2020 Global DNS Threat Report

Understanding the Critical Role of DNS in Network Security Strategy

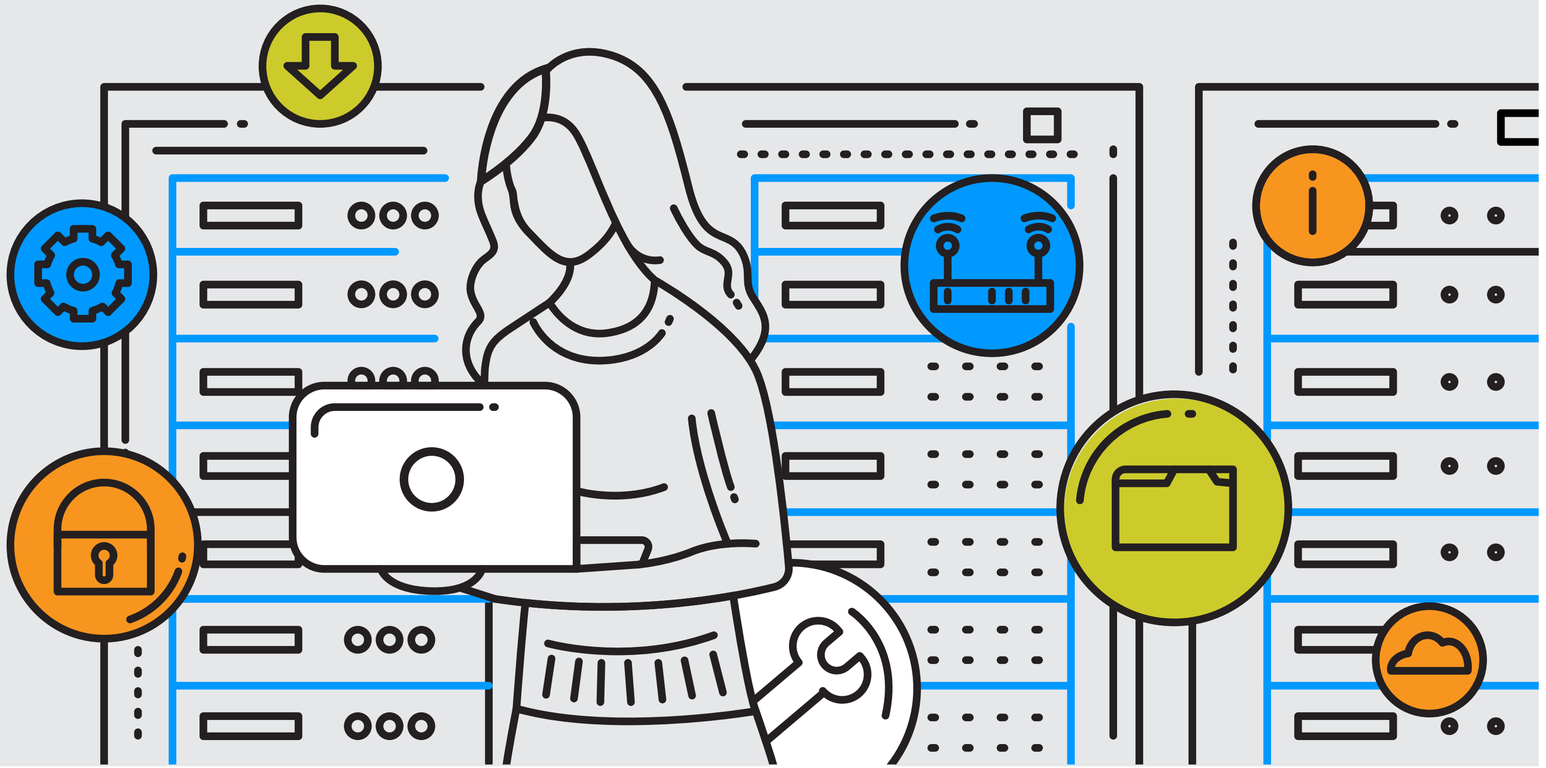
June 2020

Authors:
Romain Fouchereau, Research Manager, IDC
Konstantin Rychkov, Research Manager, IDC

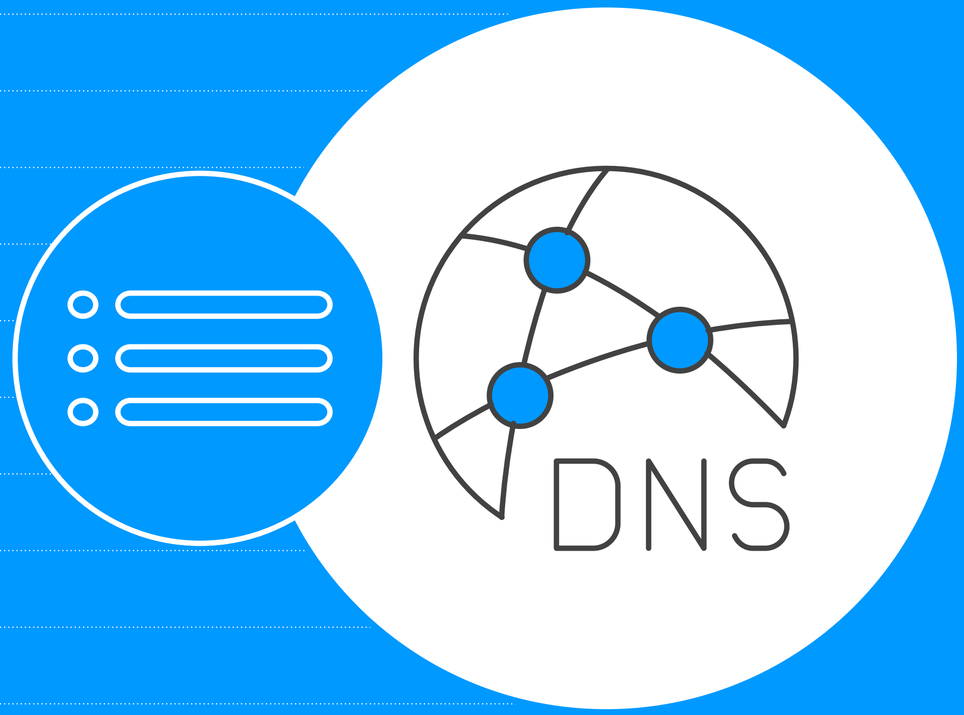
IDC #EUR146302820

Sponsored by

efficient iP™



Contents



Executive Summary

Evolution and awareness of DNS security is growing, but costs and the average number of attacks have remained high. The cloudified era has contributed to a majority of organizations being directly impacted by cloud and application downtime when facing DNS attacks.

79%
Experienced an attack

9.5
Average number of attacks in the past 12 months

$924k
Average cost of attack

82%
suffered application downtime (cloud & in-house)

Because of its foundational aspect in the network, DNS has visibility of all traffic and users. DNS can be leveraged to enhance zero trust strategies and data privacy compliance and play a key role in providing actionable intelligence for the security ecosystem.

Awareness of DNS security on the rise: **77%** deem it critical vs. **64%** last year

> It's pleasing to see that recognition of DNS security has risen sharply during the past 12 months, driven mainly by understanding of the criticality of DNS in the user-to-app journey. With the ongoing wave of key IT initiatives like IoT, Edge, SD-WAN and 5G, adoption of zero trust has also increased. However, as the survey results show, organizations are realizing that a successful zero trust strategy is dependent on DNS threat detection.
>
> **Jean-Yves Bisiaux,**
> CTO, EfficientIP

DNS Threat Landscape

Cybercriminals are well aware that "no DNS means no business." The majority of organizations therefore continue to be victims of DNS-based attacks, and the number of attacks suffered has remained high.

Organizations that were victims of DNS-based attacks:

2020 2019

79% | **82%**

Average number of DNS attacks per organization:

2020 2019

9.5 | **9.45**

DNS is an open service to the network, used by an ever-growing number of devices. The system is mission-critical for routing both internal and internet application traffic, which makes it a primary attack vector and target for hackers. The large range and size of DNS attacks illustrates this.

Top DNS-based attacks suffered

39% DNS phishing

34% DNS-based malware

27% DDoS attacks

21% DNS amplification

19% False-positive triggering

17% DNS tunnelling

Size of DDoS attacks is increasing:

2020 2019

Over 5Gbit/s

64% | **60%**

> Recognition of DNS security criticality has increased to 77% as most organizations are now impacted by a DNS attack or vulnerability of some sort on a regular basis. The consequences of such attacks can be very damaging financially, but also have a direct impact on the ability to conduct business. Ensuring DNS service availability and integrity must become a priority for any organization.
>
> **Romain Fouchereau,**
> Research Manager, IDC

Impacts and Costs of DNS Attacks

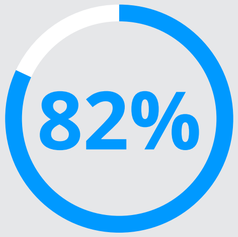
The number of apps/services being migrated to the cloud increases year on year. Cloud service downtime caused by DNS attacks has consequently risen. This has contributed to the damage cost of attacks remaining extremely high, affecting brand image, data confidentiality, and company finances.

Average cost per attack*

2020	2019
$924k	$1.07M

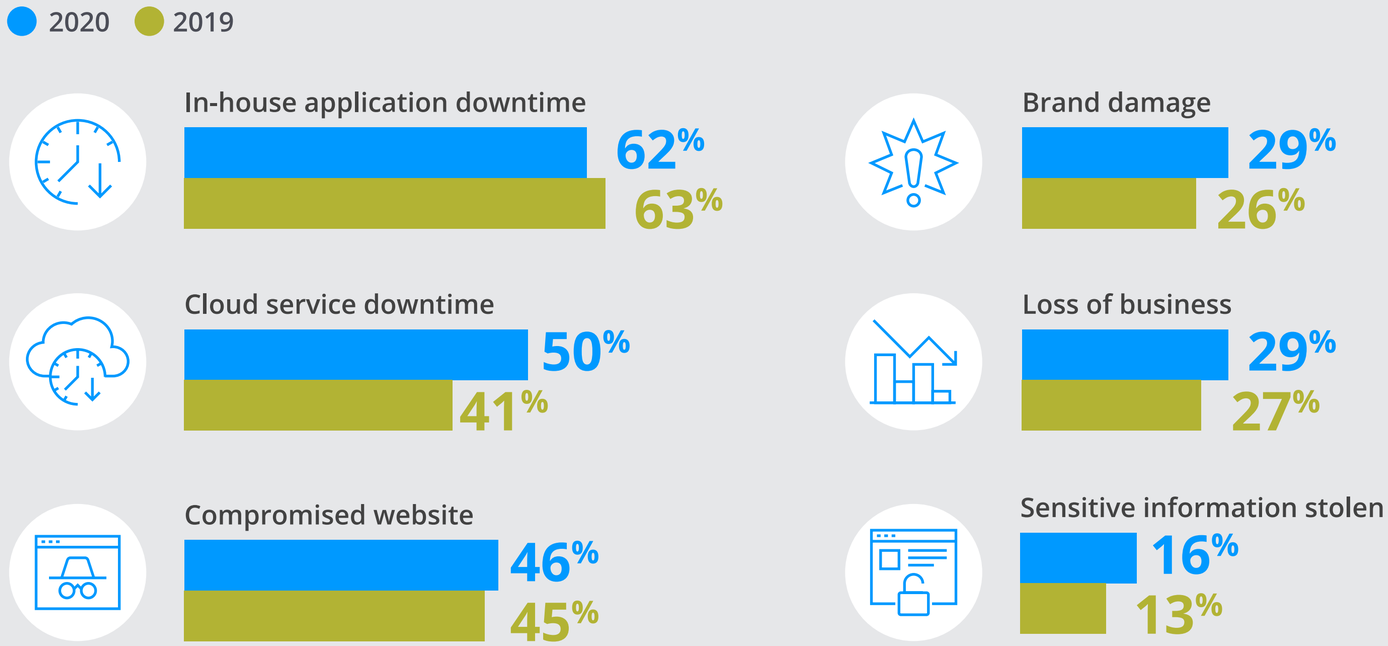
Application downtime, whether in-house or in the cloud, is in fact still the most impacting result of DNS attacks, demonstrating how critical DNS is for ensuring secure access between users & applications.

Application downtime**



DNS attacks and business outcomes are explicitly interlinked, and there are direct strong measurable business impacts.

Impact Statistics



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

Industry View

MANUFACTURING

Took longest to mitigate attacks — nearly 7 hours: impact on machinery uptime and physical safety

BUSINESS SERVICES

Highest cloud service downtime 65%: impact on business continuity and CX

FINANCIAL SERVICES

Highest cost per attack — $1.275M: criminals aim for high value targets

RETAIL

43% suffered compromised website: this is critical for their business

TELECOM & MEDIA

Most targeted industry — averaged 11.4 attacks, with 8% suffering cost over $5M per attack

Industry View

HEALTHCARE

55% shut down the affected processes and connections: potentially dangerous for patient care

EDUCATION

Highest customer information or IP stolen 21%: least secure industry with a lot of personal data

GOVERNMENT

Highest cloud instance misconfiguration abuse 22%: endangers nations not businesses

TRANSPORTATION

In-house app down-time 67%: critical infrastructure impact

UTILITIES

30% impacted by DNS malware: potential environmental and sociological concerns

State of DNS Defenses

Awareness of DNS security is on the rise, with

77% of respondents deeming it critical

VS

64% last year

Results of the survey show that

98%

of companies state they have some form of security for DNS in place in their organization.

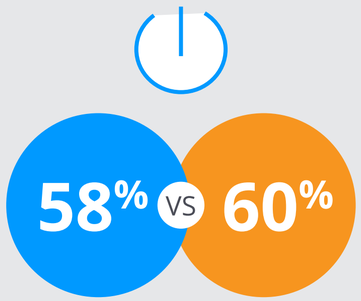
Among the 98%, companies, are increasingly using some form of dedicated DNS security solution (58%). But many solutions are not mature enough to ensure security of services:

75% of attacks were NOT mitigated using auto-remediation capabilities.

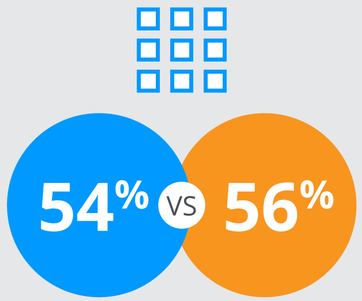
As a result, certain countermeasures are still inappropriate as they impact business continuity

Countermeasures Taken:

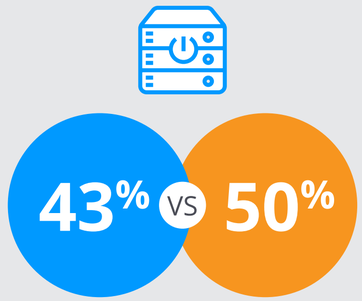
2020 2019



Shut down processes and connections



Disabled apps



Shut down business server

Time taken to mitigate DNS attacks is too long

Average time
5 ¼ hrs | 5 ½ hrs

Taking over 7 hours
21% | 21%

Lastly, the shift from reactive security is slow. To protect their DNS, and eventually their network, companies would do well to make better use of the valuable information the DNS itself provides.

25%

still DO NOT perform analytics on their DNS traffic.

(2019 = 30%)

IDC #EUR146302820

An IDC InfoBrief Sponsored by efficient iP™

No Zero Trust Success Without DNS Threat Detection

As organizations continue to rearchitect and build out their hybrid, multicloud environments, it is becoming increasingly clear that traditional network-based security is inadequate to protect the new use cases being added as part of digital transformation.

The adoption of a zero-trust security strategy has therefore significantly increased since the previous year.

Maturity of Zero Trust is increasing as companies are now moving from the planning to the implementation phase:

Implementation:

2020	2019
31%	17%

Planning implementation

2020	2019
38%	48%

User behavioral analytics (UBA), powered by AI and ML, provides a security analytics layer to automatically create individual profiles of devices and users from which statistical baselines of normal behavior are established.

Analytics on the valuable info provided by internal (east-west) DNS traffic, particularly with regards to client behavior, offers great potential for enhancing threat intelligence and filtering domains allowed to be accessed.

Adding machine learning tools brings capability to detect zero-day malicious domains (those not yet known to be malicious) and domain generation algorithms (DGAs).

For that, companies need to go beyond threat intelligence on reputation of requested domains

DNS usage for threat intelligence — to detect advanced threats better, domain filtering lists should be built based on internal traffic analysis, instead of relying just on external feeds:

35% of organizations do not make use of internal DNS traffic for filtering

Use of predictive analytics is increasing

2020	2019
55%	45%

But companies are yet to make adequate use of ML for augmenting valuable DNS info:

ONLY **12%** collect DNS logs and correlate through ML

ML is seen as being of high value for detecting unknown malicious domains and DGAs **62%**

> For a successful zero-trust strategy approach, organizations need to elevate their DNS security through the implementation of advanced threat detection capacity with user behavioral analytics (UBA)
>
> **Konstantin Rychkov**
> Research Manager, IDC

DNS Role in the Security Ecosystem

The fragmented nature of security remains a challenge for many organizations. Bringing together data from multiple sources and applying insights across increasingly complex landscapes is a difficult but essential mission for security teams.

> DNS security must become part of the overall security system in the security-by-design framework that every organization should adopt
>
> **Romain Fouchereau**
> Research Manager, IDC

With more domain names created and more devices joining the network (IoT, Edge, mobility, remote workers) and the growth of big data and analytics, sharing actionable data and valuable event information from DNS to the security ecosystem is a fast-growing requirement.

Infosecurity managers are increasingly suffering from breach fatigue, due largely to the high number of alerts they are receiving, many of which are false alarms. Rather than sending huge amounts of logs, a DNS security solution can feed SIEMs and SOCs with actionable data and events to help forensic examination, simplifying and accelerating detection and remediation.

2020 2019

Use of SIEM to detect compromised device: 29% | 27%

Organizations pass DNS info to SIEM for analysis: 33% | 22%

The DNS security solution can also provide NACs and firewalls with intent-based information for automated response and security policy enforcement.

Growth in use of NAC as way to detect compromised device

2020 2019

56% | 44%

Growth in adoption of automation for security policy management

2020 2019

59% are using automated processes VS 52%

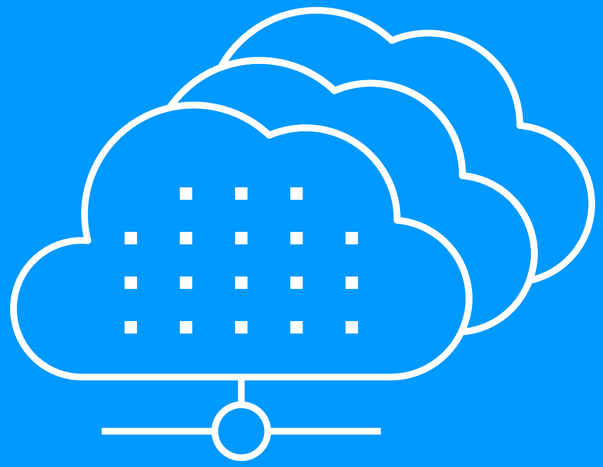
Cloud Services Continuity and Resiliency

Due to the increasing reliance on cloud services and applications, DNS security and resiliency have become of paramount importance for organizations.

Cloud services provide organizations with rapid deployments and high scalability and help to speed up installation through self-service portals. But this doesn't mean these cloud services will be "always on," as many of them can be affected by security breaches, outages, cloud provider issues, unreliable services… Hence the need to have a business continuity plan to safeguard continuous availability of the service and keep assets available at all times. DNS is key for accessing cloud services so must be protected.

50%
have suffered cloud service downtime as a result of a DNS attack

13%
have suffered a DNS attack which abused cloud instance misconfiguration



Maintenance of DNS configuration consistency over time is critical to ensure policy transparency, transferability, and compliance in dynamic environments such as cloud. To streamline associated workflows, organizations need to use the appropriate tools and automation processes

59% **are already making good use of automation for their security policy management***

[*either fully automated or with a good balance between automation and manual processes]

Data Privacy: Worldwide Initiatives

GDPR compliance has been a strong focus and a difficult task for European organizations to achieve, but following the example set in Europe, other regulations on data privacy are being implemented and planned worldwide.

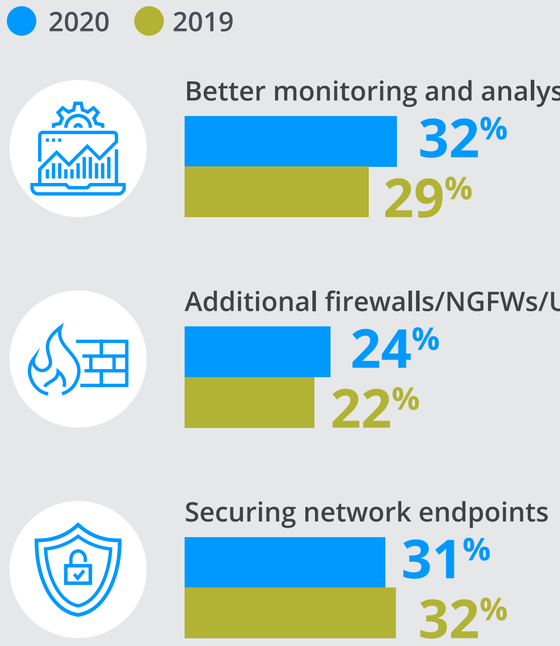
A global trend toward stricter or new data privacy laws gathered momentum after the European GDPR. California enacted the California Consumer Privacy Act (CCPA), requiring businesses to be transparent about how they collect, use, and share information, with a move to create a U.S. federal privacy law. Australia, Canada, the United States Federal Trade Commission, Singapore, and other individual states in the United States have stringent regulations around data privacy.

Organizations need to focus on data privacy management to raise trust in the enterprise and mitigate risk. Data privacy is not only a compliance issue; it is also a catalyst for business to turn personal data into a valuable asset, improve security, and gain competitive advantage. It is becoming instrumental to business growth and brand reputation and a foundation of digital transformation strategy.

But the proliferation of laws and regulations from multiple jurisdictions is bringing added complexity to data privacy compliance and management, as well as added risk and cost.

DNS is at the heart of ensuring better data privacy and regulatory compliance:

DNS monitoring and traffic analysis is now seen as the most effective way to protect data confidentiality on the network layer, overtaking improving endpoint security and deploying new firewalls.



Sensitive customer information was stolen from

16% **of respondents (vs. 13% 2019) as a result of a DNS-based attack.**

Data exfiltration via DNS often goes unnoticed as the information is hidden in normal network traffic. Measures that go beyond blacklisting, and instead focus on contextual client behavior, are far more efficient for closing back doors to data theft and combatting ransomware.

Essential Guidance

DNS offers visibility on devices and menaces across on-prem and cloud deployments to directly enrich data intelligence and reduce the complexity of threats and alert volumes that remain major challenges for SOAR solutions and security teams.

Recommendations to consider:

Elevate your threat detection capability with User Behavioral Analytics to empower Zero Trust

Using unique capability of DNS security to view and analyse client behavior improves end-to-end intelligence, and reduces risk of false positives.

Accelerate threat investigation by including DNS security in your security-by-design framework

Connecting security silos by sharing actionable DNS data with the ecosystem enhances SOC efficiency.

Ensure business continuity by implementing purpose-built DNS security with effective auto-remediation capability

Incorporating adaptive countermeasures limits attack damage by reducing mitigation times.

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

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 900 organizations across the world in early 2020.

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	10	CAWI + CATI

Yearly comparison was carried out like-for-like against a survey from 2019

Screener requirements: companies of 500 employees or more, all industry segments with quota per region, target respondent IT decision maker or security expert

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 is a subsidiary of IDG, the world's leading technology media, research, and events company. Further information is available on our websites at www.idc.com

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

Global Headquarters
5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com