IDC TECHNOLOGY SPOTLIGHT

Sponsored by: CenturyLink

Organizations that do not have the core competencies to address DDoS mitigation will benefit from turning to a managed security service provider for guidance and support. This IDC Technology Spotlight examines the benefits of this approach.

Mitigating DDoS Attacks by Partnering with a Managed Security Service Provider

March 2019

Written by: Martha Gomez Vazquez, Senior Research Analyst, Infrastructure Services

Introduction

The threat landscape has become more complex and challenging for organizations to keep up with in the era of digital transformation (DX). Factors to consider include the following:

- The proliferation of distributed applications on private/public clouds or on-premises
- An attack surface that has grown because the perimeter has expanded and enabled more vulnerabilities
- The availability of connectivity and bandwidth to meet changing technological needs, which provides bad actors with more reasons to attack an organization's infrastructures

AT A GLANCE

KEY STATS

In a recent IDC survey, nearly half of respondents said they had experienced a DDoS attack this year, with 99% responding that they are already using some form of DDoS protection.

Businesses pursuing DX seek solutions that are on-premises in their datacenter as well as those that are managed or monitored in the cloud. However, as IT environments and requirements change, it is important that organizations look to providers that can ensure the availability of those services by providing network-based distributed denial of service (DDoS) mitigation controls. The new distributed enterprise has expanded the attack surface, giving attackers more access points from which to attack an organization's infrastructure and customers. Meanwhile, the availability of connectivity and bandwidth provides a much easier means by which to deliver DDoS attacks. In fact, it is very easy for cybercriminals to buy a DDoS attack through the Dark Net for as little as $20. The goal of these DDoS attacks typically is to keep legitimate users from accessing an organization's services, but attacks take place for other reasons as well.

DDoS attacks are on the rise, so corporate awareness of them has grown. These assaults have become a greater challenge as attackers become more sophisticated, especially as organizations look to digitize their business processes. As companies undergo IT infrastructure changes to support DX, complexity gets added to the mix. The security risk becomes higher because sophisticated DDoS attacks can cause performance issues by disrupting availability.

The Evolution of DDoS Attacks

DDoS attacks are increasing in size, frequency, and sophistication of techniques (e.g., short-duration variants and more application-specific attacks). Attackers have become smarter and their attacks harder to detect. And DDoS attacks are no longer focused solely on the gaming or retail industries. All organizations regardless of size and location are at risk, especially those undergoing DX. For these organizations, the attack surface will grow so the need for security takes on greater urgency.

Enterprises increasingly require that their online websites and other mobile-based services perform reliably and with no latency for their customers. Almost every organization now relies on connectivity to its online web services. Therefore, the associated risks for organizations moving through digitization without adequate protection against DDoS attacks can include loss of availability or productivity, negative publicity, and reputational damage. Organizations cannot afford to have service disruptions, so many use some sort of DDoS protection to defend against an attack. In IDC's *U.S. DDoS Prevention Survey,* nearly half of respondents said they had experienced a DDoS attack in 2017, with 99% responding that they are already using some form of DDoS protection.

Large attacks continue to be a significant trend, but other notable attacks include those from Internet of Things (IoT) devices as well as short multivector attacks designed to cause a diversion from other threats such as ransomware and the exfiltration of confidential data.

IDC's survey noted that half the respondents have experienced a DDoS attack in 2017, with most ranging from 1Gbps to 10Gbps. These attacks were complex and classified either as volumetric, multivector, TCP exhaustion, or application attacks.

Organizations are also realizing that premises-based traditional security products cannot protect against DDoS attacks. According to the IDC survey, 99% of respondents said they have purchased DDoS services or product from a DDoS mitigation provider while 95% said they have a DDoS mitigation response plan in place.

Definitions

- Digital transformation (DX) is a strategic business imperative at the enterprise level that is driving fundamental changes to how the enterprise operates, delivers services, and interacts with its customers and supply chains. DX refers to the disruption and evolution of business models, processes, and digital experiences through new technologies leveraging cloud, analytics, mobility, social media, and the IoT.

- Managed security services (MSS) are considered part of the worldwide security services market by IDC, which defines MSS as "the around-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs)."

- DDoS attacks impact the availability of customers' internet-facing applications and services. An attack typically uses botnets (a group of compromised computers) to send traffic directly or through reflective surfaces to the victim. The flood of malicious traffic generated in such an attack makes it impossible for legitimate users to access the services provided by the victim (e.g., a website).

Knowing the Different Deployment Options

In today's IT environment, there are four DDoS mitigation solutions to consider: on-premises, cloud, defense in depth, and hybrid:

- **On-premises:** These offerings typically consist of purpose-built, appliance-based products capable of mitigating non-volumetric DDoS attacks, and they can be deployed in large enterprise, government, and managed security service provider (SP) organizations. There are a variety of security products that can have DDoS prevention capabilities such as routers, switches, firewalls, and intrusion prevention systems. However, these products typically lose the ability to adequately mitigate DDoS attacks of any significant size, especially application layer attacks. These infrastructure components can be directly targeted during DDoS attacks and become network bottlenecks if dedicated solutions have not been deployed. Dedicated solutions that are deployed in front of other infrastructure devices do not rely on stateful inspection techniques and can provide visibility into the application layer recognized to adequately defend against on-premises attacks.

- **Cloud:** Telcos and cloud providers often purchase equipment from mitigation hardware manufacturers and combine that equipment with their other assets, resources, and processes to build a mitigation service offering that can be sold to enterprises and governments. These services are often cloud based and provide monitoring and mitigation via the provider's SOC and scrubbing centers. Providers typically call this the "clean pipe" option, where the provider will block network flood attacks from penetrating the customer's network. With a cloud-based offering, a customer can become aware of an attack before the provider and proactively request that the traffic be diverted.

- **Defense in depth:** In this approach, an organization will extend its on-premises appliances to include cloud signaling to allow for mitigation in cloud-based scrubbing centers. An on-premises appliance will provide defense against smaller volumetric attacks and application layer attacks. The level of visibility and quick response offered by being on-premises is arguably much higher, especially in relation to the application layer traffic. That said, large-scale volumetric attacks can quickly overwhelm an enterprise network. If this occurs, the cloud solution can divert the traffic into a scrubbing center before rerouting it back to the customer network. The on-premises solution provides valuable information about the attack dynamics that the cloud provider can then use to more efficiently clean the traffic.

- **Hybrid:** Many DDoS mitigation providers offer an on-premises solution that is tightly integrated with the DDoS mitigation provider's cloud or network-based mitigation infrastructure. The on-premises component provides additional Layer 7 mitigating controls, improved latency when not using a cloud-based mitigation, and better control of customers' certificates when inspection of encrypted traffic is required for mitigation. According to IDC's *U.S. DDoS Prevention Survey,* 47% of organizations are using hybrid deployments to protect against the broadest set of potential attack vectors. This deployment appears to be the most common deployment among large organizations (500–5,000+ employees). Attackers are turning to multivector attacks that use a combination of volumetric, state exhaustion, and application layer attack vectors that target an enterprise simultaneously. Multivector attacks are difficult to detect and mitigate. As a result, DDoS-layered defense solutions are more effective at addressing these attacks.

Benefits of a Managed Security Service Provider with DDoS Mitigation Capabilities

Protecting against DDoS attacks is challenging especially as the security landscape and IT environments become more complex. Typically, organizations do not have the technology, people, and processes to adequately address the growing number of DDoS attacks occurring daily. Organizations that do not have the core competencies to address DDoS mitigation will benefit by turning to a managed security SP for guidance and support. Companies seeking MSS should consider providers that can:

- Develop security for the entire life cycle and provide advanced security services such as intelligence/visibility, big data analytics, incident response, forensics, and advanced detection methods.
- Provide a significant global mitigation capacity and the ability to use the underlying network for additional controls (e.g., Flowspec), as well as mitigation granularity and flexibility to integrate with premises-based mitigation appliances.
- Deliver an advanced capability able to take down the command and control (C2) infrastructure producing the attack.
- Offer customer portals with features like visualization, real-time monitoring, analytics and graphs, email reports, traffic usage, incident and source of attack information, and customized reporting.
- Investigate MSS research and development areas such as cloud evolution, threat intelligence, incident response, forensics, big data analytics, and advanced detection techniques.
- Acquire and retain talented professionals to help with security needs and challenges.
- Improve efficiencies of the security spend (reduce cost).

Organizations should consider the service delivery, reputation, longevity, and security expertise of a provider, as well as its sales and onboarding processes. It is also important to evaluate how much support the provider's team of experts will provide once the solution is implemented. According to IDC's DDoS prevention survey, respondents believe that the top 3 characteristics of a provider are expertise, support and reputation, and trust. Given the existing challenges (too many threats, not enough security budget or people, and the expanding perimeter), companies are seeking a trusted provider to extend the security on its own network to protect the company at all ingress and egress points of its architecture.

Considering CenturyLink

CenturyLink is a global managed security SP that provides a comprehensive security services portfolio to enterprises and governments. CenturyLink's multilayered DDoS mitigation approach includes global DDoS mitigation infrastructure, threat intelligence, advanced analytics, forensics and support of multicarrier deployments, global Flowspec, C2 takedown capabilities, hybrid deployment delivery models, deep integration with one of the largest IP backbones in the world, and automated detection of DDoS attacks.

CenturyLink DDoS mitigation service is global with 11 scrubbing centers located across North America, Europe, Latin America, and Asia. CenturyLink provides ~43Tbps+ of mitigation defense capacity at its network edge using BGP Flowspec. The managed security SP operates a comprehensive global network that provides it with extensive visibility into security threats to better predict problems and quickly mitigate attacks, which is very important to quelling these attacks at the carrier edge.

Customers have options around how clean traffic is returned. CenturyLink uses flow-based monitoring allowing customers to see what is occurring directly with customers' internet. The services are backed by intelligence from CenturyLink's Black Lotus Labs, its threat research and operations arm, which can identify, track, and take down command and control infrastructures used for DDoS attacks. Black Lotus Labs removes ~40+ C2s per month, according to the company.

CenturyLink DDoS mitigation service is available to customers of CenturyLink and third-party internet services. The traffic is redirected for scrubbing through BGP or DNS redirect and sent to a CenturyLink scrubbing center for mitigation. Routed (BGP) customers can choose service types such as on demand or always-on. The solution provides a carrier-agnostic generic route encapsulation (GRE), as well as CenturyLink internet-integrated and private CenturyLink connection options for returning clean traffic to the customer. Customers can choose to have flow-based monitoring added that provides proactive monitoring and alerting. Those choosing basic network protection receive managed ACLs, BGP route filtering, null routing, transit interface protection, and SOC triggered and customer-initiated destination-based blackholing. Hybrid offerings are available for customers that prefer an on-premises solution and then use cloud signaling to CenturyLink's cloud-based service.

Challenges

Providing DDoS solutions in a competitive market has its challenges as organizations can partner with a variety of players including traditional managed security SPs as well as cloud, CDN, pure-play, telecom, or cable providers. The market for DDoS services is becoming very commoditized, so CenturyLink will need to up its game to remain a top provider in the market. Organizations are turning to providers that can offer easier deployment of services, such as bundled options offered by other providers. CenturyLink will need to stay competitive from a cost perspective and tailor its solutions to smaller and midsize businesses. It should also consider providing a feature-rich solution and evangelizing its expertise in the DDoS prevention market.

Conclusion

Defending against modern DDoS attacks requires the constant attention of trained professionals and mitigating controls deployed in the network. However, many organizations will not have the dedicated resources or trained experts to manage and provide the constant 24 x 7 global support needed to stay ahead of the most advanced and sophisticated attacks. Working with a trusted managed security SP offers an effective way for an organization to defend itself.

When choosing a provider, look for one that has the mitigation capacity, global scale, and visibility to spot attacks and quash them. Consider those that offer a proactive approach to removing malicious traffic and C2 infrastructure, an approach that is especially effective in combating advanced attacks that include IoT malware and infected devices. A managed security SP like CenturyLink can provide these capabilities as well as a high level of support to address attacks quickly and effectively. To the extent that CenturyLink can address the challenges described in this paper, the company has a significant opportunity for success.

> Working with a trusted managed security SP offers an effective way for an organization to defend itself.

MESSAGE FROM THE SPONSOR

As a global communications provider, CenturyLink is in a unique position to defend against DDoS attacks, especially volumetric, as we can drop the bad traffic entering our global network and direct it to scrubbing centers only when needed, reducing latency. Therefore, because of our highly distributed network edge, we can more efficiently shift the first line of defense closer to the threat source.

For example, we can block DDoS attacks upstream at the CenturyLink network edge, nearer to attack traffic origination. In fact, we have ~43Tbps+ of DDoS defense capacity at our network edge and mitigate more than 120 customer DDoS attacks daily.

CenturyLink also has the advanced capability to take down criminal C2 infrastructure that is producing DDoS attacks. Based on our global network visibility combined with advanced threat intelligence produced by our Black Lotus Labs threat research team, we remove ~40+ C2s per month to both help protect customers and keep the internet clean.

About the analyst:

Martha Gomez Vazquez, *Senior Research Analyst, Infrastructure Services*

Martha Gomez Vazquez is a Senior Research Analyst for IDC's Infrastructure Services research practice focusing on Security Services and Hardware & Software Support and Deployment. In this role, she is responsible for IDC's worldwide research and analysis on enterprise and service provider security consulting, integration, and managed services as well as hardware and software support and deployment needs.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com