MARKET PERSPECTIVE

Infoblox Leverages Domain Name System for Detection and Response and Threat Intelligence

Christopher Kissel Monika Soltysik Frank Dickson

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Infoblox Leverages Domain Name System for Detection and Response and Threat Intelligence

Infoblox leverages the domain name system (DNS) to enhance cybersecurity through detection and response (DR) and threat intelligence. By utilizing DNS, Infoblox provides visibility into domain-to-domain connections and identifies indicators of compromise, significantly reducing mean time to respond by 34%. Infoblox's approach includes maintaining billions of DNS transaction records and actively tracking malicious domains.

Key Takeaways

- Infoblox leverages DNS for enhanced cybersecurity, offering detection, response, and threat intelligence capabilities that are crucial for businesses to maintain network security and operational efficiency.
- DNS — while fundamental for internet connectivity — is used to connect to malicious domains and data exfiltration via DNS tunneling, making DNS hygiene and visibility essential for preemptive threat mitigation.
- The integration of DNS -based security solutions with existing IT and security operations without the need for additional agents offers a proactive and efficient method to enhance cybersecurity posture, making it a strategic consideration for businesses aiming to bolster their defense against cyberthreats.

Recommended Actions

- Prioritize DNS hygiene by implementing response policy zones (RPZs) to grant access to known good sites and block malicious ones, establishing a DNS firewall with zero trust controls to enhance cybersecurity posture.
- Integrate DNS detection and response capabilities with network detection and response (NDR) platforms and threat intelligence vendors to achieve a comprehensive view of DNS connections, enabling the identification and mitigation of threats that bypass traditional perimeter defenses.
- Leverage DNS logs and response logs to identify indicators of compromise (IOCs) such as evidence of DNS tunneling, high numbers of DNS queries, and DNS queries that result in failed access attempts to enhance on -premises threat detection and response strategies.

Source: IDC, 2024

August 2024, IDC #US51470924

NEW MARKET DEVELOPMENTS AND DYNAMICS

Introduction

For all of the griping that is done about social media and security exposures, the internet is pure magic. The internet includes protocols that allow a user to initiate contact with another site, conduct a session, receive information in a proper sequence (by this we mean the orderly flow of packets), terminate the session, and begin again. This IDC Market Perspective focuses on the session initiation phase and more specifically IP addresses and domains.

IP addresses are assigned to all devices that access the internet. In the common IPv4 address protocol, there is a 4-number set ranging from 000.000.000.000 to 255.255.255.255 (which is basically full) and there is a spill over into IPv6. The domain name system (DNS) is the ingenious directory that translates IP addresses into domain names — in many ways, this is similar to a contact list in a cell phone where phone numbers are converted into a person's name and by and large not thought about again.

It is fair to say that a business of any size has a dedicated DNS server. If businesses did not, they would allow their employees to use their own internet service provider (SP) which may cause latencies during a DNS query because there would not be a common cache. In addition, the enterprise would also cede the safety of DNS queries to each individual's ISP. This is an adequate description of the IT implications of DNS — however, utilizing the DNS has great potential in threat prevention, threat intelligence, and detection and response.

IT is concerned with the smooth operation of the network pertaining to the line of business. The security operations (SecOps) team is concerned with keeping the adversary off of the network and the ability to monitor miscreants in the course of operations. DNS is common to both. The IT team needs to create domain good lists to expedite sessions and applications and bad lists to block dangerous access. The security operations team should handle the unknowns.

Understand, though, that this simple example is about intranet and internet activity. The DNS ecosystem is not restricted to individual networks. If properly mapped — in theory — all public DNS sessions can conceivably be recorded and used in a forensic investigation (which is the value proposition to Infoblox Threat Intel). This means that even containers that may have IP addresses and operational technology (OT) devices such as surveillance cameras or health

monitoring equipment that cannot have agents installed and have proprietary operating systems can be monitored. SIEM is concerned with logs, devices are concerned with germane activities in point-to-point connectivity, and network detection and response (NDR) platforms are concerned with the business network. Cybersecurity DNS is concerned with the history of the connections of all IP addresses.

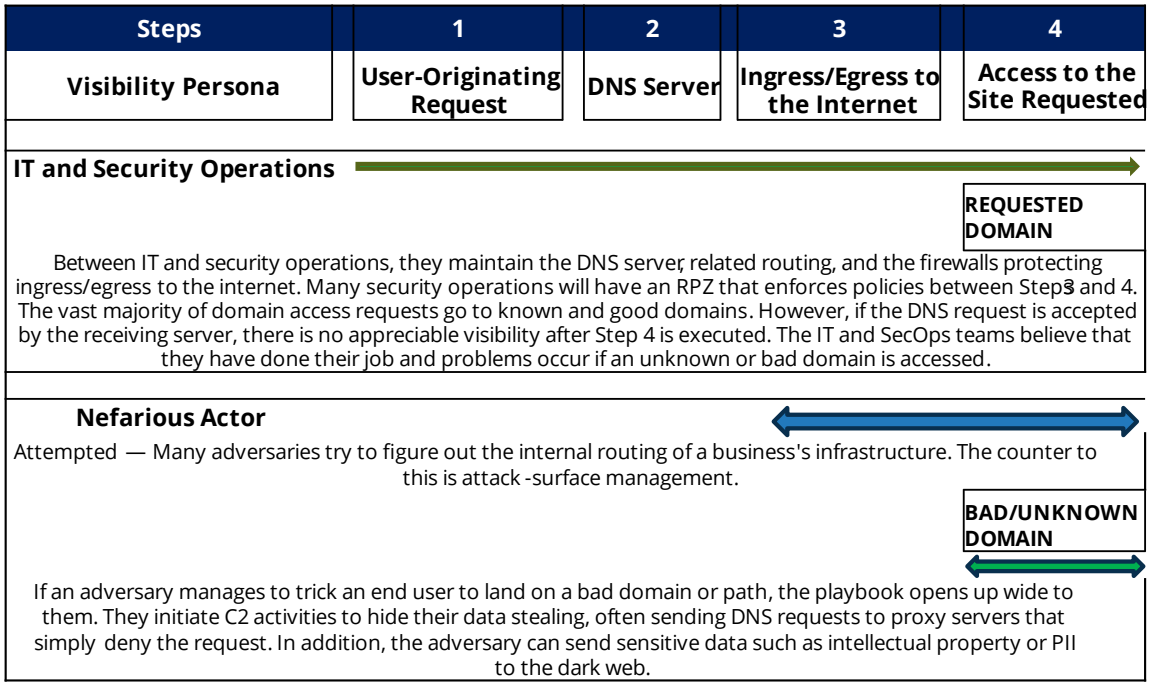
DNS Visibility: The Principles Behind Detection and Response

DNS hygiene is a necessity for a business of any size. DNS is a double-edged sword. If it is left alone and properly configured, when end users access their DNS server to visit websites the transaction is smooth —essentially without latency — and proper response policy zone (RPZ) policies block end users from accessing malicious and high-risk sites.

Perhaps an illustration of a DNS query and what happens after the query is initiated will provide an understanding of the value of DNS as a preferred detection and response technology (see Figure 2).

FIGURE 2

DNS Visibility After a DNS Query



Source: IDC, 2024

The chart shown in Figure 2 is largely self-explanatory. The end user is trying to access a website (eBay, ESPN, or IDC). In the majority of instances, the good list has been cached and the query moves off of the DNS server and goes into the routing hierarchy that ties the DNS server to the internet ingress/egress server where it is reviewed by perimeter tools such as firewalls and antivirus. The query becomes an encrypted session and leaves the premises as a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) session. Do note that this is almost exclusively an HTTPS handoff as the major browsers will not allow non-HTTPS communication to occur.

Unfortunately, the authorized HTTPS session is when the IT team and security operations are done. This remains the great failing of cybersecurity tooling in general. If a session occurs and it looks as if it has happened from the authenticated user or within protocols, security is done with it — this occurs with firewalls, SIEM, endpoint protection, and the majority of cybersecurity appliances/technologies. In fairness to IT SecOps, since the vast majority of HTTPS sessions are to valid websites or properly vetted devices, it would be highly inefficient to track what happens from the accessed website even if a business's IT SecOps team had the tools to do so. Obviously, if an IT team allows an end user to contact a malicious domain or an end user is initiating an insider threat, the problems begin.

All of the fun things that an adversary can do now come into play in the following ways:

- The end user is deceived into requesting an upload that can destroy the machine or hide spyware or malware in the machine to spread the infection.
- The adversary can steal data — possibly all at once or at intervals designed to avoid detection.
- The adversary can create alternate routing to disguise the maliciousness of the receiving server.

DNS visibility is a valuable defense posture strategy as it shows whether a user/device is going to a high risk or malicious domain and if there is data exfiltration happening via DNS to a malicious destination. It can then block those DNS queries from resolving, proactively protecting the user/device from downloading malware. In addition to Infoblox, other companies such as Cisco Umbrella, DomainTools, and EfficientIP as well as threat intelligence vendors such as Recorded Future and ZeroFox provide an overview of the internet. The

use cases are apparent, but remember that the use cases mentioned here are out of the grasp of a business' own IT SecOps team. In detail:

- DNS detection and response (DR) companies provide visibility into C2 servers and high-risk domains owned by threat actors that could be used in future attacks. DNS cybersecurity vendors can look for evidence of beaconing activity (slow and persistent sessions).
- DNS cybersecurity vendors can look for servers that host malware. Certain domains are used over and over again to push malware. If there is enough evidence, the DNS provider can work with domain registrars to "take down" the domain. If the DNS provider doesn't offer a takedown service, the DNS service provider can ask the content delivery networks to "take down" the domain — but this process is not always granted or immediate. If a takedown cannot occur, an organization can bad list the IP address of the malware-pushing server.
- IP address management (IPAM) data such as device type, network location, and user info can be used to help speed up incident response to security events. IPAM — when used with DNS — can provide powerful visibility.

Indicators of Compromise Unique to DNS

The first sections about DNS were primarily about DNS detection and response. In addition, DNS logs and DNS response logs can be used to find indicators of compromise (IOCs) on premises as follows:

- **Evidence of DNS tunneling exists.** One misnomer about DNS tunneling is that it has no legitimate use case, and that is not true. DNS tunneling is used to carry encapsulated data from another protocol and can be legitimately used by content delivery networks, music streaming services, and other applications. However, an adversary can use DNS tunneling for stealing intellectual property to avoid detection by DLP tools. If a business decides to use DNS tunneling for legitimate business purposes, it had better keep a comprehensive use of these domains on hand.
- **If there is a high number of DNS queries, this is a reliable IOC.** When a domain is new there may initially be a number of DNS queries, but once the domain is known to be safe, different protocols are used to access a site. However, if the domain is carrying data or is being used as a C2 proxy server, the DNS requests will be high.
- **DNS queries that resolve in failed access attempt or NXDOMAINS exist.** This requires monitoring of DNS response logs, but basically this is

an adversary trying to phish for usernames or applications that can be used to contact a C2 server. The book *The Hidden Potential of DNS In Security: Combating Malware, Data Exfiltration, and More — The Guide for Security Professionals* is an excellent resource for describing DNS-related attacks as well as DNS detection techniques.

The use case for DNS DR is fairly novel but the cybersecurity implications are powerful. Perhaps the way to think about DNS detection and response is to consider that DNS can be used for more than simple "good lists" and "bad lists." In detail:

- **Look-alike domains are exceedingly difficult to identify.** Many look-alike domains are not readily apparent. The use of a lower case "i" can substitute for a capital "I." Cyrillic characters look like English zeros and "o's". The obfuscation can extend to landing pages or in the path name after the domain name.
- **It is virtually impossible to keep a valid good list of domains.** The hope is that internet browsers will prohibit end users from initiating a session with a malicious domain; however, it often takes months to identify a bad site/domain. Even if a list of known good domains could be refreshed daily, there are 200,000 new domains registered every day. That mix includes legitimate domains. Often, a basic investigation will simply block access to an unknown domain which is likely better from the perspective of a business than allowing an employee untrammeled access to an unknown site. However, none of this prohibits the adversary from doing the exact same thing the next day with newly registered domains.
- **The DNS system covers everything, even the nooks and crannies of where the adversary dwells.** The adversary may do any number of things but every communication on the internet and dark web can be monitored. Routing activities from one server/domain to another can be monitored and these histories can be cataloged.
- **DNS DR can greatly reduce mean time to respond (MTTR).** A study initiated by Infoblox showed that clients using its DNS DR service improved MTTR by 34%. There were several reasons for this. First, each machine/identity has a DNS history. Infoblox can provide a list of device activities faster than a security team can retrieve the data from logs. Second, Infoblox has histories of device IP addresses that the user had as well as their communication history.

What Is Novel about Infoblox Threat Intel

Infoblox Threat Intel was relaunched with new capabilities in April 2024. Traditionally, threat intelligence has been focused on the types of malware signatures and tactics used in adversarial attacks. However, much like Infoblox's DNS DR service, Infoblox Threat Intel collects important contextual information about threat actors.

Domain registration is problematic; there is a donut hole in how cybersecurity accounts for new domains. In the first case, roughly 200,000 new domains are registered every day and many of these are malicious — these can be phishing sites, knock offs of websites used to gather information, C2 routing servers, dark web markets, or other types of nefarious activity. Very often, a new domain is neither on a good list nor on a bad list. As such, without a proper assessment a cybersecurity team may not have the proper controls in place to deny access. The problem is even more acute for the first few hours that a domain is online. The second problem is the "forgotten domain." Often, an adversary will register a domain and let it lie dormant for several months at a time. When they finally decide to use the domain for dangerous practices, the domain — which is neither on a good list nor bad list — slips through DNS detection.

Infoblox decided to build a threat intelligence service based on its comprehensive DNS tracking. In detail:

- **Infoblox maintains 20 billion–30 billion records on DNS transactions every day.** The DNS record would include how domains are in contact with one another — essentially, DNS routing.
- **Infoblox is actively tracking 4 million DNS records from known threat actors.** This might be the most trenchant weapon in the Infoblox service. Think about a specific threat actor or a nation state. It must have a routing mechanism. In the longer sense, routing can include C2 activities to home sites and back out to dark web markets. If this routing is understood, the domain or the IP address can be blocked.
- **Infoblox discovers 3.5 million high-risk and malicious domains each month.** This statistic is important in and of itself; however, there is a hidden but significant benefit to blocking domains at the DNS request protocol. Infoblox estimates that DNS query blocking reduces 50% of the load on the internet ingress/egress firewall. Successful blocking alleviates stress on the endpoint detection and response (EDR) agent/cloud apparatus as well.

- **Data science is deployed on top of DNS transactions.** Remote Access Trojans (RAT) have distinctive characteristics compared with other types of legitimate internet transactions. Obviously, several types of modeling around entropy between DNS communications can be a reliable indicator of compromise. IDC cannot verify this, but Infoblox claims that its threat intelligence detections have a .0002% false positive rate.
- **DNS can be used for cybersecurity-adjacent use cases.** Two use cases come to mind. Increasingly, when companies enter into a merger or acquisition, the overall cybersecurity hygiene of the company to be merged/acquired is becoming a factor during purchase. Moreover, DNS DR can help in securing supply chains. Often, original equipment manufacturers or other types of products require tens to hundreds of vendors to make a product complete. The reliability, availability, and cost of components from vendors is key to these relationships, but supply chain safety is also a factor.
- **Infoblox can block 60% of threats before the first DNS query and block 82% of malicious queries within the first 24 hours by combining known adversarial tactics with data science and comprehensive DNS records.** Threat campaigns discovered by Infoblox include Decoy Dog, Profiling Puma, Savvy Seahorse, and VexTrio Viper.

The Infoblox DNS DR can be deployed as either a software appliance or a remote SaaS application or even an agent installed on an endpoint. In addition, DNS DR is available for AWS and Azure environments.

ADVICE FOR THE TECHNOLOGY SUPPLIER

Usually, vendors offering a cybersecurity product or service have to educate the potential client about the mechanisms of its solution. The client already uses DNS. In this case, persuading a client to consider DNS-related security products for threat intelligence has the virtue of providing proactive defense while not requiring any CPU for the network. In detail:

- **Recommend the use of response policy zones.** The RPZ itself acts like a firewall granting individual users access to known good sites and blocking access to bad sites. A "block" is the default setting for unknown sites. Smart RPZ architecture in combination with access control lists essentially establishes a DNS firewall with zero trust–like controls.
- **Focus on integrations toward visibility with NDR and threat intelligence vendors.** An NDR platform is designed to account for events

that happen at ingress/egress to and from the internet. It is the last bastion of hope after point products. DNS DR is a pan-telemetry vantage point for all DNS connections. The DNS DR perspective unifies the perimeter and post-perimeter defenses. Collaborating with threat intelligence vendors will help to find threat actors that may have what appear to be legitimate sites. When threat intelligence vendors determine the motivation of threat actors, these activities may possibly be retrofitted to HTTPS sessions to further trace the footsteps of the adversary.

- **Integrate with SIEM, firewall, antivirus, and IT ticketing platform providers toward response.** Aside from RPZ — which can be updated — added information about domains stays siloed without integration with either SIEM or antivirus or firewalls or IT ticketing systems or endpoint protection platforms. SIEM is an especially powerful integration as bad domains can be searched for in SIEM to possibly find the earliest existence of the adversary on the network. Of course, integrations with antivirus, firewalls, and endpoint protection systems can block an intrusion as well. In the past few years, automation has become more prevalent in IT and security functions. However, many IT and security operations systems still rely on tickets to generate a workflow.
- **Use DNS as a platform for detection and response or threat intelligence as it does not require an agent.** IT and cybersecurity teams are in a constant battle to keep enough headroom for a smooth end-user experience and proper cybersecurity vigilance on a given machine. There are any number of agents on a machine, and even lightweight agents require CPU. The worst thing is that agents can be compromised by attackers, degrade over time, or be dropped altogether in software upgrades. DNS enforcement does not require agents.
- **Use DNS in the incident detection and response life cycle as it is both preventative and proactive.** Businesses often toggle between prevention and detection but DNS-based observability for cybersecurity offers both.

Other Competitive Approaches to Infoblox

We are lauding Infoblox for its DNS-based cybersecurity approach in both detection and response and threat intelligence, but this is part of a greater fusion of technologies involving DNS and IP addresses. While IDC believes that Infoblox has an early-mover advantage, we also believe that the following technologies and the companies that offer products/services could conceivably adapt their platforms to do much of what Infoblox is doing. In detail:

- **DNS resolver protection services:** The DNS resolver protection is generally used as an IT/OT function where businesses can establish good lists and port the good list to the DNS resolver. Cisco Umbrella, DNSFilter, DomainTools, EfficientIP, OpenDNS, and OpenLabs are companies with this technology. DomainTools provides both an investigation platform and a predictive risk score for newly accessed domains. DNSFilter has roughly 1 billion domains that it has cataloged. In addition to tracking domains, it also monitors proper usage of SSL, analyzes images, and has scanning and metrics to determine if a website is legitimate.
- **Third-party risk management (TPRM):** TPRM is a vast category that can include aspects of governance, risk and compliance, identity, and vulnerability management. In this case, we are addressing companies like Bitsight, Panorays, SafeDNS, and SecurityScorecard. This type of technology provides a comparative posture-assessment score that can be based on attack surface management, vulnerability scanning and exposures, IP reputation, and DNS health among other considerations. It is worth noting that SecurityScorecard has had a threat intelligence service for roughly three years now.
- **Threat intelligence providers:** As a part of digital risk protection, companies such as Recorded Future, CrowdStrike, Mandiant, and ZeroFox monitor the dark web for market activity, monitor individual identities, and tie threat actors to threat tactics. They may not have the breadth of DNS monitoring that the DNS resolver service providers do, but their threat intelligence is directly linked to threat actor activities.
- **Attack surface management (ASM):** Traditional vulnerability management performs internal scans while attack surface management platforms scan the internet, provide an external view of an organization, and surface weaknesses in systems where cyberattackers could take advantage. The adversary can literally inventory and try to map all the internet-facing assets that a company may have. What ASM does is beat the adversary to the punch by taking an external view, suggest remediations such as installing patches or certificates, and maybe suggest different routes. In truth, ASM has become more of a prevention cybersecurity technology, but the principle of domain and IP address comprehension and how it can be leveraged remains (for more information, see *Worldwide Attack Surface Management and Breach and Attack Simulation Software Forecast, 2024–2028: Proactively Discovering Potential Attacks*, IDC #US50272123, February 2024).

Summary

The internet — despite its security exposures — remains a marvel of technology, particularly due to protocols like the domain name system that facilitate seamless online interactions. This document delves into the critical role of DNS in cybersecurity, emphasizing its potential in threat prevention, intelligence, and detection and response. Businesses, regardless of size, typically operate a dedicated DNS server to avoid latency issues and security risks associated with using an internet service provider's DNS. This setup is crucial for both IT operations (which aim for network efficiency) and security operations (which focus on threat mitigation).

DNS serves as a common ground for IT and security teams, enabling the creation of "good lists" and "bad lists" to manage access. However, the scope of DNS extends beyond intranet and internet activity, offering a comprehensive view of all public DNS sessions. This visibility is invaluable for forensic investigations and monitoring devices that cannot host traditional security agents such as operational technology devices.

This document highlights the necessity of DNS hygiene and the dual nature of DNS as both a facilitator of smooth online transactions and a target for adversaries. Attacks like DNS reflection and distributed denial of service (DDoS) highlight the vulnerabilities associated with DNS servers. Despite these challenges, DNS remains a preferred technology for detection and response due to its ability to provide insights into domain-to-domain connections and post-perimeter monitoring.

Infoblox emerges as a key player in leveraging DNS for cybersecurity, offering services that improve threat detection and response. Its DNS DR service, for instance, has been shown to reduce mean time to respond by 34%. Infoblox's approach to threat intelligence is particularly noteworthy, focusing on the contextual information surrounding threat actors and the dynamic nature of domain registration. By maintaining billions of DNS transaction records and actively tracking malicious domains, Infoblox provides a robust defense mechanism against cyberthreats.

This document concludes with advice for technology suppliers, emphasizing the importance of educating potential clients about DNS-based security products. It suggests focusing on response policy zones, integrating with network detection and response platforms, and leveraging DNS for both preventative and responsive cybersecurity measures. In addition, it acknowledges the competitive

landscape by mentioning other technologies and companies that could adapt their platforms to offer similar benefits.

In summary, DNS plays a pivotal role in cybersecurity, offering unique advantages in threat detection, intelligence, and response. Infoblox's innovative use of DNS demonstrates its potential to significantly enhance cybersecurity measures, making it a critical tool in the fight against cyberthreats.

LEARN MORE

Related Research

- *IDC Market Glance: Threat Intelligence, 2Q24* (IDC #US52358624, June 2024)
- *Worldwide Threat Intelligence Forecast, 2024–2028: Beyond Reaction — The Rise of Predictive Threat Intelligence* (IDC #US51961824, April 2024)
- *Market Analysis Perspective: Worldwide Threat Intelligence, 2023* (IDC #US51245623, September 2023)
- *Worldwide Threat Intelligence Forecast, 2023–2027: Is There Room for Individual Vendors to Make Money While Serving the Greater Good?* (IDC #US50210623, June 2023)
- *IDC Market Presentation: Worldwide Threat Intelligence Report: Observing the Adversary When They Retreat to the Dark Web and Behind Social Media* (IDC #US50480023, March 2023)

Synopsis

This IDC Market Perspective focuses on how Infoblox leverages the domain name system (DNS) to enhance cybersecurity through detection and response and threat intelligence. By utilizing DNS, Infoblox provides visibility into domain-to-domain connections and identifies indicators of compromise, significantly reducing mean time to respond by 34%. Infoblox's approach — which includes maintaining billions of DNS transaction records and actively tracking malicious domains — offers a novel and effective method for preemptive threat blocking and cybersecurity management without the need for additional network agents.

"DNS is the unsung hero in cybersecurity, transforming threat detection and intelligence with every query. Infoblox elevates DNS from a basic network function to a cornerstone of cybersecurity strategy." — Christopher Kissel, research vice president, Security and Trust at IDC

"Through DNS, we uncover the hidden narratives of cyberthreats, offering unprecedented visibility and response capabilities." — Monika Soltysik, senior research analyst, Security and Trust at IDC

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, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps 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.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC report sales at +1.508.988.7988 or www.idc.com/?modal=contact_repsales for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2024 IDC. Reproduction is forbidden unless authorized. All rights reserved.