IDC

2023 Global DNS Threat Report

# Augmenting Cyber Threat Intelligence

## Proactive Detection and Early Threat Response with DNS Observability

AUGUST 2023

Romain Fouchereau
Research Manager
European Security, IDC

InfoBrief sponsored by

efficient iP®

# Contents

# Executive Summary

Organizations are facing an ever-growing number of more sophisticated cyberattacks. As a result, they increasingly recognize the importance of utilizing threat intelligence and zero trust principles as part of their overall security strategies.

In this context, DNS threat intelligence data is being acknowledged as an extremely valuable and actionable source of information for organizations looking to strengthen their cybersecurity defenses.

**90%** ↑ experienced one or more DNS attacks

**$1.1m** ↑ the average cost of an attack

**7.5** ↑ attacks on average per organization in the past 12 months

**73%** ↑ suffered app downtime (cloud and in-house)

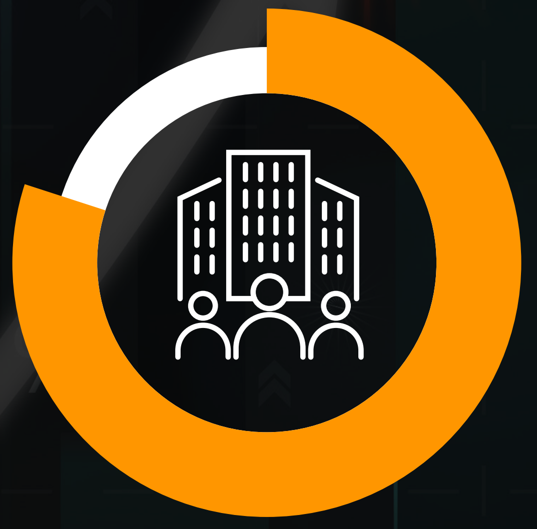
**54%** ↑ were victims of phishing attacks

**32%** New were subjected to ransomware attacks

**29%** ↑ had data stolen as a result of an attack

**60%** New view threat intelligence as crucial for security

**Awareness of DNS security is rising**



↑

**80%** of organizations see it critical to business, but only **21%** today make use of DNS data as a source for their threat intelligence

**The impact caused by DNS attacks is real and ever-increasing, so the time to act is NOW!**

**Enterprises need to consider DNS security end to end and evolve their security infrastructure to achieve a holistic and more integrated approach.**

**Consolidating DNS threat intelligence and observability across the security ecosystem enables proactive defense, reduces cyberthreats, and enhances protection.**

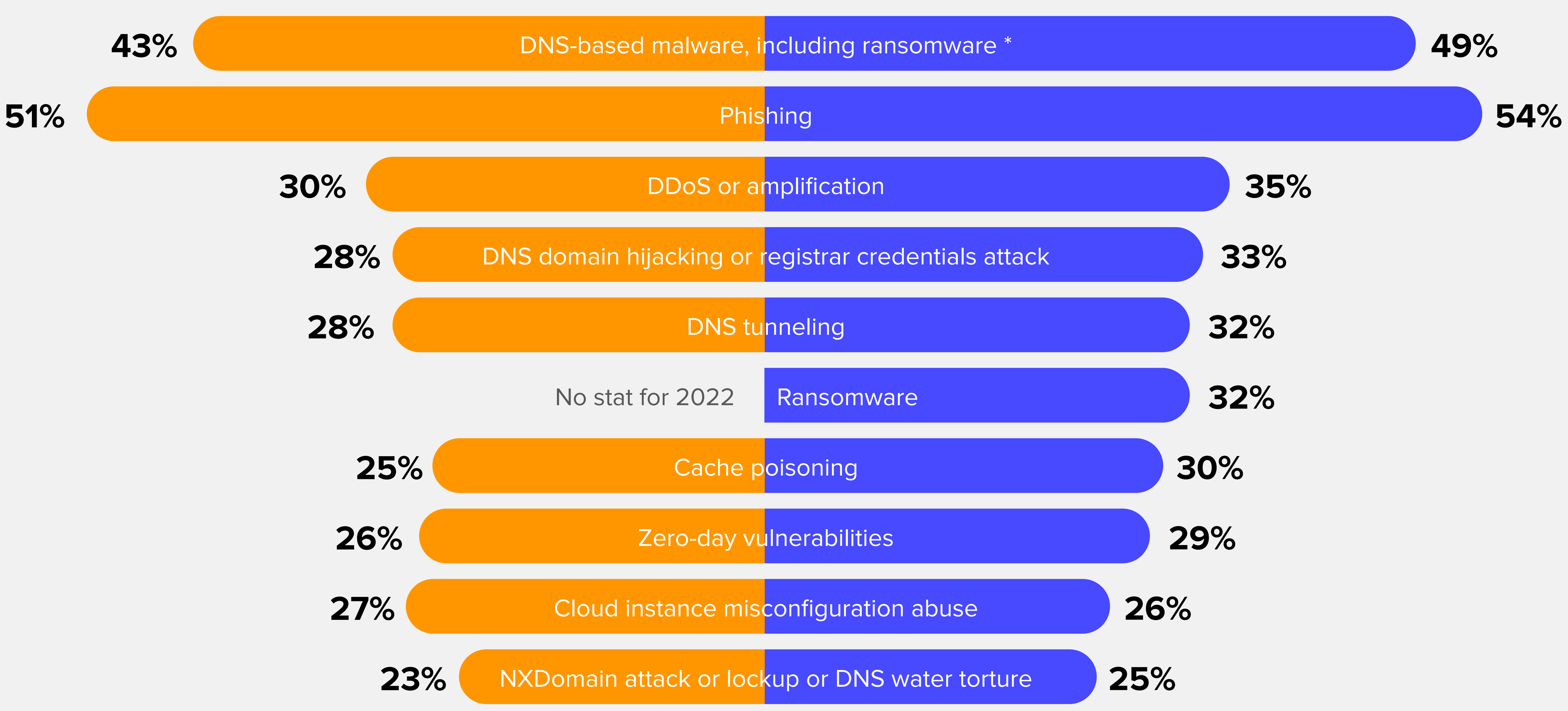
Romain Fouchereau, Research Manager, European Security, IDC

**By leveraging DNS threat intelligence data, organizations can gain deeper insights into potential threats and take proactive steps to mitigate risk, making DNS a key component of any comprehensive cybersecurity strategy.**

# Threat Landscape

Considering the essential role of DNS in the functioning of the Internet and the enterprise network, as well as its potential as a vector for the most dangerous cyberattacks, organizations need to prioritize DNS security as part of their overall cybersecurity strategy.

## Top DNS-based attacks



Attack sizes remain high

**90%** experienced an attack

**7.5** attacks on average

**51%** over 5Gb/s

### Ransomware:

A trend in ransomware is the use of multi-extortion: Attackers not only encrypt the data but also threaten to leak sensitive information if the ransom is not paid. This tactic is particularly effective against organizations that store large amounts of sensitive data, as the potential damage from a data breach can be much greater than the cost of paying the ransom.

**The expansion of the threat landscape and the increasing sophistication of cyberattacks mean organizations need greater visibility and control over network activity. A purpose-built DNS security solution will enhance the security posture and help prevent data breaches and other cyberthreats, while actionable DNS data can be leveraged for threat intelligence.**

*The result for 2023 is an aggregate of ransomware and other DNS-based malware.

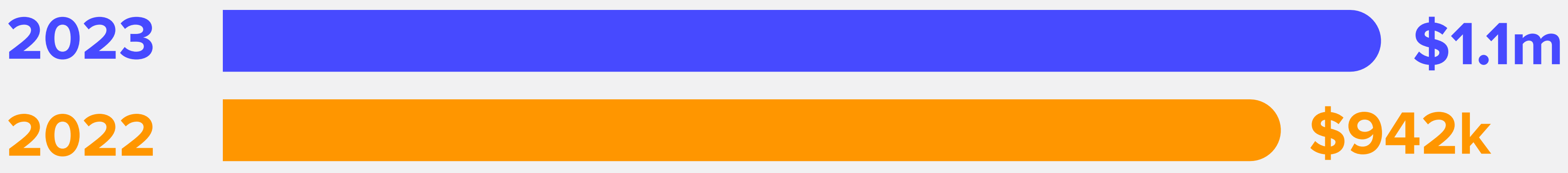
# Impacts and Cost of DNS Attacks

A DNS-based cyberattack can have significant impacts in both the short and long term.

In the immediate aftermath of an attack, an organization may experience downtime or loss of productivity as a result of systems being taken offline or employees being unable to access important data or applications, leading to revenue loss, missed deadlines, reputational damage, and regulatory fines.

Long-term impacts on an organization include damage to brand reputation, loss of customers, and decreased market share. Moreover, a successful attack can result in the theft of sensitive data, including intellectual property or financial information, which can lead to further financial losses or legal liabilities.

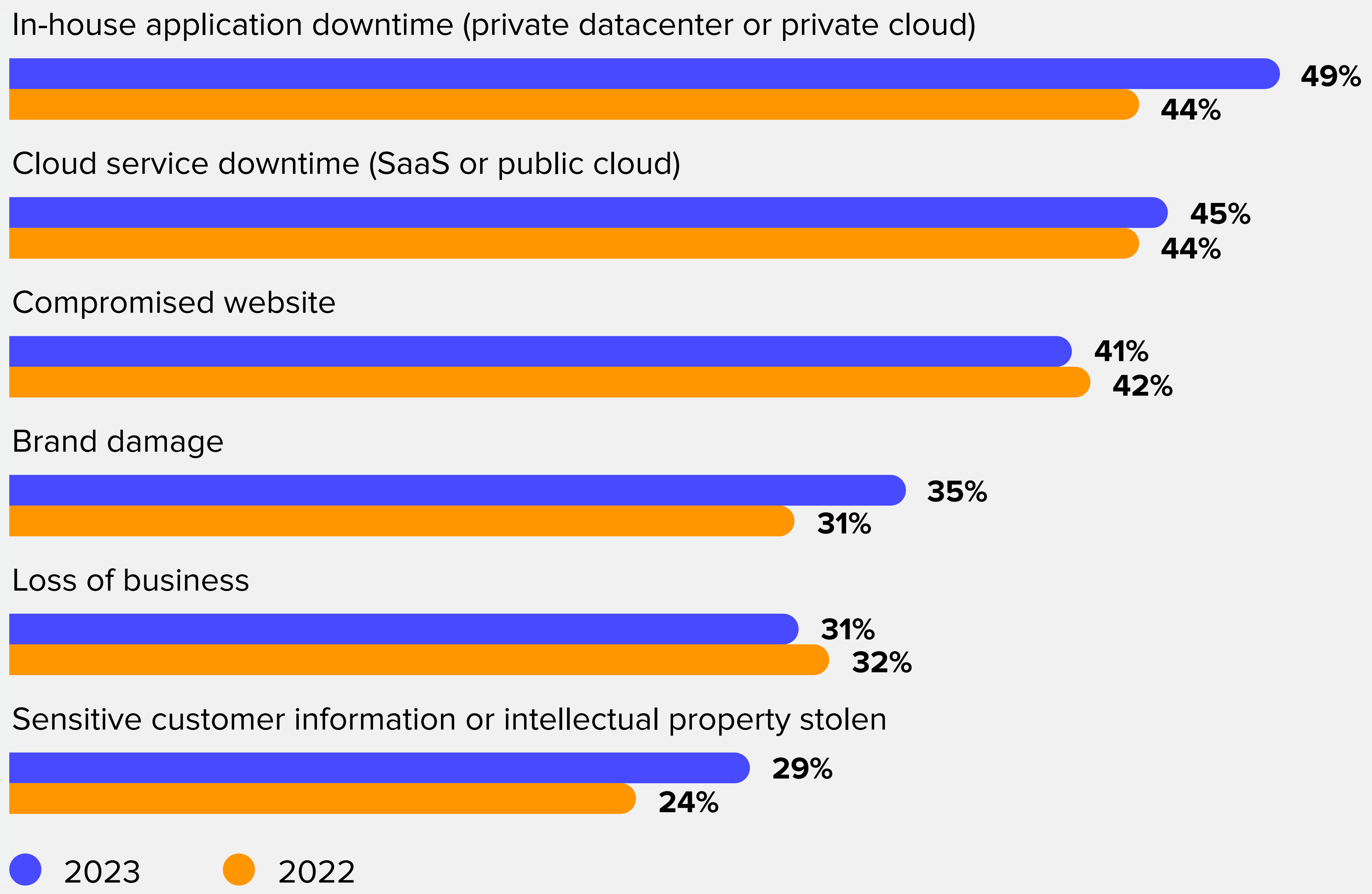
## Average cost of an attack*:



Consolidated application downtime (in-house applications and cloud services)
**73%** against **70% in 2022**

Data theft:
**29%** against **24% in 2022**

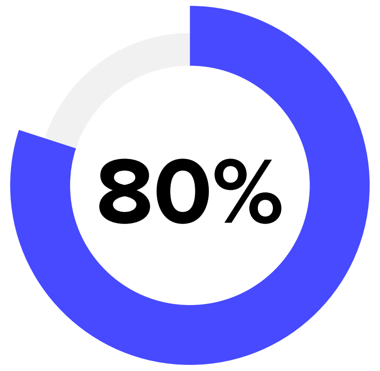
## Impacts of DNS-based attacks



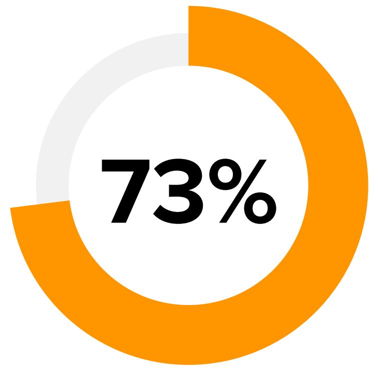
*The cost includes cost of mitigation, full-time-equivalent (FTE) hours spent, and business damage

# State of Defenses

## Awareness of DNS security is at an all-time high with organizations deeming it critical



in 2023



in 2022

The average time to mitigate an attack remains high, at

**5h 59 min**

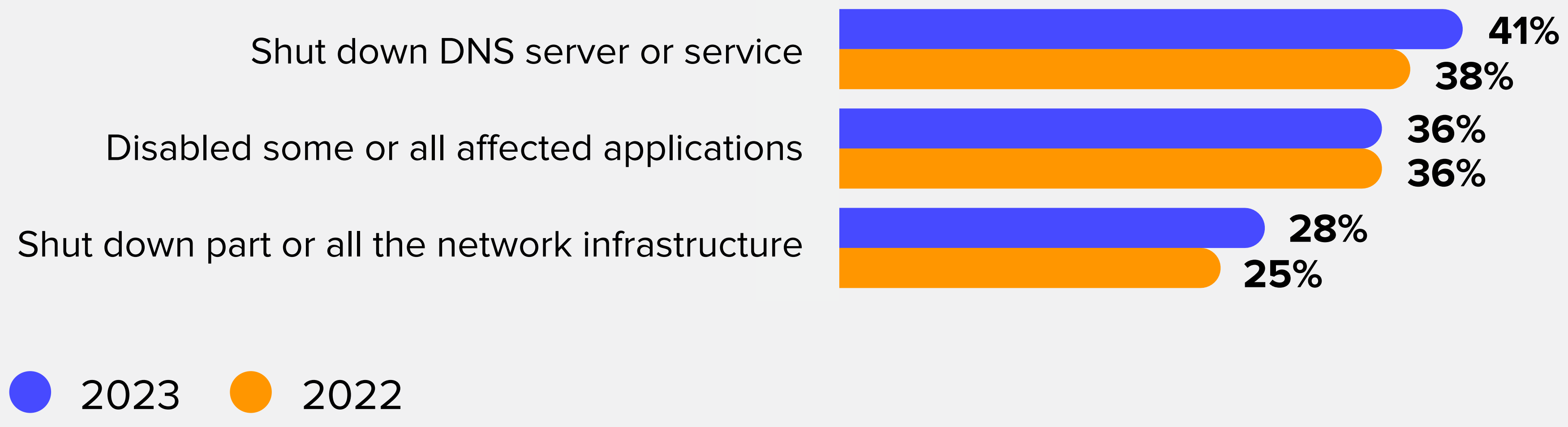
**99%**

of organizations have some DNS security in place

**31%** still do not leverage the added business continuity, data protection, and user protection benefits from a specialized security solution built into a DNS server.

## Business Continuity

This year's results show that unsuitable countermeasures taken to mitigate the effects of the DNS attacks are negatively impacting business continuity and are on the rise.



**59%**

still do not use auto-remediation from an existing security solution for attack mitigation to ensure security of services

## Valuable DNS data is being underutilized

**36%** don't collect or analyze their DNS data. DNS traffic analysis can provide many benefits: early detection of threats, real-time threat intelligence, proactive threat hunting, improved incident response, and better visibility into network activity.

**79%** do not yet make use of DNS data as a source for threat intelligence.

**To truly protect against cyberthreats, organizations need a DNS service capable of performing robust security tasks in real time: protection against malicious domains, as well as protection of users, applications, and data with an assurance of full service continuity. In addition, DNS is a critical source for threat intelligence, providing insights into suspicious domain names, IP addresses, and other indicators of compromise.**

# All Industries are Targeted: Disruption for Businesses and People

## Potential Impacts

**FINANCIAL SERVICES**

Highest average cost per attack, at
**$1.2M**

Attacks can disrupt financial services, such as payment processing and transactions, which can have widespread impacts on the broader economy.

**RETAIL**

Highest data theft, at
**33%**

Retailers may face financial losses and regulatory fines due to fraudulent charges, causing reputation damage and loss of customer trust.

**TELECOMS AND MEDIA**

Most attacked, at
**94%**

The interruption of critical and essential services, such as voice, data, and video communications, impacts customer satisfaction and increases churn.

**HEALTHCARE**

Highest in-house app downtime, at
**59%**

Disruptions to services, such as patient monitoring, diagnostic imaging, and medication dispensing systems, can lead to potential harm or loss of life.

**EDUCATION**

Highest phishing rate, at
**61%**

Compromised research data, academic journals, and patents can have long-lasting impacts on the institution's research capabilities, competitiveness, and funding opportunities.

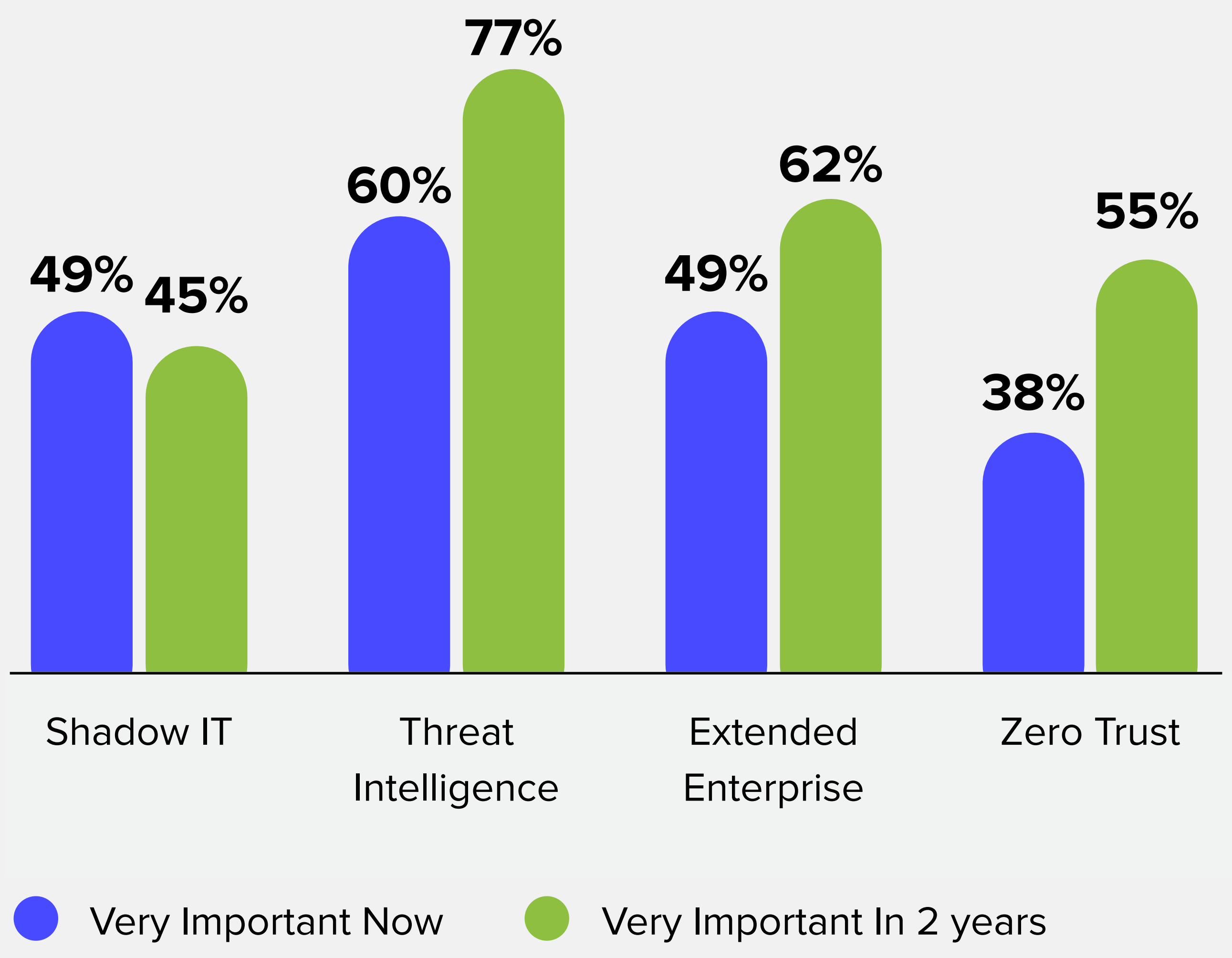
# All Industries are Targeted: Disruption for Businesses and People

| | | Potential Impacts |
|---|---|---|
| **GOVERNMENT** | Highest cloud service downtime, at<br>**50%** | Service disruptions and an inability to access public services (e.g., to pay taxes, obtain permits, or access important documents) cause inconvenience and frustration among citizens. |
| **UTILITIES** | 2nd highest brand damage, at<br>**42%** | Loss of trust can lead to customer churn, with customers switching to providers they perceive as more secure and reliable. |
| **MANUFACTURING** | Highest for disabling affected applications, at<br>**43%** | Process disruptions in production-line and supply-chain-management systems cause manufacturing interruptions, decreased output, delays, and revenue losses. |
| **TRANSPORTATION** | Highest victims of distributed denial of services (DDOS), at<br>**41%** | Compromised traffic management systems cause traffic accidents and delays; disrupted public transportation systems cause chaos, accidents, and injuries/fatalities. |
| **BUSINESS SERVICES** | 2nd longest time to mitigate attack, at<br>**6.5 hours** | Employees being unable to access the tools and resources they need to work effectively negatively impacts business productivity. |

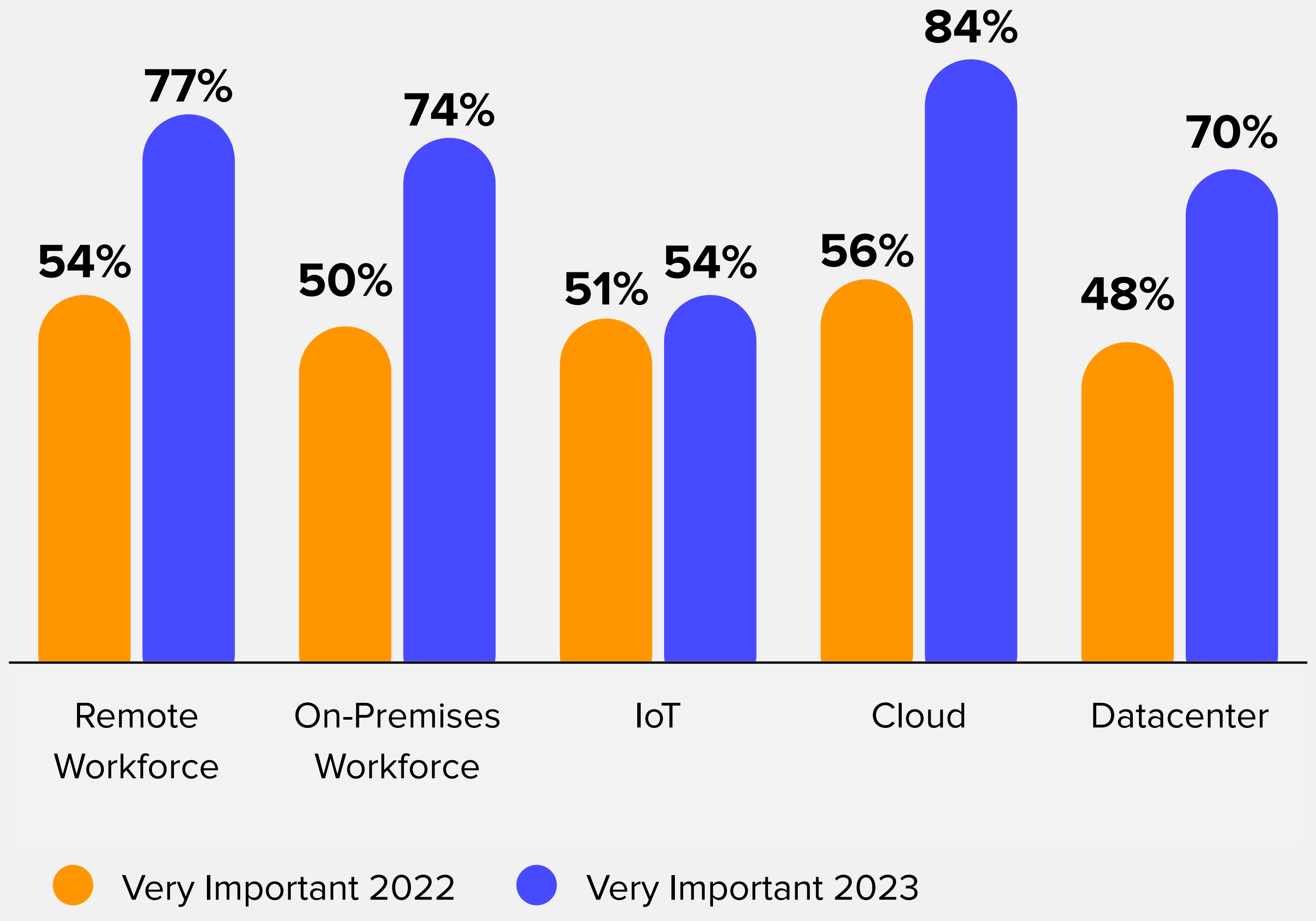
# Security Strategies for Organizations: Where DNS Fits

Given the evolving threat landscape and diversity of infrastructure, organizations need to evolve their security infrastructure and adopt a more holistic, risk-based, and integrated approach. In their strategy, they need to embrace all aspects: diversity of infrastructures and devices, diversity of workers, any upstream sources of data, and strengthening their security posture with more integrated and complementary models involving zero trust and SASE.

## Importance of DNS in organizations' security strategy



## Importance of DNS as a component of the overall security



**DNS plays an important role in the implementation of various security concepts, helping to protect organizations against the threat landscape and ensure the security of their resources: users, devices, applications, and services.**

## Where DNS Fits in Key Strategies

**Threat intelligence:** DNS can be used to monitor for and block access to known malicious domains, helping to prevent malware infections and other types of cyberattacks.

**Zero trust and zero trust network access:** DNS can be used to provide secure access to company resources by using DNS-based security controls to ensure that only authorized users and devices are allowed to access those resources. This includes micro-segmentation, controlled by DNS-based policies, to allow fine-grained access control.

**Secure access service edge (SASE):** DNS can be used as part of a cloud-based security solution to provide secure web gateway services, such as URL filtering and content inspection.

**IoT devices:** DNS can be used to manage and secure IoT devices to access only its backend resources using allow-list filtering.

**Datacenter and cloud:** DNS can be leveraged in application access control, service continuity protection, and threat detection.

# Augmenting Threat Intelligence for Proactive Defense

Threat intelligence has emerged as a pivotal aspect of cybersecurity defense, with 60% of organizations considering it vital to company strategy and defense against cyberattacks. The reasons are many and varied: Cybercriminals are monetizing successful attacks through various means, including ransomware, strategic data leaks, damage to brand reputation, and the sale of intellectual property, highlighting the need to analyze their motivations and objectives — their intent. By observing the patterns and actions exhibited by threat actors — their behavior — organizations can enhance their ability to proactively detect and mitigate threats.

## Top 3 attack types benefiting from threat intelligence for mitigation:

| | |
|---|---|
| 57% | DNS-based malware |
| 55% | Phishing |
| 51% | Ransomware |

## Actionable DNS data as a source for threat intelligence is regarded as valuable but is being underutilized:

**21%** use it now

**30%** plan to use it in 2 years

### Threat intelligence benefits expected from the collection of actionable DNS data:

| | |
|---|---|
| 77% | Better malware detection |
| 75% | Improved phishing detection |
| 75% | Better ransomware detection |
| 54% | Improved access control to apps and data |

Cyber threat intelligence feeds, built from AI-powered algorithms applied to DNS data, can help accelerate early detection against threats, such as domain generation algorithms (DGA) and phishing.

**22%** of respondents leverage threat intelligence coming from open source or third party vendors as part of their DNS filtering rule management.

> **DNS can provide organizations with valuable threat intelligence capabilities by analyzing DNS traffic for patterns and indicators of compromise.**
>
> **For an effective threat intelligence strategy, making use of a DNS threat intelligence feed is a no brainer.**
>
> Romain Fouchereau, Research Manager, European Security, IDC

**By utilizing a specialized DNS-centric threat intelligence solution, organizations can gain valuable insights into suspicious network traffic, empowering them to proactively defend, detect, and effectively respond to threats and stay ahead of emerging threats.**

# The Critical Role of DNS for Extended Enterprises

Securing modern IT environments requires addressing challenges related to complexity (number of devices, applications, data types, and network architectures), scale (of cloud deployments and IoT), visibility (numerous devices and endpoints generating vast amounts of data), and access control (cloud services, IoT devices, and remote and roaming workers). Organizations must implement and enforce robust, consolidated security policies and controls across the extended enterprise to mitigate these challenges and ensure that their applications, services, users, and IT environments remain secure.

## Critical Role of DNS in the Extended Enterprise: 2023 vs. 2022

### Hybrid workforce

DNS is critical in securing:

**Remote workforce**

77% | 54%

**On-prem workforce**

74% | 50%

In addition to VPN and firewall, 45% consider a private encrypted DNS solution to be useful for protecting apps and services while making them accessible to remote workers.

### IoT

DNS is critical at securing:

**IoT**

54% | 51%

51% think DNS is very/extremely valuable for improving IoT security by filtering IoT device access (allow/deny) to specific apps.

### Cloud

DNS is critical at securing:

**Cloud**

84% | 56%

45% suffered cloud service downtime as a result of a DNS-based attack. 26% were victims of cloud configuration abuse. Cloud continuity and resilience is vital for business.

### Datacenter

DNS is critical at securing:

**Datacenter**

70% | 48%

Datacenters are high-value targets due to the vast amounts of sensitive data they store and the critical infrastructure and services they provide to organizations. Risk of unauthorized access or intrusion can lead to data theft and network disruption.

**Private enterprise DNS security brings significant benefits to the extended enterprise by providing comprehensive visibility and control over network traffic. Organizations can protect their data, users, and assets from advanced threats with the same policies and security features, regardless of where they are located.**

# Zero Trust: Lessons Learned

Zero trust (ZT) is adopted to counter modern cyberthreats through a proactive approach to security, based on least privilege access. When implemented correctly with a multi-layered defense strategy, a ZT model delivers robust security and strengthens a business's cyber-resilience by allowing only verified users with authorized devices to access resources at all times.

ZT and SASE complement each other: ZT provides access control security, while SASE offers network architecture to implement and enforce ZT policies. Combining the two creates a security model that provides secure access to applications and data, addressing the security challenges of a distributed and remote workforce and the increasing use of cloud-based applications and services.

However, ZT adoption faces complexity challenges due to sprawling IT estates, legacy technologies, multiple security vendors, and disparate cloud platforms. **DNS offers simple steps to start a zero trust journey**.

### Adoption of zero trust: top of mind but difficult

**36%** are currently running or piloting ZT vs. **29%** last year. Growth is slow, as organizations are struggling with sprawling IT estates, legacy systems, multiple security vendors, disparate cloud platforms, and a lack of resources.

### Management complexity is a hindrance

Despite some improvement, **54%** of organizations (**66%** last year) are still not satisfied with the management complexity of their security solutions in terms of preventing the lateral propagation of threats.

### Improving application access control

**58%** make use of granular DNS access control and filtering to help enforce security policies and restrict access to sensitive data and applications, thus reducing the attack surface and minimizing the risk of breaches and attacks.

**RECOMMENDATION:**

### DNS offers an easy starting point on your path to zero trust

DNS provides additional layers of security, visibility, and control over network traffic. Implementing the principle of "never trust, always verify" provides early access control and threat detection and a natural first line of defense.

Network segmentation based on access policies enables malicious code, executable files, and other security breach factors to be virtually isolated and blocked from lateral movement when a network segment is compromised.

**DNS security tools are essential for implementing a zero trust security strategy, particularly around flexibility and provisioning. Implementing these tools provides quick and pragmatic steps toward access control to ensure that only authorized users, devices, and applications are allowed to access sensitive resources. Start your zero trust journey using DNS.**

# End-to-End Defense: DNS Role in the Security Ecosystem

Organizations are taking a more proactive approach to security by identifying potential threats and vulnerabilities in advance and implementing measures to prevent them.

Moving from reactive to proactive defenses requires an integrated approach to security. DNS is a fundamental component of that approach, particularly when valuable DNS data is shared with security systems like security information and event management (SIEM) or security orchestration, automation, and response (SOAR) via Open APIs.

## SOAR

Very strong adoption of automation for network security policy management: **66%** are using mostly automated solutions (**60%** last year).

## SIEM

**20%** of organizations share DNS data with SIEM for analysis; **24%** plan to in 2 years time

**Thanks to APIs, valuable DNS insights can be used to implement security policies, automate security responses, and integrate with SIEM, SOAR, and the entire ecosystem to improve security operations center (SOC) efficiency. Organizations can then achieve a more integrated and holistic security infrastructure, driving end-to-end protection of their systems, devices, and data from cyberthreats.**

## Empowering SecOps and NetOps

Organizations use actionable data for observability, monitoring, prevention, and remediation:

**78%** of organizations already leverage DNS telemetry to share data and security events with the SecOps team, **29%** of which as a fully automated process.*

This fosters collaboration between NetOps and SecOps teams, resulting in a more efficient and effective security ecosystem.

## Best practices for making DNS data actionable include:

- Regularly analyze DNS data to identify traffic anomalies
- Fuel security tools with DNS data
- Ensure DNS data is always accurate and up-to-date
- Securely store and make DNS data accessible only to authorized people
- Build a plan for automating incident response

*2023 Global Network Automation Report

# DNS for Earlier and Enhanced Detection of Ransomware

Ransomware is an ever-evolving threat that continues to adapt and become more sophisticated over time. In recent years, ransomware attacks have become more targeted to maximize profits and cause brand damage.

**32%** of organizations have been victim of a ransomware attack

**85%** of malware actors are using DNS to develop their attack, making DNS a foundational component of an effective threat intelligence strategy for any organizations

**51%** of organizations believe they would benefit from threat intelligence against ransomware

## DNS is instrumental in detecting and responding to ransomware attacks in real time

**DNS traffic analysis** helps identify unusual patterns of traffic, unveiling for instance zero-day malicious domains used for data exfiltration by ransomware.

**54%** of organizations use or are considering using DNS security for ransomware and malware protection.

**75%** of organization say they would benefit from actionable DNS data — which they currently lack or struggle to collect — for protection against randsomware.

**DNS filtering** is an effective way to block access to known malicious domains and prevent ransomware from communicating with its command and control (C&C) servers, thwarting the attack before it can cause any damage. DNS filtering can also be used to block access to known phishing sites, which can help prevent ransomware attacks being initiated in the first place.

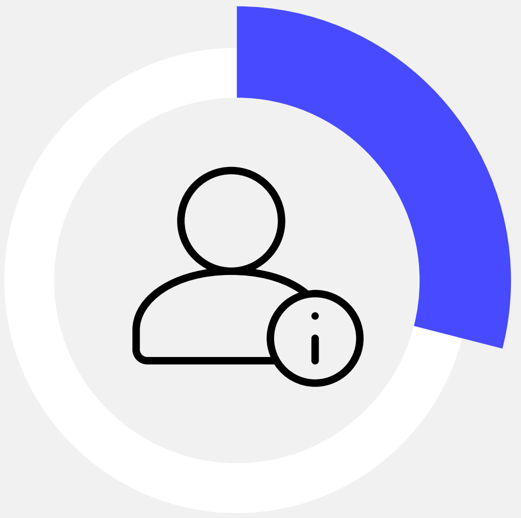
**49%** of organization believe threat intelligence is important for DNS filtering capability against ransomware.

**By using DNS traffic analysis and filtering in conjunction with other security technologies, organizations can detect unauthorized access attempts and respond to ransomware attacks quickly, minimizing potential reputation damage and reducing the risk of financial loss.**

# Handling Stricter Regulatory Compliance, Data Privacy, and Theft

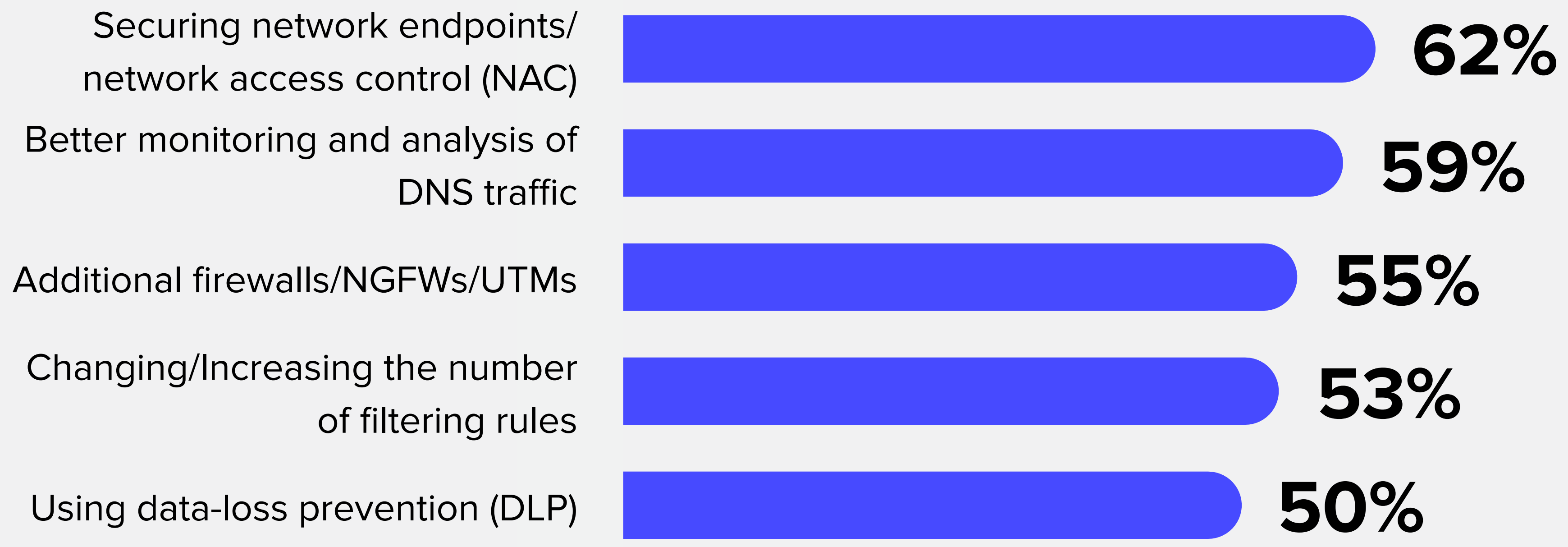
The state of data protection and compliance is a complex and constantly evolving landscape, and organizations must stay up to date with the latest regulations, standards, and best practices to protect their data and maintain compliance. Regulations on data protection and privacy, including GDPR, CCPA, and NIS2, are multiplying and becoming increasingly strict, reflecting the growing concern over global cybersecurity threats and data breaches.

## Rise of data theft via DNS attacks



**29%** of organizations had sensitive customer info or IP stolen vs. **24%** last year.

## Most effective actions to prevent data theft



**59%** of respondents report that DNS security can help prevent data exfiltration by detecting improper DNS flow and blocking related traffic. DNS is a specialized layer of defense complementing security systems to strengthen data protection.

## Data privacy

**45%** of organization consider using DNS over HTTPS (DoH) with a PUBLIC or free provider to be a privacy risk

**48%** of organization are using or considering setting up a private DoH solution to limit risk

Private DoH helps with data privacy by encrypting DNS traffic and preventing unauthorized access to DNS data, which means queries and responses cannot be intercepted and monitored by anyone with access to network traffic.

**Regulations and compliance are becoming stricter, with new acts being introduced to address the increasing threats to data privacy and security. DNS is a valuable tool for helping organizations achieve regulatory compliance by providing domain filtering, data privacy, logging and analysis, and compliance reporting on DNS traffic, thus boosting security overall.**

# Visibility and Observability to Detect Ungoverned Network Activity

Visibility and observability challenges arise from the complexity and scale of modern networks and the evolving threat landscape. Modern networks often consist of multiple cloud and on-premises environments, making it challenging to gain a unified view of network activity, leading to blind spots and gaps in visibility, which can be exploited by attackers.

**50%** **of organizations expect to gain visibility into all connected assets with insightful DNS data.**

DNS can be used to detect unauthorized developments or use of resources, such as rogue databases or unapproved cloud services. By monitoring DNS traffic, IT and security teams can detect and block unauthorized access or use of resources, ensuring that the network remains secure and compliant.

In cloud environments, where resources are often dynamically provisioned and scaled, DNS helps maintain visibility into the network. Without DNS, it would be difficult to discover and track the various services, containers, and virtual machines that make up a cloud environment.

## Comprehensive visibility encompasses multiple aspects

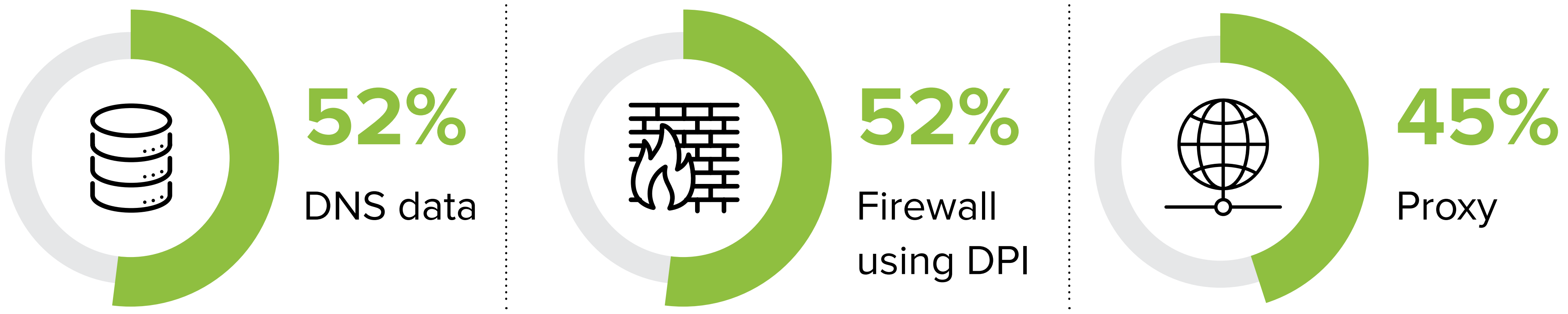
- Load visibility to monitor network traffic
- Performance visibility to optimize network performance
- User and device visibility to track resource usage
- Compliance visibility to ensure adherence to regulations and internal policies
- Security visibility to detect policy and access control violations

## Handling Shadow IT

The detection and management of shadow IT has become a priority for 49% of organizations as part of their security strategy, as such IT can pose significant security and compliance risks and can also lead to inefficiencies and decreased productivity.

Confidence in the detection of shadow IT is improving, with 45% confident with their current detection of shadow IT (39% last year).

## Top solutions used to detect shadow IT:



**DNS is a central component for achieving complete visibility in clouds, devices (including IoT), and applications. DNS serves as a fundamental building block for network data discovery, as it maps domain names to IP addresses, enabling communication between different systems and services. It enables the analysis of user behavior and intent, providing relevant data that can be used to identify and respond to potential threats and ungoverned services.**

# Essential Guidance

Despite 80% of organizations acknowledging that DNS security is critical, investment in DNS knowledge and usage remains worryingly low. Costs and impacts of DNS attacks continue to cause severe damage, year after year. It is therefore time for organizations to take DNS seriously and act now!

Specialized threat intelligence on DNS is needed due to the importance of the DNS protocol in today's threat landscape. To harden network protection, DNS security tools and actionable data need to be better utilized to provide proactive defense and early threat detection, secure connectivity for work from anywhere, and be a simple starting point for zero trust strategies.

## Recommendations

1

**Strengthen your security posture by increasing knowledge of DNS tools and tangible benefits from actionable DNS data**

Using a specialized DNS-centric threat intelligence solution enables organizations to proactively defend, quickly detect, and protect against cyberthreats.

2

**Use DNS to advance your zero trust journey by enhancing access control and micro-segmentation**

Incorporating DNS security tools into a zero trust strategy ensures only authorized users, devices, and applications are allowed to access sensitive resources.

3

**Detect data breaches and ungoverned services earlier with DNS visibility, observability, and smart analytics**

Monitoring and analyzing DNS traffic enhances ransomware or any suspicious network activity detection and ensures regulatory compliance.

4

**Integrate DNS data with the security ecosystem to increase proactivity, automate security response, and accelerate threat remediation**

Evolving to a more integrated and holistic security infrastructure will increase overall efficiency, reduce complexity, and achieve better ROI.

**For a free DNS risk assessment to identify vulnerabilities and improve your protection, click here or visit our website.**

# Message from the Sponsor

EfficientIP is a network security and automation company, specializing in DNS-DHCP-IPAM (DDI). We promote business continuity by making your IP infrastructure foundation reliable, agile, and secure.

Since 2004, we have continued to expand our reach, providing solutions, professional services, and support all over the world with the help of select business partners. Our passionate teams have delivered successful projects to over 1,000 customers globally, and ensured operational efficiency through dedicated customer care.

**Our goal is to enable secure and dynamic IP communication between users and apps/services. We achieve this by:**

- Securing DNS services to protect users, apps, and data, and ensure service continuity
- Simplifying life-cycle management of DDI resources, via smart automation, cross-platform visibility, and policy control through a single pane of glass

Companies rely on us to help control the risks and reduce the complexity of the challenges they face. This applies particularly to modern IT initiatives such as cloud applications, virtualization, mobility, digital transformation, and SDN.

**For more information, visit:**

**www.efficientip.com** and follow **@efficientip** on Twitter.

efficient iP®

# Methodology

Analysis of this InfoBrief is based on a survey IDC conducted on behalf of EfficientIP among 1,000 organizations across the world in early 2023 using computer assisted telephone interviewing (CATI) or computer assisted web interviewing (CAWI) methodologies.

The data collected represents their experience from the previous year.

- A year-on-year comparison was conducted using data from 2022.
- Screener requirements: companies with 500 or more employees; all industry sectors covered with quotas by geography; and target respondents in IT-related functions with decision-making input for security strategies.

## 5 Business Size Segments

**Midsize Enterprise:**

- 500 to 999 employees: **256**

**Large Size Enterprise:**

- 1,000 to 2,499 employees: **216**
- 2,500 to 4,999 employees: **194**
- 5,000 to 9,999 employees: **172**

**Very Large Size Enterprise:**

- 10,000 or more employees: **162**

## 10 Countries

**North America:**

- Canada: **73**
- United States: **230**

**Europe:**

- France: **100**
- Germany: **109**
- Italy: **75**
- Spain: **78**
- United Kingdom: **110**

**Asia:**

- India: **85**
- Malaysia: **70**
- Singapore: **70**

## 10 Industry Sectors

- Business services: **81**
- Education: **103**
- Financial services (banking, insurance, and other financial services): **114**
- Government: **102**
- Healthcare: **102**
- Manufacturing: **111**
- Retail and wholesale: **113**
- Telecommunications and media: **113**
- Transportation: **81**
- Utilities: **80**

Unless specified otherwise, all data in the InfoBrief is based on 1,000 respondents.

# About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data and marketing services company.

## IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

**IDC UK**
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100

@idc | @idc | idc.com

© 2023 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

Privacy Policy | CCPA