White Paper

Cloud Security Services Provides the Next Generation of Protection

Sponsored by: Neustar Inc.

Philip D. Harris, CISSP, CCSK
November 2021

IDC OPINION

While internet threats are not new, they are problematic and can severely disrupt a business. As attacks continue unabated, organizations must adapt and even extend protection even further than the confines of their datacenters and networks. The post-COVID-19 pandemic world and the race to digital transformation (DX) have introduced the new edge that extends well past the traditional organizational boundaries.

With the addition of the new edge, the overall attack surface has grown dramatically for most organizations that, in general, feel they may not be prepared to withstand or prevent the continued variety of attacks that come as a result. As the "edge" continues to expand with the inclusion of IoT, VPN usage growth, multicloud environments, and application development, this creates fertile ground for attackers to find new and creative ways to exploit weaknesses.

This is where many organizations appear to be struggling with the choices to protect themselves. Do they continue extending on-premises security solutions, or do they venture to the cloud for protection services? Organizations can choose to go it alone and try and fend for themselves, or they can seek out cybersecurity services to take on the lion's share of security and protection against the various threats. This is where cloud-based security solutions can provide protection as a natural extension of the traditional suite of security solutions.

Neustar is one such company with a portfolio of cloud security services. Neustar offers an integrated suite of network and application security solutions and capabilities that include web application firewall (WAF), distributed denial of service (DDoS), DNS services, security intelligence, and bot management. Neustar has continuously added security features to address both the current and future needs of their customers. According to customers, Neustar security solutions deliver the protection they need consistently. Neustar customers also tend to be satisfied long-term customers that have built a partnership over time.

Organizations should consider augmenting their current suite of security solutions with tools that are specially designed to deal with today's evolving security issues. Taking advantage of Neustar's cloud security services as an integrated suite specifically designed to reduce the risk of attack will have organizations on much better footing to withstand or prevent such attacks. The ability to prevent attacks from entering the network perimeter will enable organizations to focus their attention on various other priorities.

IN THIS WHITE PAPER

This IDC White Paper highlights Neustar security services that secure a company's digital presence against risks and downtime through their cloud-based application and network security capabilities, DNS security, and security intelligence. In today's world of growing dependence on digital landscape expansion, companies are becoming more reliant upon cloud-based security services that protect both the company and customers they service.

SITUATION OVERVIEW

Introduction

When organizations think about cloud security, certain topics come up such as DDoS protection, web application firewalls, DNS security or, even, bot security. However, there seems to be some confusion across buyers such that if they have DDoS security protection, they seem to think they automatically get WAF protection, or if they have WAF protection, they may think they get bot protection as a result. What buyers need to understand is that these are discrete protection services that, on the one hand, operate separately and differently from each other, but on the other hand, these services can operate together as a consolidated layered set of services that are knit together such that they share intelligence and inform each other to provide the optimal layered protection.

It's very similar to how traditional security architectures work where there are different solutions that provide different and unique security protection, but in the total, they contribute to the overall protection of the environment. For example, if you buy an antimalware solution that doesn't mean you automatically get EDR capabilities, or if you buy a network firewall, you don't automatically get a web application firewall. Cloud security services work in very much a similar fashion. The only difference is that it is an extension of the traditional security architecture that is managed and operated solely from the cloud. In many ways, this added layer of cloud protection can prevent or significantly reduce the risk of attacks such as disrupting business operations, loss of data or intellectual property, or brand or reputation damage.

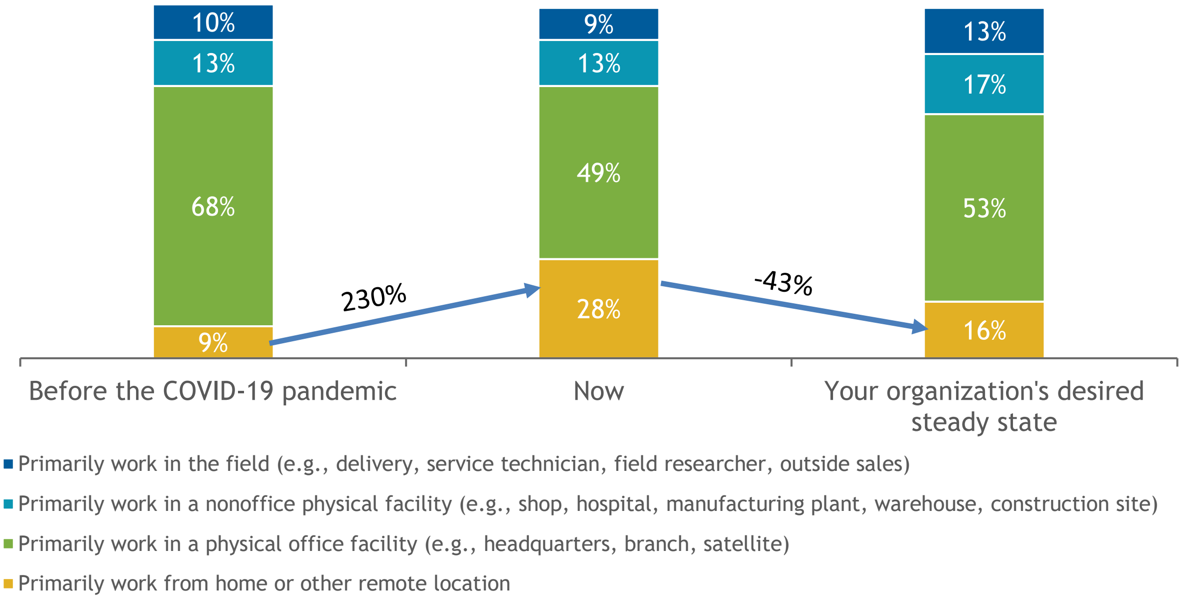
Neustar is one such company that provides a set of cloud security services that is an extension to traditional security architectures. Cloud security services have become a crucial next layer of security to protect companies from evolving attacks especially since the advent of the pandemic, explosion of remote workers, drive to digital transformation, and dramatic growth in IoT devices.

The dramatic rise in remote workers since the beginning of the pandemic has resulted in changes to the security profile of organizations as these remote workers effectively become the new edge in many cases through the increased use of VPNs. According to IDC, over 50% of the post-COVID-19 workforce is expected to work either completely from home or in some hybrid fashion (see Figure 1). This has also resulted in growth in exploitation of yet another attack vector for adversaries.

FIGURE 1

Rapid Workforce Realignment

Q. *What percentage of your company's workforce was, is, or is expected to be in each of the following categories?*



n = 791

Note: Steady state means that an organization has reached a relatively stable condition that does not change significantly over time.

Source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 6,* July 2021

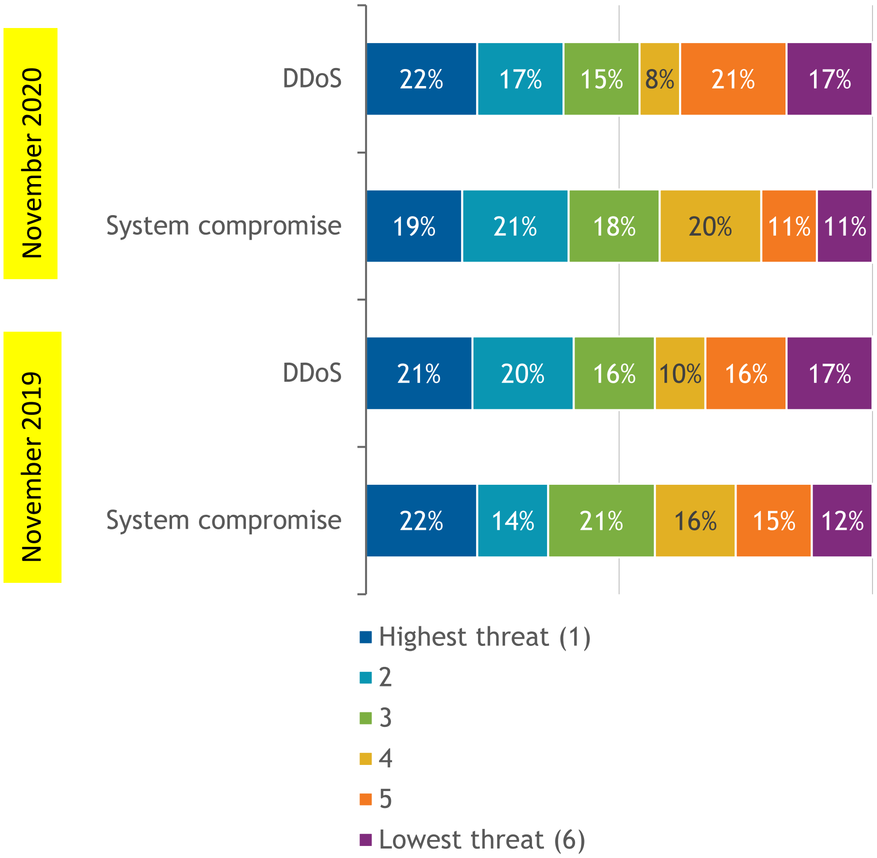
Other results of the transition to the new normal of business have shown a shift of business processes and technologies to become more ecommerce dependent regardless of whether these companies were ready or not. The move to digital transformation has accelerated in 2020 bringing a slew of new threats. In *Cybersecurity Risk Management Lags with Digital Transformation* (IDC #US47988920, June 2021), it was noted that with the race to DX, organizations were willing to tolerate more risk to be first in the marketplace, with 17% indicating less business risk as a result from DX, whereas over 42% indicated the needed outcome to reduce risk over the next two years. This lack of cybersecurity has introduced more threats due to the relative newness of DX solutions.

As organizations invest in a "cloud-first strategy," they're moving swiftly to the cloud where attackers take great advantage of this by wreaking havoc with increased DDoS attacks to cause a major data breach or business disruptions. While DDoS attacks have gotten more sophisticated over time, the increase of DDoS attacks becomes apparent as organizations extend the traditional network borders to the new edge including cloud and remote workforce. From a survey that Neustar conducted among its clients (see Figure 2), DDoS attack concerns have risen ahead of system compromise concerns from 2019 to 2020.

In a recent article from *Business Insider,*[1] 2022 is expected to be the first trillion-dollar year for online retail sales. With that growth, businesses may not be ready for the rise in attacks as they are lined up in the crosshairs of attackers. Additional capabilities in the form of a type of cloud security layer are needed. Solutions that provide at least DDoS, bot, DNS services, and web application firewall protection are coming to the forefront to address this growing and ever-changing set of needs.

FIGURE 2

Cyberthreats Ranked in Order of Level of Concern, November 2019 and 2020



Source: Neustar's *NISC Survey,* 4Q20

Neustar Cloud Security Services

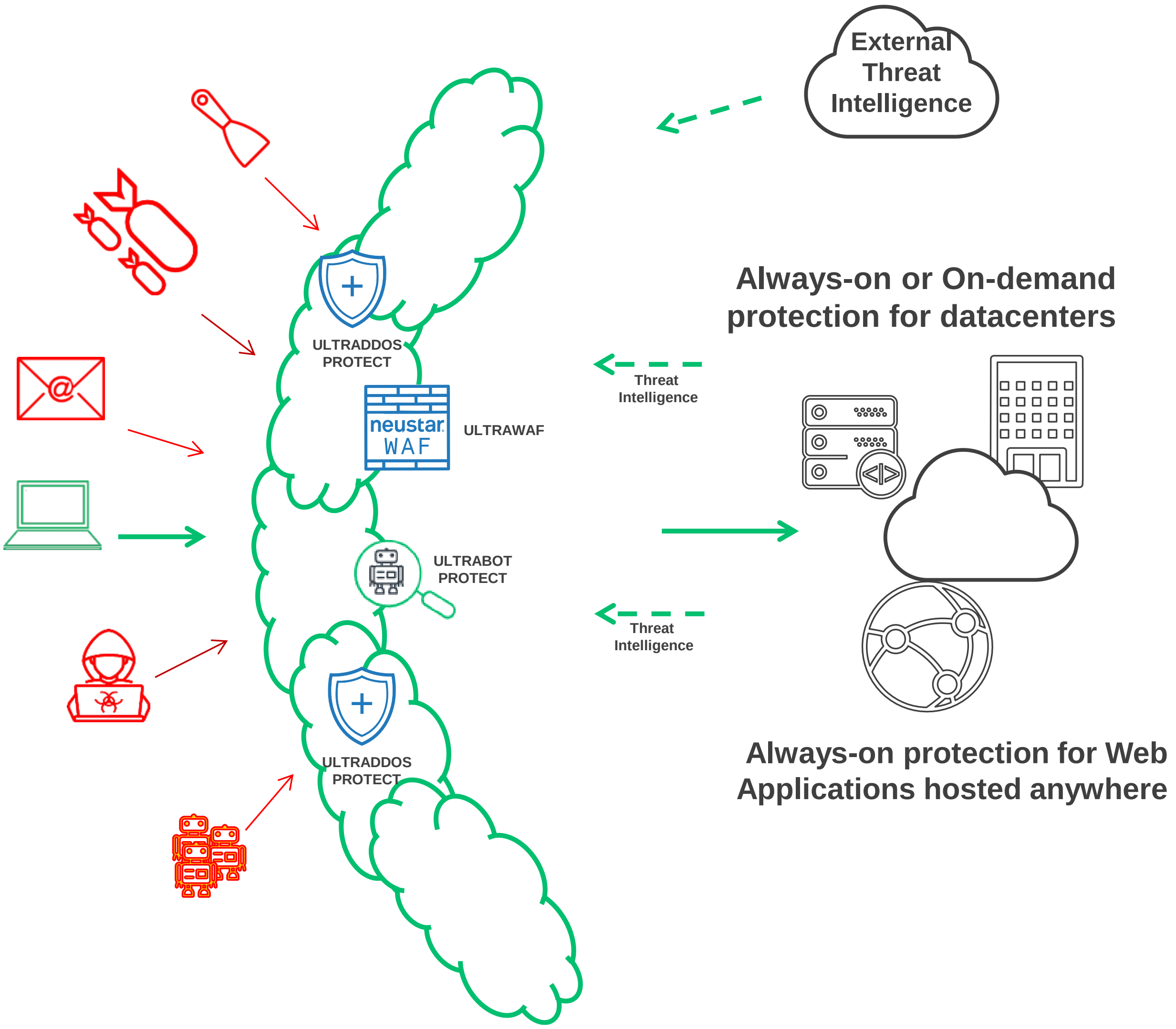
Neustar offers a comprehensive cloud security solution with protection from DDoS, bot, web application, and DNS attacks all through a cloud-agnostic set of security services with integrated security intelligence. Neustar's offerings come in the form of a SaaS offering with various discrete

[1] For more details, see *2022 is expected to be the first trillion-dollar year for online sales, largely thanks to the COVID-19 pandemic,* March 15, 2021, *Business Insider.*

services that include DDoS protection, web application firewall, DNS protection, dynamic bot management capabilities, and security intelligence (see Figure 3).

FIGURE 3

Neustar Cloud Security Services


External Threat Intelligence
Always-on or On-demand protection for datacenters
ULTRADDOS PROTECT
neustar WAF
ULTRAWAF
Threat Intelligence
ULTRABOT PROTECT
Threat Intelligence
ULTRADDOS PROTECT
Always-on protection for Web Applications hosted anywhere

Source: IDC and Neustar, 2021

DDoS Protection

Neustar asserts it has one of the largest dedicated scrubbing networks in the world with 12TBps+ of scrubbing capacity to aid customers in remaining available during the most aggressive of DDoS attacks. This solution is offered as a cloud-based service.

The cloud-based UltraDDoS Protect can be the optimal solution for customers that prefer a cloud-first strategy maintaining little on-premises infrastructure or for customers that prefer to have a minimal amount of on-premises hardware. Traffic is mitigated in minutes based upon customer needs whether DNS or BGP redirection is required leveraging Neustar's DNS services. Another key feature is the VPN protection capability that ensures employees connecting from home or offsite locations are not subject to DDoS attacks by proxying VPN traffic through Neustar's VIP proxy strategy that strips malicious traffic and routes all traffic through the UltraDDoS Protect infrastructure. In addition, Neustar will manage SSL certificates and encryption throughout its solution.

WHAT NEUSTAR'S CUSTOMERS SAY

"Neustar's security services have helped us to protect our networks for over 15 years. We trust them."

"Layered protection is the only way to ensure coverage. Neustar has successfully mitigated DDoS attacks on our network. Their solutions work!"

During the pandemic, VPN protection allowed customers to quickly move employees or contractors to work from home (WFH), reducing the risk of disruption to business activities. Neustar's NetProtect supports 100GBps clean data bandwidth and connects with the UltraDDoS Protect platform from more than 500 datacenters with multiple tier 1 partners around the world ensuring the most minimal amount of network latency, thereby ensuring less impact to customer experience.

Web Application Firewall

Neustar's WAF solution, known as UltraWAF, bridges the gap between more traditional on-premises services sets providing lighter-weight filter list-based cloud capabilities. Neustar's belief is that in addition to protecting against traditionally known bad activity, the solution must be able to continually change and mature as attackers change and mature their tactics, techniques, and procedures.

So, while providing an automated machine learning- and artificial intelligence (AI)-based learning mode is important, it is also important to have tools to apply very specific, very targeted rules for the organization's environment at the same time. Neustar's capabilities are integrated with the company's own custom intelligence sets such as IP Geo data, IP reputation data, and IP intelligence data. This allows customers to spend more of their precious time and efforts to analyze, investigate, and take action.

Key features of Neustar's UltraWAF include:

- **Agnostic –** UltraWAF is a cloud-, hardware-, and environmentally agnostic solution enabling customers to protect their applications anywhere these are hosted. This provides customers with the ultimate flexibility and negates being forced to use other WAF vendor networks or other proprietary technologies, eliminating costs that customers would otherwise have to pay. Another key feature is the flexibility to configure consistent rules without any restrictions.
- **OWASP protection –** While UltraWAF is configured to defend against all of the OWASP top 10 vulnerabilities, Neustar has taken great care to bring added focus to the most common threats critical applications are faced with such as SQL injection, cross-site scripting, cross-site request forgery, and buffer overflow.

- **Zero-day threat protection –** UltraWAF is designed specifically to offer protection against zero-day threats or attacks that feature malformed packets or non-RFC-compliant traffic.
- **Negative and positive security –** UltraWAF supports both negative and positive security methods. Negative security assumes that all traffic is allowed except already identified threats or attacks, while positive security ensures that unless traffic is explicitly permitted, it is denied. Traffic heuristics also provide the ability to match profiles against known online traffic for organizations' applications.
- **Learning mode –** UltraWAF's unique learning mode enables profiling of traffic over time and recommends new rules based on profiling to distinguish between legitimate application traffic versus anomalous behavior. Appropriate rules based upon the results are then applied.
- **Signatures –** UltraWAF offers a policy editor that enables customers to create their own rules across a variety of formats as well as provides the option to continuously add new threats (signature protection for CVE and CWE, such as CMS vulnerabilities) captured by the Neustar threat research team.
- **Certificate protection –** UltraWAF leverages a hardware security module (HSM) to securely protect and store sensitive digital certificate information, providing an added layer of security for encryption processes.
- **Ease of administration –** The UltraWAF portal enables seamless administration to manage all security features and capabilities instantly. Reporting and logging features allow administrators to inspect and analyze all aspects of UltraWAF security.
- **On-premises traffic reduction –** Since UltraWAF is positioned between organization's network and the internet, UltraWAF can easily filter out bad traffic, reducing the overall network load prior to reaching your on-premises applications.

DNS Services

Neustar's UltraDNS and UltraDNS Firewall capabilities provide and enable security, reliability, and performance for organizations that count on their internet presence to continuously drive their businesses forward.

With UltraDNS, organizations can outsource their DNS completely or take advantage of secondary DNS services. This service leverages IP Anycast routing and can handle over 10 trillion global DNS queries per day. Neustar's DNS network is built upon a proprietary non-open source application that reduces risks to online and zero-day threats. In addition, it provides nameserver segmentation and DNSSEC support to further reduce the risk of malicious activity.

Neustar's UltraDNS Firewall is another feature that provides additional methods to prevent threats from making their way to an organization's network. It acts very much like an early warning system by identifying threats and malicious activity well before any corporate assets are impacted. Other features include the ability to prevent access to known malicious sites and prevent inappropriate content through category and custom filtering lists.

Dynamic Bot Management

Bots are not a new problem that attackers bring to the world. Attack automation using bots has enabled attackers to increase both duration and scale against companies that are targeted. Bot focus has changed to target the application layer as resources have moved to the cloud, applications have become more complex, applications have become more dependent on open source components, and security teams are stressed to keep up with patching of components. The recent pandemic has driven more work to online services. As such, the surface area to protect has increased exponentially opening more potential for attackers to find newer ways to increase both fraud and logic abuse through credential stuffing, content scraping, stream manipulation, or shopping cart attacks.

Neustar has introduced the UltraBot Protect capability that addresses many of the bot threats companies are faced with, such as exploiting application vulnerabilities, and Neustar has bundled UltraBot Protect with UltraDDoS Protect and UltraWAF to create an impressive array of cloud security features built upon a solid foundation. UltraBot Protect provides the following initial key features, with more features planned for rollout over time:

- Block Lists and Allow Lists are customizable lists leveraging IP addresses, subnets, and policy expressions that are either prevented from accessing or allowed to access web applications.
- IP Reputation ensures that bot traffic from malicious IP addresses is examined.
- BOT Rate Limits examines inbound requests that are received within a predefined period of time from either a client IP address, a session, or a configured resource (e.g., URL).
- Device Fingerprinting reviews incoming traffic to determine whether the originating device has a fingerprint in the incoming request header and browser attributes that could be considered malicious or that should be blocked or notified about.
- BOT Traps examines incoming bot traffic to determine whether it's from a human versus automated bot, and based upon the results, it will route the bot to a BOT Trap URL to block any further traffic.
- BOT Transactions Per Second (BOT TPS) detects incoming bot traffic and compares requests and percentage increase against a preconfigured time interval.
- Challenge Expression, such as Captcha, is used to detect whether inbound traffic is from a human versus automated bot by presenting a challenge expression (e.g., CAPTCHA or Java challenge) and will block automated bot traffic that fails.

Security Intelligence

To keep abreast of all the various threat and attack activity, security intelligence is of utmost importance. As organizations around the world work to prevent being the next victim of a data breach or other form of compromise, many are clear they do not possess enough intelligence information about the unique attack patterns or attacker communities. This is why many organizations seek to obtain threat intelligence from a number of different types of sources such as open source intelligence, social media intelligence, human intelligence, technical intelligence, or intelligence from the dark web.

Various technology vendors also provide their unique types of threat intelligence that is specifically derived from their own solutions and tailored to address their customer needs for protection. Neustar is such a vendor that has leveraged its own ecosystem to generate and curate current and actionable threat information forming its own unique perspective on internet activity known as UltraThreat Feeds.

Neustar UltraThreat Feeds are a proprietary body of near-real-time threat data used to detect potential threats and identify and stop bad traffic, both inbound and outbound. Neustar leverages the DNS exhaust from its globally distributed network of authoritative and recursive DNS service sites. Altogether over 100 billion lookups are processed every day. Through machine learning and artificial intelligence, the data is continuously analyzed to create focused threat feed information, enabling customers to detect and neutralize rapidly evolving threat before there is any serious impact or disruption.

With the Neustar UltraThreat Feeds, organizations can detect, identify, and stop bad traffic, both inbound and outbound. The types of malicious threats that are actioned include:

- **Malicious domain generation algorithms –** Algorithms that are used to generate domains infected with malware that connect back to command and control servers
- **Suspicious DNS tunneling attempts –** When domains use the DNS protocol to create a tunnel to exfiltrate data past customer security controls
- **Newly observed, published, or recently deactivated domains –** When newly observed domains with little or no history or when a deactivated domain suddenly becomes active
- **Domain updates (nameserver or hosting IP address) –** When there are indications that a domain has been hijacked
- **Anonymous proxies –** Identification of proxies to uncover users who are attempting to hide their location and/or activity

The Neustar UltraThreat Feeds provide an added level of certainty for customers who want to prevent unwanted threats from infiltrating their environments.

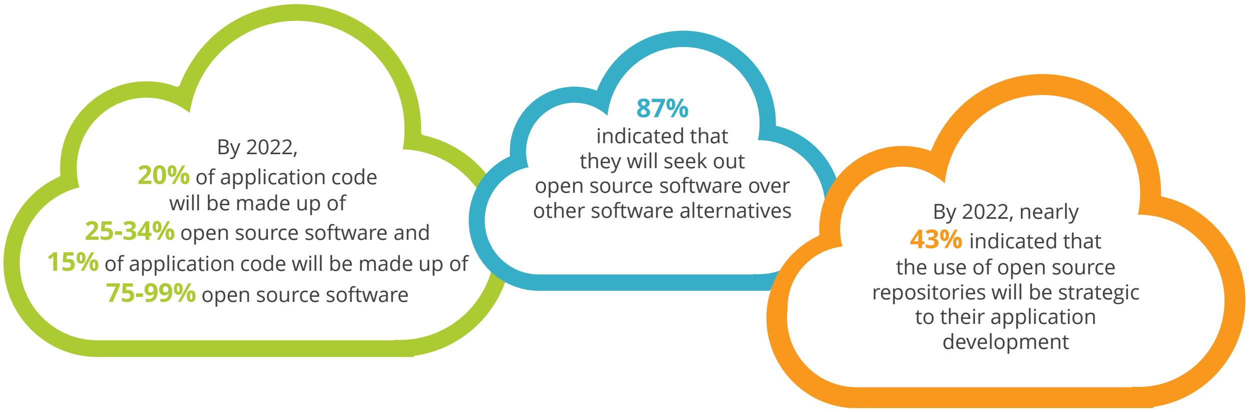
FUTURE OUTLOOK

Organizations will continue to develop, buy, or otherwise make available cloud applications to conduct various forms of business. We will continue to see growth in the use of DevOps to make this happen. It is expected that by 2022, the use of open source software and repositories will grow well beyond today's usage by DevOps (see Figure 4).

This will in turn see growth in the number of vulnerabilities from these applications if left unchecked or unaddressed. Cloud security vendors such as Neustar may be able to aid defending against this by developing or integrating vulnerability scanning capabilities above and beyond their current WAF capabilities. This will allow cloud security vendors to shield organizations from attacks and could also provide a feedback loop to customers to aid them in addressing security vulnerabilities while being shielded.

FIGURE 4

Open Source Software and Repositories for Composite Application Development



Source: IDC's *U.S. DevOps Survey,* September 2020

CHALLENGES/OPPORTUNITIES

There's been an increase in attention toward web application API security. Attackers have been focusing more attention to the API layer of web applications. Various types of attacks that can be perpetrated against APIs include injection, DoS, broken authentication, sensitive data exposure, broken access control, parameter tampering, and man-in-the-middle attacks.

To that end, Neustar has added the area of API security to its road map as a natural extension to its current capabilities. This means that Neustar will be providing a discovery capability whereby the APIs for cloud applications will be identified and protected throughout an organization's cloud presence.

CONCLUSION

Given the expected continued growth in the types of attacks against cloud environments, it is imperative that cloud security vendors continue to mature, expand, and develop services to address growth in attack surface. This attack surface begins with the new edge that includes multicloud environment expansion, growth in remote workers, exponential use of IoT, growing use of DevOps, the race to digital transformation, and strategic use of open source software and repositories.

Security organizations must view the cloud security layer as a key provision of their go-forward security strategy where there are companies such as Neustar that specialize in providing the needed capabilities such as DDoS, WAF, bot management, DNS security, and security intelligence. Otherwise, these security organizations could go it alone by cobbling together various solutions that may not integrate well and continue to exacerbate the challenges in managing multiple solutions on their own in the hopes they can prevent an attacker from some form of business disruption.

Neustar is positioned to provide such a security platform not only in its current form but as a continuously expanded platform over time to address the changing threat landscape.

APPENDIX: DEFINITION

- **Bot —** An internet bot, a web robot, a robot, or simply a bot is a software application that runs automated tasks over the internet. Typically, bots perform tasks that are simple and repetitive much faster than a person could. In the context of this paper, malicious bots are bots used to automate actions considered to be cybercrimes. Common types of malicious bots include:
  - Denial-of-service (DoS) or distributed-denial-of-service (DDoS) bots, which use an overwhelming number of bots to overload a server's resources and thus halt the service from operating
  - Spambots, which post promotional content to drive traffic to a specific website
  - Hackers, which are bots made to distribute malware and attack websites
  - Other malicious bots, including web crawlers, credential stuffing, email address harvesting, and brute force password cracking (Organizations can stop malicious bots by using a bot manager.)
- **Distributed denial of service —** A denial-of-service attack is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet.

- **Security intelligence —** In its simplest form, security intelligence is the practice of collecting, standardizing, and analyzing the information relevant to protecting an organization. This information can be generated by networks, applications, and other IT infrastructure in real time, including the processes, policies, and tools that are designed to gather and analyze the information collected. The collection and usage of this intelligence provides organizations with the ability to assess and improve their security posture as well as protect from internal and external threats.
- **Web application firewall (WAF) —** A WAF is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. WAFs can be either on premises based or cloud based.

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.

Global Headquarters

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