



2022 Global DNS Threat Report

Securing Anywhere Networking

DNS Security for Business Continuity and Resilience

JUNE 2022

Author:
Romain Fouchereau
Research Manager
European Security, IDC

IDC #EUR149048522

An IDC InfoBrief, Sponsored by



Content

Executive Summary	3
Threat Landscape	4
Impact of Attacks	5
State of Defenses	6
No Industry Is Immune — All Organizations Are at Risk	7
Enabling Zero-Trust Models with DNS	9
Securing the Extended Enterprise and the Hybrid Workforce	10
Actionable DNS Event Data for the Security Ecosystem	11
Continuity and Resilience of Cloud and Services	12
Data Privacy, Theft, and Compliance	13
Improving Detection and Monitoring of Shadow IT	14
Essential Guidance	15
About EfficientIP	16
Methodology	17



Executive Summary

Hybrid work models and more reliance on cloud applications mean more attacks, and more attack types on infrastructures mean greater disruption. To respond and defend against these threats, organizations increasingly recognize the importance of DNS as part of their security strategies.



88%
experienced one or more attack



70%
suffered application downtime (cloud or in-house)



\$942k
average cost of attack



51%
were victim to a phishing attack



7
attacks on average per organization in the past 12 months



24%
had data stolen as a result of an attack



Awareness of DNS security is very strong:
73%
say it is critical



With organizations adopting a “work from anywhere” approach, the **2022 DNS Security Survey** shows that the frequency and damage cost of DNS attacks remain as high as ever, causing worrying impacts on service continuity and data confidentiality for on-premises, cloud, and remote workers.

The good news is that the importance of DNS for overall network security is being more and more acknowledged, with companies understanding its value for strengthening resilience, protecting data privacy, and for providing an early security barrier by controlling access to critical apps and services.

Jean-Yves Bisiaux
CTO, EfficientIP



DNS is a powerful tool to guarantee availability and integrity of the network, and a great instrument to detect and mitigate threats before they can propagate thanks to its full visibility over all network activity. DNS security is a key component of the overall security ecosystem of tools, products, and services.



Threat Landscape

DNS has been the Achilles' heel of the network since its creation, making it a target of choice for cybercriminals to exploit weaknesses, gain access to the network, and exfiltrate data. This is why it is vital for organizations to deploy a proper DNS security solution to mitigate risks and increase network security:



88% of organizations experienced an attack last year



7 attacks per year on average for each organization

Hybrid work models have created new challenges for IT teams. With the disappearance of the perimeter, both attack surface and cloud usage have increased considerably. Survey results show that the number and size of attacks remain very high, and cybercriminals are using all available tools to gain access to networks, disrupt operations, and steal data by leveraging vulnerabilities and cloud misconfigurations.

Top DNS-based attacks: all types of attacks have increased

● 2022 ● 2021

DNS tunneling:
28% vs 24%

DNS phishing:
51% vs 49%

DNS-based malware:
43% vs 38%

Zero-day vulnerabilities:
26% vs 23%

DDoS attacks:
30% vs 29%

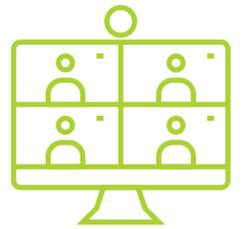
DNS hijacking/credential attack:
28% vs 27%

Cloud instance misconfiguration abuse:
27% vs 23%

The size of the DDoS attacks remains very high:

52% of attacks were over 5Gb/s (54% last year).

Hybrid Workforce



According to IDC research on the hybrid workforce:

45% believe remote and hybrid work models will be part of accepted work practices.

98% anticipate challenges in implementing hybrid work.

As digital enterprises adopt hybrid work models, IT teams need to enable secure access for all employees, but also drive improved productivity and better work experience and increase overall business agility and resilience.

Security challenges:

- Unsecure home networks
- Targeted cyberattacks
- Proliferation of shadow IT
- IoT devices on home networks

New challenges related to hybrid workforces include the privacy of the data traffic of the remote workers. A dedicated DNS security solution will provide better control and security to protect applications, users, and data.



Impact of Attacks

Average cost of attack*:

2022 **\$942,000** | 2021 **\$950,000**



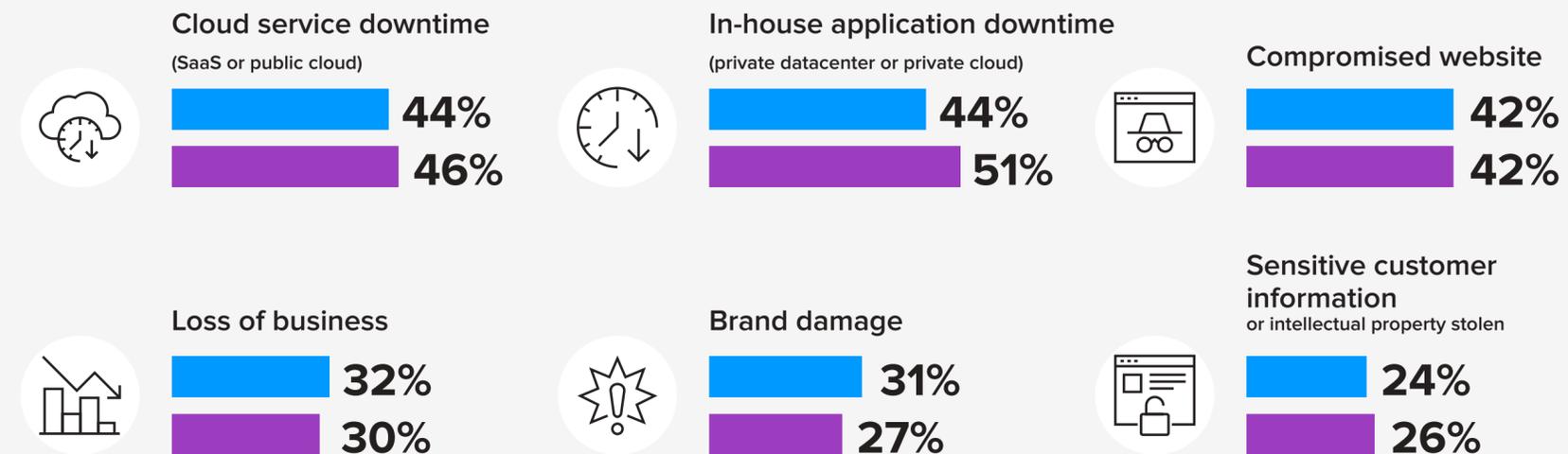
Because of the high costs and frequency of attacks, many companies will struggle to remain in business. Breaches not only directly affect an organization's finances, but also its reputation, intellectual property, and customers. DNS-based attacks such as ransomware are becoming more pervasive, and cybercriminals are specifically targeting the hybrid workforce. No organization — of any size, in any industry — is safe.



As a result of attacks, downtime — from in-house applications or cloud services — means employees, customers, and partners are not able to access anything for hours. This shows how important DNS is for resilience and to secure access between users and applications.

DNS attacks directly impact business outcomes, and the result can directly be measured on the business:

● 2022 ● 2021



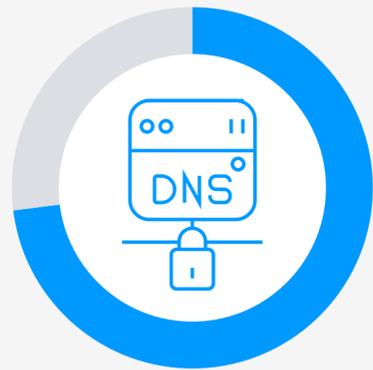
DNS allow/deny filtering capabilities play a critical role in reducing the impact of DNS-based attacks — such as application downtime and other more long-term business losses — as they can stop malware from spreading at the time of infection.



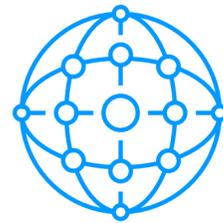
State of Defenses

Awareness of the importance of **DNS security** remains high and a concern for most organizations:

73%
say it is critical for their business.



The survey shows that over **99% of companies do have some form of security for DNS** in place, but **43% do not use a security solution built into a DNS server** to benefit from the added advantages of these solutions, such as business continuity, data protection, and user protection.



Business continuity

● 2022 ● 2021

Although the situation is improving year by year, organizations are still taking **inappropriate countermeasures** when attacked, and this is having a negative impact on **business continuity**:

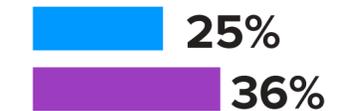
Shut down the DNS server or service



Disable applications



Shut down part or all of the network infrastructure



Average time to mitigate increased to **6H 07M** (+29 minutes) with **24%** taking longer than 7 hours (was 23%).

Digital transformation resulted in faster multicloud adoption, but this also translated into an overall increase in management complexity for the IT security teams, making mitigation even more time consuming and difficult.



To ensure security of services during a DNS-based attack, **62%** of organizations are still **NOT using auto-remediation**.



DNS analytics can provide actionable information to improve security of the workforce and IoT deployments, strengthen resilience, and enhance user experience, but **25%** of organizations still **don't collect or analyze** their DNS traffic.

To ensure business continuity and global resilience of all apps and services, it's important to leverage DNS capabilities to mitigate DNS-based attacks with adaptive countermeasures.



No Industry Is Immune – All Organizations Are at Risk

FINANCE



Most attacked (**9.5 times**) and for the highest value **\$1.3 million**. Most targeted industry by ransomware (**50%**).

RETAIL



Highest results in cloud service downtime as a result of attack (**50%**) and data stolen (**31%**).

TELCO



Most targeted by DDoS attacks (**37%**) and highest suffered loss of business (**35%**).

HEALTHCARE



Most likely to shut down the network infrastructure during an attack (**29%**); **53%** were a victim of phishing attacks.

EDUCATION



Largest DDoS attacks; **12%** suffered attacks over 50Gb/s; **64%** do not have confidence in their shadow IT detection capability.

No Industry Is Immune – All Organizations Are at Risk

GOVERNMENT



39% suffered a ransomware attack; **39%** shut down their DNS server or service (third highest).

UTILITIES



Longest to remediate attack: 7h 35m; **38%** brand damage (highest with risk of customers switching to another provider).

MANUFACTURING



Highest cloud instance misconfigurations (**29%**); **30%** of organizations were victims of zero-day vulnerabilities (the highest in the survey).

TRANSPORTATION



50% of organizations have had their website compromised; highest in-app downtime (**52%**).

BUSINESS SERVICES



Most likely to fall for phishing attacks (**58%**); **49%** hit by cloud service downtime.

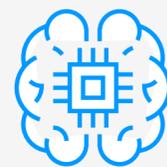
Enabling Zero-Trust Models with DNS

Zero trust is a key approach in security strategies, founded on least-privilege access principles and requiring control of which devices can access which apps and services. Building a cybersecurity program around zero-trust principles will generate security data that can be used to make decisions that can be fed back into each individual area of a security program through updated policies and adjustments, making each one more efficient and effective.

Maturity of zero trust: Zero-trust implementations have increased over the past year, with only 24% of organizations not yet exploring it.



Threat intelligence and DNS filtering: Threat information comes from data and telemetry generated by the DNS and from data based on internal network activity, such as alerts, logs, and traffic flow.

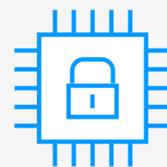


Threat intelligence:
74% make use of internal DNS traffic analysis vs 70% last year.



To manage DNS filtering lists:
22% still use only third-party feeds.

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 flow.



To improve application access control, 56% already use DNS.



DNS domain deny and/or allow lists are valuable for 83% (vs 77% in 2021) to improve control over which users can access which apps.

App access control:



Filtering access with allow/deny lists is essential for a successful zero-trust strategy. But management complexity is a major hurdle, especially when dealing with firewalls.

66% of organizations have medium to low satisfaction with the management complexity and implementation cost of their security solution in terms of preventing the lateral propagation of threats.

IT security teams need simpler solutions:

- DNS is simple to set up and acts early in the communication process.
- For filtering access, DNS offers high reward for low effort.

In zero-trust strategies, DNS security becomes another layer of the framework to increase and support application access control using deny/allow lists. Microsegmentation for intelligent control can be done at the DNS level to simplify deployment and management operations.



Securing the Extended Enterprise and the Hybrid Workforce

Digital transformation and hybrid work models are changing the network with the adoption of new technologies, strategies, and delivery models. Security must also extend beyond the traditional enterprise perimeter to address new imperatives such as IoT, cloud, remote workforce, datacenter, SD-WAN, and 5G.

The extended enterprise:

As organizations better understand the risks and vulnerabilities their organizations face, they see the critical role of DNS in their overall security strategy for the extended enterprise.

DNS is critical in securing:

● 2022 ● 2021



IoT deployments
51% vs 47%



Cloud deployments
56% vs 52%



Datacenter
48%

DNS security for IoT protection



To improve IoT security, the use of **DNS for filtering access of IoT devices** to specific apps is seen as important by **84%** of organizations. DNS complements other IoT security products as it can control access from devices to specific parts of the network, apps, and services through **allow and deny lists filtering**. This will help identify and block any rogue device or botnet threats on the network and mitigate threats and reduce risk.

DNS security is seen as a strong asset for securing the **hybrid workforce**. Organizations say it is a critical component of their overall security:

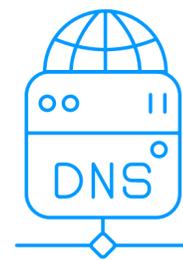


54% for the remote workforce



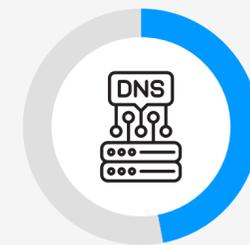
50% for the on-premises workforce

DNS security can also protect data and application traffic to ensure safe and secure online activities:



49% see private enterprise DNS solutions as useful for protecting apps and services while making them accessible for remote workers (in addition to VPN and firewall). This was **42%** last year.

Rather than relying on expensive, complicated, and unscalable VPN solutions, companies often use standard ISP/public DNS services, exposing themselves to privacy and data security vulnerabilities. Using private DNS will prevent snooping and keep data related to traffic within the organization.



47% are considering setting up a private DNS system to limit the privacy risks of using DoH with a public provider (49% last year).

As well as offering more controlled privacy, private DNS also enforces security policies for all users and devices.

Private DNS security can be leveraged to reduce management complexity, boost privacy, and extend the same on-premises policies to the extended enterprise: cloud, IoT, SD-WAN, remote workers, etc.



Actionable DNS Event Data for the Security Ecosystem

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. A holistic approach can be achieved by sharing actionable data and security events.



DNS traffic analysis is the **third most used** tool to detect compromised devices (behind AV and FW logs).

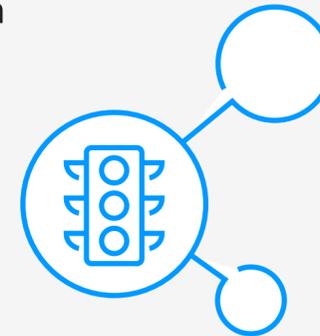


23% of DNS traffic is sent to SIEM for analysis vs 27% last year.



SOAR: rise in use of automation for network security policy management: **60%** are using mostly automated solutions (57% last year).

Monitoring **DNS traffic can be a rich source of data** for security operations center (SOC) teams as they monitor and analyze the security posture of the organization. DNS can **help enforce security policies and automate security responses** — and then feed pertinent security events into a SIEM and/or SOC (and reduce cost), as well as other components of the security ecosystem.



NetSecOps:

Networking and Security Collaboration



To successfully deliver their digital transformation strategies and focus on business outcomes, organizations must be aware that collaboration between networking and security teams is essential.

From SD-WAN implementation to cloud migration or datacenter modernization, it is vital that network and security teams successfully work together:

- Security teams need network data from DNS traffic (ideally already analyzed data as raw data is not relevant/efficient) to get visibility and to understand the infrastructure.
- Networking teams need a security-by-design approach to their operations to function safely and to enhance collaboration between NetOps and SecOps.

Secure automation requires comprehensive source of truth data on the configuration of a network and the state of that network:

75% of network teams share their DNS-DHCP-IPAM data with security teams

(source: EMA 2021 NetSecOps Report).

DNS security provides real-time insights into the full security ecosystem of products and services for enriched threat intelligence to help identify threat indicators, assess risk, and prevent future attacks. DNS will help enhance and secure the day-to-day function by adding relevant telemetry and analytics on top of software-defined networking and security tools.



Continuity and Resilience of Cloud and Services

DNS is critical for users to access their apps and services stored on premises or in the cloud; when DNS services are affected, users are unable to access their applications: no DNS means no business.

The cloud-first approach has contributed to most organizations being directly impacted by cloud and application downtime when facing DNS attacks, from enterprises to service providers and even into the midmarket, and a DNS platform can help secure networks, applications, and data.

Continuity requires smart management of app traffic. DNS can be used to intelligently steer app traffic to ensure app availability and improve user experience.

As result of a DNS-based attack:



44%

were hit by in-house application downtime



44%

were hit by cloud service downtime

The importance of continuity and resilience:



How Facebook completely disappeared from the internet

On October 4, 2021, Facebook and its subsidiaries became globally unavailable for seven hours. The outage also prevented anyone trying to use “log in with Facebook” from accessing third-party sites and cut off all Facebook’s internal communications.

The issue was identified as a border gateway protocol (BGP) withdrawal of the IP address prefixes in which Facebook’s DNS servers were hosted, making it impossible for users to resolve Facebook and related domain names and reach services.

As a result, Facebook’s share price dropped 5% and the company lost at least \$60 million in advertising revenue during that time.



56% view DNS as a critical component of their overall cloud strategy (up from 52% last year) and **48%** for the datacenter. **27%** suffered a DNS attack abusing cloud misconfiguration (up from 23% last year).

With so much reliance on cloud, and the difficulty of managing multicloud, it is vital to ensure continuity and resilience of their cloud apps and services, but relying on the DNS service of the cloud providers is complex and requires constant monitoring and updates, often leading to DNS misconfigurations impacting continuity.

Maintaining DNS services resilience is vital for many enterprises because they rely on their online presence for their customers, partners, and employees. Malfunctioning or unavailable DNS services could lead to internet invisibility and impact business and reputation, resulting in a loss of revenue and brand damages.

During DNS attacks organizations still reacted by shutting down:

38%

DNS services

36%

Applications

25%

Infrastructure

DNS security provides analytic tools such as behavioral threat detection and adaptive countermeasures and disaster recovery features to safeguard DNS service.



Automation as part of the DNS solution in multicloud environments will enable automated provisioning and deprovisioning of IP resources and eliminate the risk of misconfigurations. Constant monitoring and management will ensure deployment is optimal for stronger DNS service continuity and resilience.



Data Privacy, Theft, and Compliance

Accelerated digital transformation and the shift toward a hybrid work model requires organizations to rethink their data protection strategies and upscale their data security infrastructures for cloud environments.

Data theft via DNS is a major concern and remains high:



24% had sensitive customer information or IP stolen

Data theft



Traditional security solutions cannot detect exfiltration, so organizations can remain unaware of a data theft for a long time. Through real-time analysis of DNS transactions, organizations can detect signs of DNS tunneling and stop data theft quickly. Organizations therefore see it as their top solution for protecting their intellectual property and sensitive data.

Top 3 solutions considered most effective for preventing data theft from the network:

Better monitoring and analysis of DNS traffic

26%

Securing network endpoints/NAC

24%

Additional firewalls/NGFWs/UTMs

19%

Data privacy



As they move to hybrid workforce models, most organizations are concerned about data privacy when using DNS from public providers. A private DNS will protect all DNS requests through encryption, preventing eavesdropping and keeping data safe from public providers that could use the information for their own analysis.



72% consider using DoH with a public provider to be a main risk (74% last year).



49% consider private DNS a useful tool for limiting privacy risk.

Rise of ransomware



43% of organizations were victims of ransomware.

Ransomware has become a profitable industry, resulting in substantial ransom demands, major disruptions, and leaked or stolen data.

DNS security is the top method for protection against malware and ransomware at **57%**.

As basic DNS is no longer adequate, recommendations to protect against ransomware include:

- Investing in response policy zones (RPZs), threat intelligence, and log analysis
- Using a high-performance dedicated DNS

DNS can be used as a foundation tool for anti-ransomware programs.

DNS tools can take cybersecurity privacy and compliance programs to the next level through constant and real-time traffic monitoring and analysis of all data for protection and privacy. DNS security checks will protect from data exfiltration and help organizations to achieve their compliance regulations (GDPR, CCPA, PIPEDA, PDPA, etc.).



Improving Detection and Monitoring of Shadow IT

Shadow IT is becoming a major concern for IT departments as lines of business and/or employees acquire or run IT systems, services, solutions, or technologies without their knowledge or approval.

Organizations are worried about the increasing risk of new vulnerabilities in security, compliance, cost, efficiency, and even potential data issues linked to cloud residence.



39% of organizations have a high level of **confidence with their shadow IT detection** capability.

DNS traffic and network data will help businesses better understand employee behavior and therefore detect shadow IT in terms of unsanctioned and unmanaged cloud apps, but also detect, identify, and monitor machine-to-machine communications.

Organizations are realizing the value of DNS to help detect Shadow IT:



DNS is used as the primary solution to detect shadow IT at **51%** of organizations surveyed, alongside firewalls using deep packet inspection (DPI), also at **51%**, and proxy at **48%**.

However, the majority of organizations are putting little focus on shadow IT detection, despite the concerns around cloud services, apps, devices (including IoT), unauthorized developments (for example, rogue DB), or use of resources from unauthorized users that can weaken the overall security posture of the organization:

61% have **NOT** made shadow IT a priority for their organization in 2022.

For those companies, DNS offers an easy option as it is a great tool to start enhancing protection against shadow IT: it is a simple, efficient, and cost-effective solution (as it is already there) and it's easy to implement.



DNS security enables complete visibility in clouds and apps, and organizations can leverage network data for discovery, giving the often-overwhelmed security teams more visibility into their cloud-based applications with detection and monitoring of shadow IT.



Essential Guidance

For strengthened network security, DNS is by nature your first line of defense thanks to threat detection over user behavior, access control capability at client level, and potential to automatically share data and qualified security events with SecOps teams.

DNS is a foundational component for reinforcing the overall security chain to protect data and business operations.

Recommendations:



Prevent lateral movement of threats by creating an early security barrier

Combining DNS filtering with allow and deny client and domain lists provides a first point of control to ensure only specific users are permitted access to specific apps and services.



Reduce risk of new vulnerabilities by enhancing shadow IT detection

DNS visibility across both on-premises and cloud offers a simple cost-effective solution for detecting unauthorized apps and services.



Speed up threat remediation by improving NetSecOps collaboration

Automated sharing of actionable data and events coming from DNS traffic analysis with security teams simplifies SOC investigation and response.

For a free DNS risk assessment to identify vulnerabilities and improve your protection,

[click here or visit our website](#)



About EfficientIP

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 challenges they face. This applies particularly to modern key IT initiatives such as cloud applications, virtualization, mobility, digital transformation, and SDN.

For more information, visit

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



Methodology

This InfoBrief is based on an IDC survey conducted on behalf of EfficientIP of 1,080 organizations worldwide in early 2022.

The results represent their experience for the previous year.

Regions	Number of Business Size Segments	Number of Countries	Number of Industry Sectors	Method
Europe North America Asia	5	9	10	CAWI + CATI

- A yearly comparison was carried out like for like with survey data from 2021.
- Screener requirements: companies with 500 employees or more, all industry segments with quotas per region, target respondents have an IT-related job function, are decision makers, and set the security strategy in the organization.

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

Copyright Notice

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

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

Copyright 2022 IDC. Reproduction is forbidden unless authorized. All rights reserved.