2021 Global DNS Threat Report

Elevating Network Security with DNS

Better prevention, risk mitigation and resilience

June 2021

Author:
Romain Fouchereau
Research Manager,
European Security, IDC

IDC #EUR147652021

Sponsored by

efficient iP™

Contents

Executive Summary

Evolution and awareness of DNS security continues to grow, but cost, frequency, and number of attacks remain high. COVID-19 and working from home (WFH) have resulted in huge disruption for organizations. Attacks on infrastructure are at an all-time high — phishing and ransomware in particular. According to the *2021 DNS Security Survey*:

87%

Experienced one or more attack (+8 percentage points compared to last year).

7.6

Average number of attacks per organization in the past 12 months

$950k

Average cost of attack

76%

Suffered application downtime (cloud and/or in-house).

26%

Were the victim of data theft (+10 percentage points).

76%

Deem DNS security critical for their organization

As a critical part of the overall security strategy, DNS is the first line of defense as it sees the intent of virtually all IP traffic. DNS can be used to detect threats, simplify and accelerate mitigation, and enhance trust strategies to protect from data theft and ensure privacy.

> This year's *2021 DNS Security Survey* confirms that nearly all companies have had their apps and services disrupted by DNS attacks. With enterprise boundaries blurring, organizations have added a focus on securing remote workers as well as their on-premises and cloud infrastructure. To meet zero-trust objectives via network segmentation and application access control, the key role of DNS for visibility over client behavior and granular filtering is becoming recognized as vital for preventing the spread of attacks as early as possible in the traffic flow.
>
> **Jean-Yves Bisiaux**
> CTO, EfficientIP

DNS Threat Landscape

DNS remains a prime target for hackers as it enables them to gain first entry into networks and gain access to data for exfiltration:

Rise in organizations that experienced attack:

2021 2020

87% | **79%**

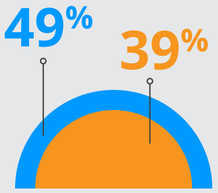
The average number of attacks remains high

7.6 attacks a year

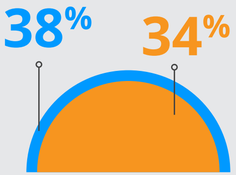
With the pandemic rapidly increasing cloud usage and the number of people remote working, the attack surface has increased considerably. As a result, organizations have suffered more diverse types of attacks than ever before, showing that cybercriminals are using all the tools at their disposal to exploit both the DNS protocol and misconfigurations.

Top DNS-based attacks:

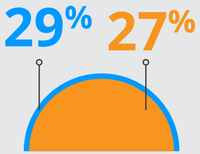
2021 2020



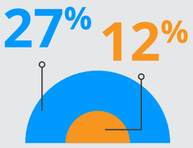
DNS phishing:
remote workers have become phishing targets



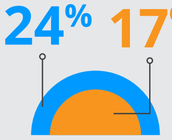
DNS-based malware:
lucrative ransomware as a service is increasingly targeting large organizations



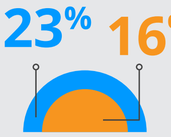
DDoS attacks:
growing intensity and volume



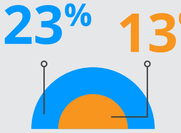
DNS hijacking/ credential attacks:
DNS hijacking attacks targeting home routers



DNS tunnelling:
to achieve command and control inside the protected network



Zero-day vulnerabilities:
expanding targets, new attacks leveraging vulnerabilities on Android and iOS



Cloud instance misconfiguration abuse:
as organizations increasingly migrate to the cloud

Size of DDoS attacks:

54% of attacks were over 5Gb/s

The COVID-19 pandemic has created new challenges for businesses as they adapt to WFH operating models. DX initiatives are accelerated, and cybersecurity becomes a major concern:

- Remote workers fall more for phishing scams
- Vulnerabilities leading to credential stuffing and DNS spoofing
- Use of personal devices for work and corporate PC for personal use
- VPNs not user friendly, using too much bandwidth, creating latency leading to poor user experience
- Reliance on home Wi-Fi and home security

Impacts and Costs of DNS Attacks

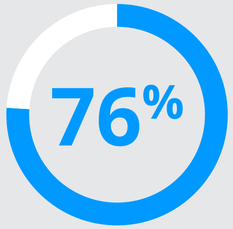
The impact and cost of attacks remain extremely high and continue to increase year over year. This not only affects company finances but also brand image and data confidentiality. With the pandemic, ransomware has increased to become an industry in its own right and a major concern for most organizations. Using DNS filtering and blocking is critical as it can help to stop ransomware attacks right after the infection, when the malware tries to contact command and control (C&C).

Average cost of attacks*

2021	2020
$950k	$924k

Downtime (from in-house applications or in the cloud) remains the most damaging impact of DNS attacks, demonstrating how critical DNS is to ensure resilience and to secure access between users and applications.

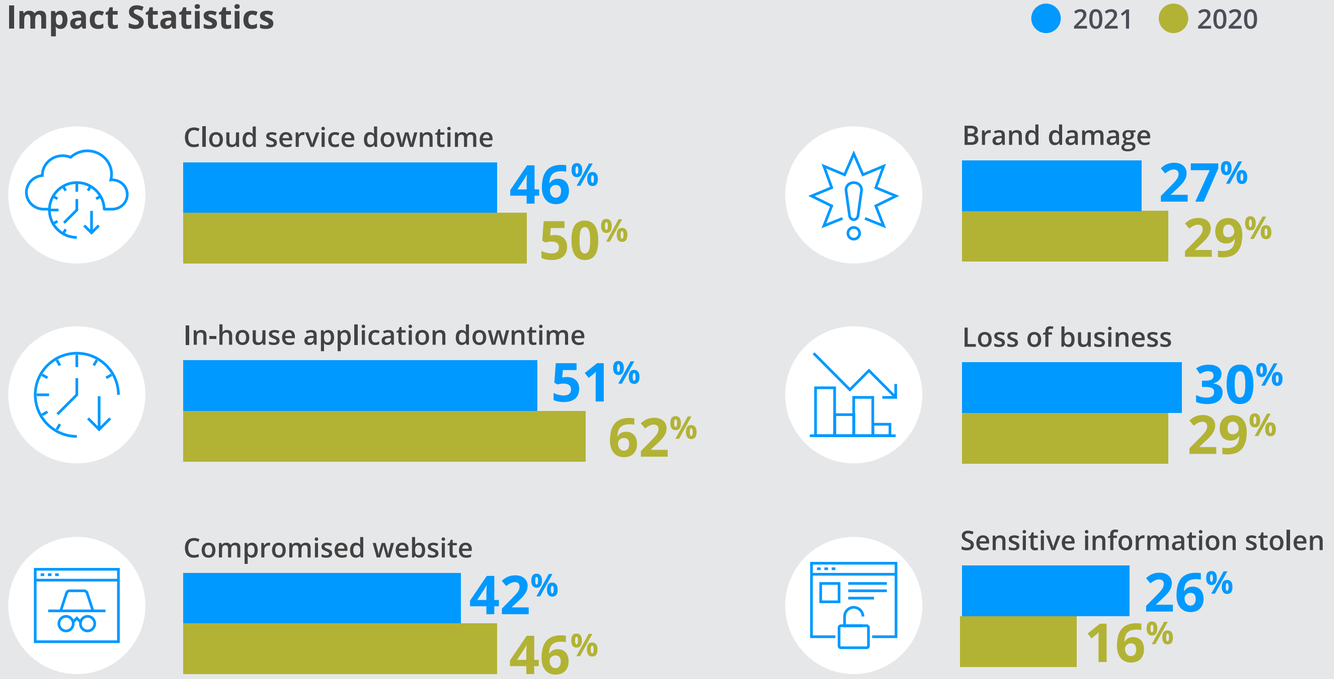
Application downtime**



* Includes cost of mitigation, full-time-equivalent (FTE) hours spent, and business damage
** Consolidation of in-house app and cloud service downtime

DNS attacks and business outcomes are interlinked, and the impacts can directly be measured on the business:

Impact Statistics



Industry View

TELCO

Most targeted industry, averaging 8.6 attacks per telco; Highest customer information stolen via DNS at 29%; 31% suffered brand damage – can lead to high customer churn

FINANCE

High-value opportunities — highest average cost damage per attack at $1.08M; 52% of organizations in the financial sector suffered cloud service downtime as a result of an attack — the highest percentage for all industries

RETAIL

41% of organizations in retail suffered from a compromised website as a result of an attack; they also saw the highest cloud instance misconfiguration abuse (of all industries), at 29%; in retail, online presence and protecting user credentials are critical for business

GOVERNMENT

Safety of citizens and public infrastructures — 44% of organizations shut down network infrastructure to mitigate an attack last year, meaning citizens have no access to apps and services

HEALTHCARE

Highest app downtime 53%, 36% had to shut down part or all of the infrastructure; can be a matter of life or death, especially in the pandemic era

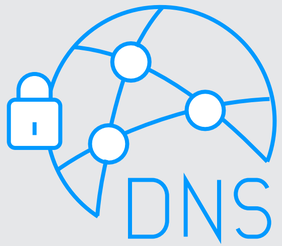
EDUCATION

2020 saw a shift to education at home — 49% had to shut down their DNS server or service as a result of an attack last year, though DNS is vital for access to apps and services, e.g. online tuition and research

State of DNS Defenses

Awareness of DNS security remains high

76% deem it critical for their business



Results of the survey show that

99% of companies say they have some form of security for DNS in place, but many do not benefit from the advantages of purpose-built DNS security (business continuity, data protection, user protection).

Some countermeasures are still not viable as they impact business continuity:

Shutting down part or all of the network infrastructure **36%**

Shutting down DNS server or service **47%**

Disabling applications **38%**

Time taken to mitigate DNS attacks is too long

2021 2020

Average time

5hrs 37mins | **5 hrs 15 mins**

Taking over 7 hours

23% | **21%**

DNS can provide very valuable information to make security strategies more proactive, but 25% of organizations don't collect or analyze their DNS traffic. DNS analytics should play a key role in securing any new strategic IT initiative such as cloud, SD-WAN, IoT, or edge.

The maturity to ensure security of services is rising

42% are using auto-remediation versus only 25% last year.

Although DNS security is established as a critical component of the overall security strategy, and almost all (99%) organizations have a solution in place, **42%** are not yet using a dedicated DNS security solution to help them fill the potential vulnerability gaps left by traditional network security products.

Zero Trust? Not Without DNS Threat Protection

Users expect to work on any kind of network, using any kind of device, and access all the data and applications they need to work. The zero-trust approach relies on valuable and accurate data and deployment of intelligent security enforcement engines. For this, monitoring and analysis of user behavior and controlling access to apps and services are vital.

DNS has the potential to analyze client behavior and make decisions to control User Behavior Analysis (UBA) and filtering. By providing valuable insights and analytics for threat detection, DNS addresses the risks and reduces the complexity and challenges that organizations face with IT initiatives such as zero-trust architectures.

Maturity of Zero Trust:

Zero-trust implementations have changed little over the past year (the focus might have been more on resilience and secure remote working enablement), but more organizations have moved to the planning stage:

Implementation:

2021	2020
32%	31%

Planning implementation

2021	2020
43%	38%

Not yet explored

2021	2020
25%	31%

UBA:

Organizations are realizing that effective threat detection requires internet DNS domain filtering built using internally compiled lists as well as external feeds.

Threat intelligence:
make use of internal DNS traffic analysis

2021	2020
70%	65%

Application access control:

Network segmentation of user groups, mapped to allow/deny domain lists for DNS filtering of client queries, can reduce exposure risk by offering a security barrier controlling app access at the earliest point in the flow.

DNS

DNS domain deny and/or allow lists are seen as very valuable for 43% to improve control over which users can access which apps.

Combating DGAs:

To do this effectively requires real-time analysis of client behavior and ML to detect unknown malicious domains. Organizations are realizing this more and more.

Use of analysis of both client behavior and domain name to combat DGAs:

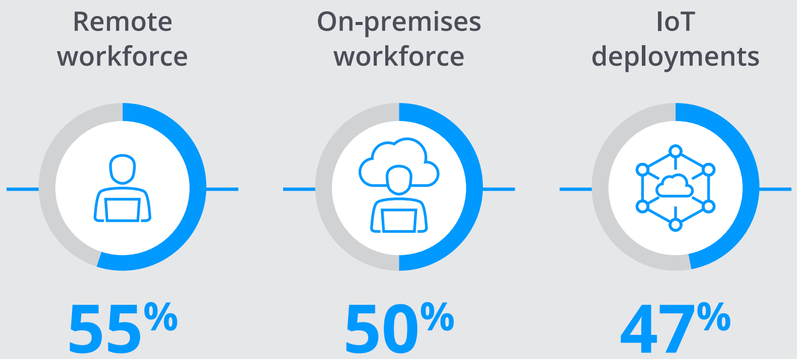
63% VS 32%

When adopting a zero-trust architecture, DNS will help with policy creation and enforcement by providing information on network usage and client behavior, and details on access to applications and data, as well as visibility and detection of threats before they can spread.

Securing the Extended Enterprise

With the boom in remote workers and adoption of IT initiatives such as IoT and SD-WAN security/SASE/SDSA, organizations need to gain full visibility of traffic and all connected devices, across all platforms, to be able to detect hidden threats. DNS is a central component of SASE/SDSA platforms, enabling a more streamlined security through corporate policy enforcement across the entire SD-WAN infrastructure.

DNS in the overall security strategy for the extended enterprise is seen as a critical component for:



Outside the corporate network, users and devices must be protected with traffic encryption, access control, and application access filtering with DNS security and DoH, which also help with regulatory compliance. Encryption of traffic is highly recommended when using home networks, using a VPN back to the organization network, or with DNS ciphering using DoH.

In addition to VPN and firewall, what tools do you consider useful for protecting your apps and services while making them accessible for remote workers?

PRIVATE ENTERPRISE DOH

42%

Software-defined secure access (SDSA) is an IDC category of access security and control solutions which establish secure connections based on context-aware, identity-aware, and device-aware policies, from an authenticated user to only authorized apps.

However, the survey highlights the privacy concerns with DoH, meaning organizations prefer privacy-by-design frameworks recommended by security organizations such as the NSA:

75% Consider using DoH with public providers to be a main risk.

51% are therefore considering setting up a private DoH system to limit that risk.

Organizations that do not include DNS security as part of their extended enterprise security strategy are more vulnerable to privacy issues. DNS security can not only protect their remote users, but also data and application traffic to ensure safe and secure online activities.

DNS Role in the Security Ecosystem

> To improve their overall security posture, organizations should better leverage the extensive insights provided by DNS to feed actionable threat intelligence data to the whole security ecosystem
>
> **Romain Fouchereau**
> Research Manager, IDC

DNS is an essential component of the overall security-by-design strategy and can be used to detect threats, simplify and accelerate mitigation, and be leveraged to improve visibility and control of basic services:

50% Use DNS traffic analysis to detect compromised devices.

DNS is the first line of defense as it sees the intent of virtually all IP traffic. Use of DNS provides information for automation of security policies and helps power a security orchestration, automation, and response (SOAR) platform, but this is being underutilized:

Automation for network security policy management:

57% are using mostly automated solutions.

As part of their security information received, SIEM platforms can make use of DNS traffic logs:

27% DNS traffic sent to SIEM for analysis

However, these are normally huge volumes of data, causing inefficiencies and breach fatigue. A smarter option would be for DNS to feed SIEMs and SOCs with only the relevant and actionable data on specific behaviors, translating into greater efficiency as SOCs won't need to analyze all traffic:

For those who do NOT use SIEM,

70% collect DNS traffic but analyze it manually.

Making use of DNS security event triggers would help simplify analysis and bring significant time savings.

DNS helps to overcome security holes that are often left by firewalls and IPS, particularly when coupled with other security components such as data loss prevention (DLP) and network access control (NAC):

Use of network analysis tools to detect compromised device:

NAC = 49%

NAC and DNS are very complementary tools for maximizing the discovery of compromised devices: NAC performs the static tasks for network access, while DNS performs dynamic functions with filtering for application access.

As a crucial element of any security-by-design framework, DNS security provides the whole ecosystem of security products and services with real-time analysis to elevate global threat intelligence to predict and stop malware containing algorithm-based malicious domains with instant policy enforcement, as well as information for automation of service configuration.

Cloud Services Continuity and Resiliency

Relying on the DNS service of the cloud providers is complex when starting multicloud and this requires continuous (at times manual) updates and monitoring. Amid cloud sprawl, this is time-consuming, complex, and error-prone. In the long run, it can lead to DNS misconfiguration, which can impact the services, especially if the enterprise is running in a multicloud environment:

52%
view DNS as a critical component of their overall cloud strategy (and 45% for edge)

46%
suffered cloud downtime as a result of a DNS attack (vs 50% last year)

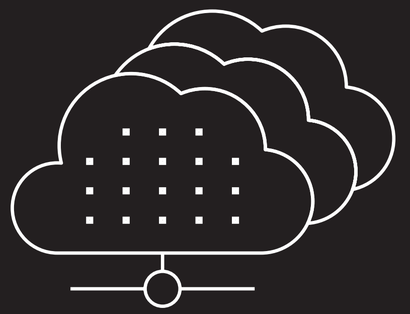
23%
suffered a DNS attack abusing cloud misconfiguration (vs 13% last year)

Rise in DNS hijacking attacks:

With these attacks, users are connected not to the desired service but to a fake one, and last year saw a big rise in this type of attack, with 27% of surveyed organizations — more than twice that in the previous year (12%).

Strong password management hygiene and deployment of DNSSEC (DNS Security Extensions) on the authoritative servers on all domains and on the recursive servers will protect against these attacks and ensure that information has not been altered from the server to the user application.

According to the **Cloud Security Alliance**, in its *State of Cloud Security 2020 Report*, **cloud misconfiguration** remains **the top cause of data breaches in the cloud**.



Misconfigurations and oversights in cloud environments can cause severe damage. Forgotten VM IP addresses in the cloud, for example, can leave the door open for DNS attacks, which tend to target organizations with large and complex infrastructures. Using a dedicated DDI (DNS-DHCP-IPAM) solution will help eliminate the risk of misconfiguration, particularly if automation is included.

Data Theft and Compliance: Cybersecurity Frameworks

Exfiltration of data by hiding it in normal DNS traffic goes unnoticed by traditional security components like firewalls, so companies are often not even aware of data being stolen until months afterwards.

Data theft via DNS is on the rise as cybercriminals exploit this:

Sensitive customer information or IP was stolen:

26%

16%

Timely detection of data theft therefore requires a DNS security solution that can analyze DNS transactions in real time. Businesses have acknowledged this and consider it one of their top priorities for protecting their IP and the sensitive data of employees and customers, helping with data compliance regulations such as GDPR, the US Cloud Act, NISD, and PDPA.

Solution considered most effective by organizations to prevent data theft from their network:

Better monitoring and analysis of DNS traffic

26%

Securing network endpoints

31%

Additional firewalls/ NGFWs/UTMs

21%

Purpose-built DNS security will protect against data exfiltration, even in the cloud. It offers adaptive and analytics-driven features such as behavioral threat detection, resilience, and disaster recovery features ensuring DNS service continuity and end-to-end visibility over all IP resources. Data-driven analysis of DNS activity can be leveraged to detect unknown (zero-day) malicious domains and therefore add another layer of security on top of antivirus products. DNS' detection and blocking capability can also be used to accelerate remediation of the infected devices through tight integration with endpoint remediation solutions or NAC to provide indicators of compromise when an endpoint is trying to exfiltrate data.

Cybersecurity frameworks help organizations to implement and adopt industry-standard best practices to reduce risk. DNS tools have a crucial role to play in these frameworks with both data theft and compliance.

Monitoring and traffic analysis abilities will enhance protection and confidentiality of data on the network, while compliance checks will ensure data is not exfiltrated or transferred to unauthorized locations.

Essential Guidance

To protect data, apps, cloud services, and users — whether on premises or remote — DNS plays a key role in the security ecosystem due to its understanding of network traffic intent, ability to filter client access, and enhanced control over user privacy.

Recommendations:

Enhance the privacy of your remote workers with a private DoH solution

Using a private infrastructure for DNS resolution and security improves control and better protects user privacy by keeping data related to traffic within your organization.

Eliminate cloud service downtime caused by cloud misconfigurations

Automating life-cycle management of IP resources for both provisioning and deprovisioning eliminates configuration errors and optimizes resource utilization.

Prevent the spread of attacks by making DNS your first line of defense

Combining DNS' unique traffic visibility for behavioral threat detection with domain threat intelligence and DNS query filtering enables breaches to be detected early in the network flow and strengthens application access control.

For more information, **click here to contact an EfficientIP security expert**

About EfficientIP

A Network Automation and Security Company

DNS
DHCP
IPAM

110+ COUNTRIES

Safeguard Data
Protect Users
Ensure Service Continuity

Open
Ecosystem
Integration

Enable Dynamic & Secure Communication Between Apps & Users

HQ

USA — Philadelphia
EMEA — Paris
APAC — Singapore

1000+
Customers
Across All Industries

Extend Visibility
Accelerate Deployment
Enforce Policies

Methodology

Analysis of this Infobrief is based on a survey IDC conducted on behalf of EfficientIP of 1,114 organizations across the world in early 2021.

The data collected represents their experience for the previous year.

Demographics:

REGIONS	NUMBER OF BUSINESS SIZE SEGMENTS	NUMBER OF COUNTRIES	NUMBER OF INDUSTRY SECTORS	METHOD
Europe North America Asia	5	9	6	CAWI + CATI

Yearly comparison was carried out likes for likes with survey data from 2020

Screener requirements: companies of 500 employees or more, all industry segments with quota per region, target respondent Network managers and IT security officers, decision makers and influencers for IT security

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Corporate Headquarters
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
508.872.8200
www.idc.com