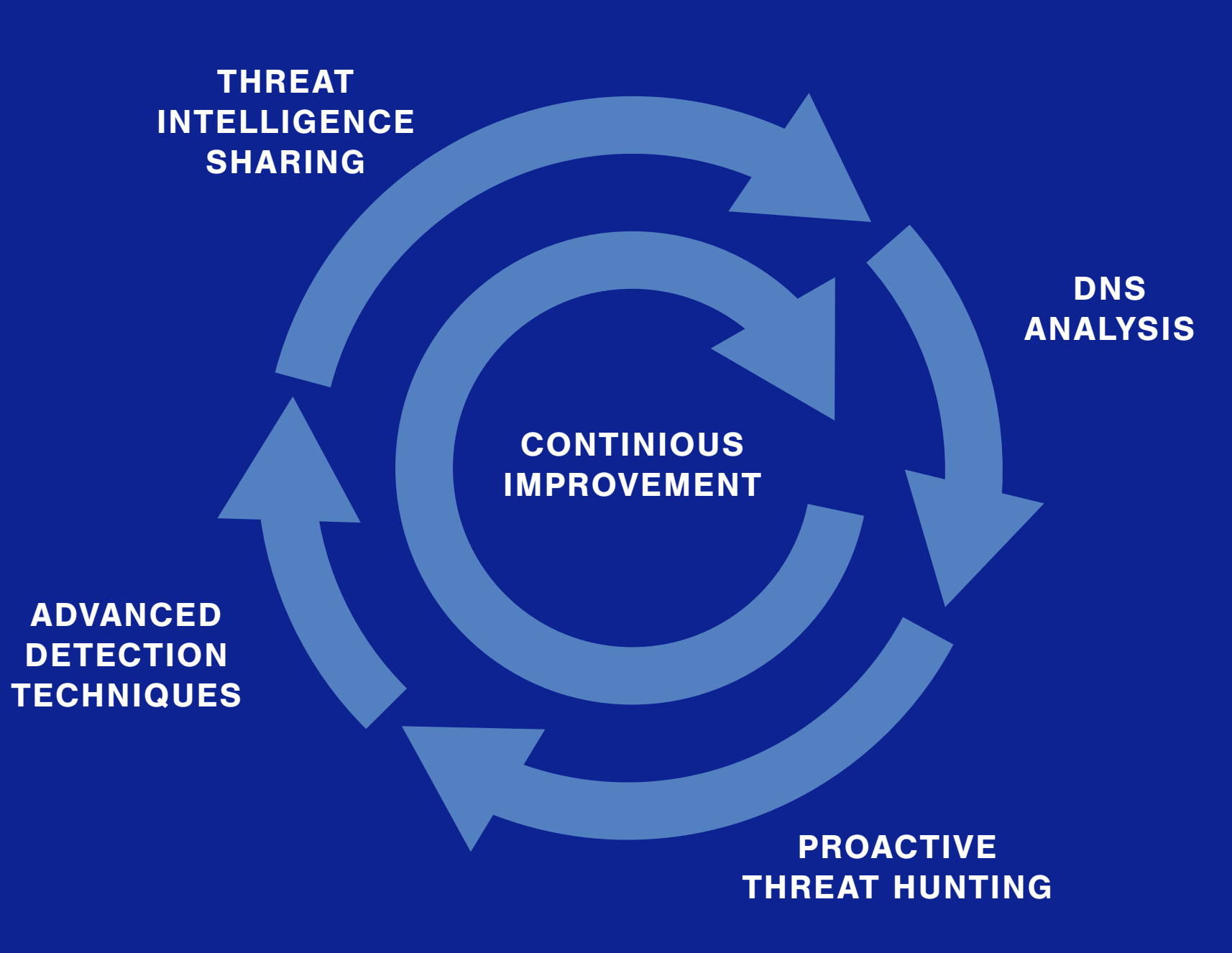
Data coming from active DNS threat hunting, malware analysis and evidence of malicious behavior spotted by automated systems monitoring.

WHY IT MATTERS

Aid in identifying, mitigating and responding to immediate threats.

PROACTIVE THREAT HUNTING

Infoblox's threat hunting approach focuses on identifying threats by analyzing DNS traffic, registrar activity and other resources for patterns. Key aspects of that process are:



DNS ANALYSIS

Leverage both DNS and security expertise to analyze suspicious domains and DNS queries, including indicators of potential threats before they are weaponized.

PROACTIVE THREAT HUNTING

Trace threat actor infrastructures using Threat Intel insights to monitor and analyze threat actor behavior, which allows security teams to stay ahead of emerging threats.

ADVANCED DETECTION TECHNIQUES

Including everything from reverse engineering and sandboxing to specialized systems to identify lookalike domains, DNS command and control (C2) malware, etc.

THREAT INTELLIGENCE SHARING

Infoblox shares detailed research on specific threat actors and associated indicators of compromise (IOCs) to help others bolster their defenses.

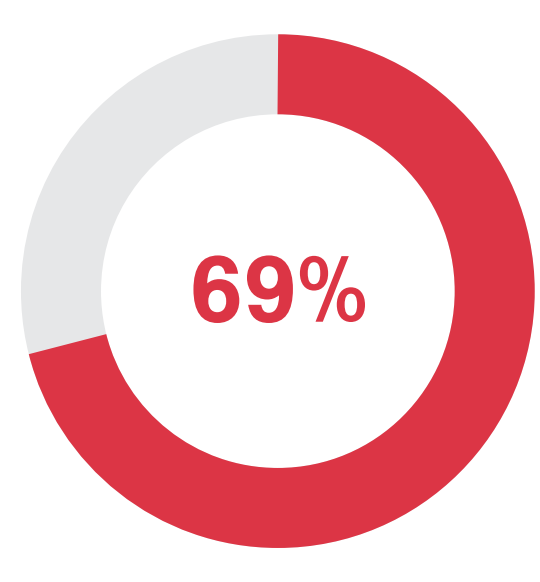
CONTINUOUS IMPROVEMENT

Infoblox Threat Intel is continuously updated with new indicators and behavioral insights to support more robust, current threat detection capabilities.

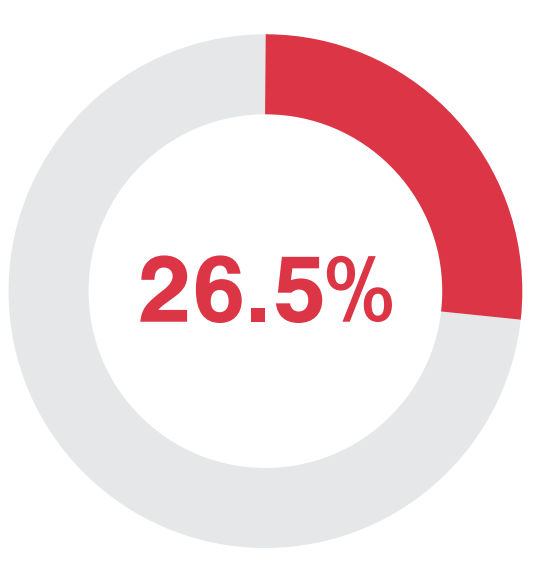
The **Infoblox** Solution

Overall, **92%**[7] of cyber threats can be blocked by DNS. But Infoblox's DNS-based intelligence solution also offers proactive safeguards against threat actors by identifying their infrastructure early and blocking communications to attacker-controlled domains, even before many attacks begin.

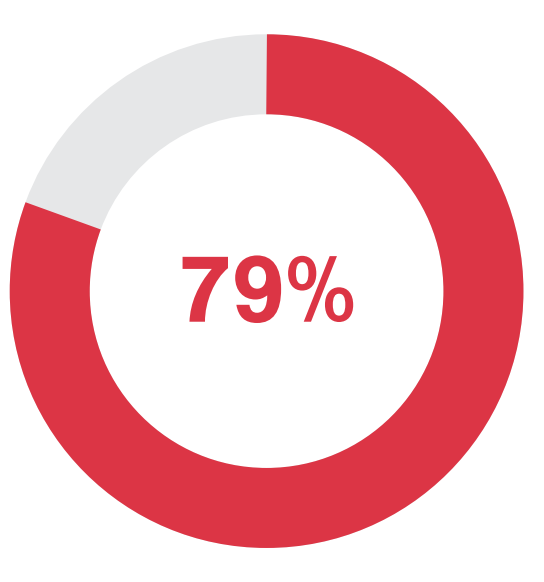
- Infrastructure-based DNS threat intelligence combines DNS expertise with cutting-edge data science at scale
- Streaming analysis on enterprise DNS queries to help detect and block dangerous domains as soon as they are registered
- Correlation of DNS intelligence with network telemetry gives enterprises full visibility over their security operations and dramatically reduces response times



Infoblox solutions lead to **69%** lower staff hours per year through automated cloud network discovery.[8]

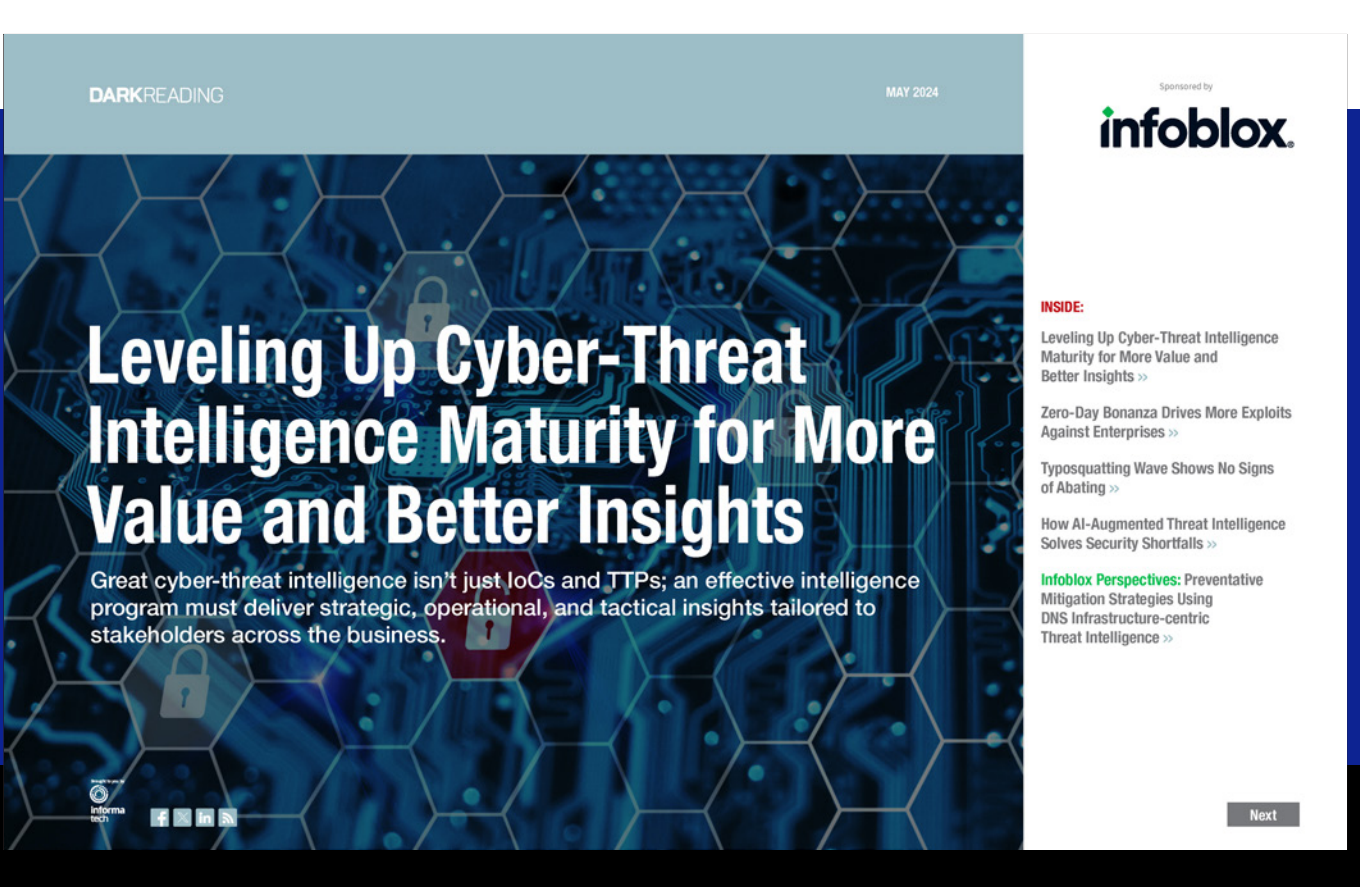


Implementing Infoblox solutions resulted in a **26.5%** reduction in data breaches, audits and fees.[9]



Implementing Infoblox leads to a **79%** reduction in operational costs for a 16-person network security team.[10]

GET THE FULL REPORT ↗



DARKREADING infoblox

1. Infoblox & CRA Business Intelligence, 2023 Global State of Cybersecurity Study
2. Proofpoint, 2024 State of the Phish
3. Google Threat Analysis Team, "Buying Spying: How the commercial surveillance industry works and what can be done about it", 2024
4. Recorded Future, 2023 State of Threat Intelligence
5. Recorded Future, 2023 State of Threat Intelligence
6. SANS, 2023 CTI Survey: Keeping Up with a Changing Threat Landscape
7. https://executivegov.com/2020/06/anne-neuberger-on-nsas-secure-dns-pilot-program/
8. https://www.tolly.com/publications/detail/222110
9. https://info.infoblox.com/resources-analyst-reports-2023-the-total-economic-impact-of-infoblox-ddi