White Paper

Protecting Applications and APIs in Multicloud/Hybrid Cloud: Consistent Protection Must Follow Wherever Applications Go

Sponsored by: Citrix Systems

Christopher Rodriguez
December 2019

Introduction

Digital transformation (DX) holds the potential for massive growth as businesses embrace emerging technologies to improve the precision and accuracy of messaging, increase interaction with customers, and deliver new customer experiences. However, the road to DX requires businesses to reshape their IT infrastructure with 3rd Platform technologies consisting of cloud, big data and analytics, social, and mobile. More importantly, adopting these technologies as a true platform rather than siloed systems and practices drives enterprises toward an integrated, intelligent architecture that unlocks digital innovation. A key consideration is that the adoption of public cloud infrastructure is climbing. IDC predicts that the percentage of organizations using public cloud services will grow from 58% in 2018 to over 70% in 2019. The agility and scalability of public cloud have unleashed a torrent of application development, with an entire generation of cloud-native applications being built to enable DX use cases.

Yet security has proven to be a speed bump on this path. IT organizations have identified numerous challenges in attempting to translate traditional security models to cloud environments. Organic cloud adoption has resulted in applications being deployed across multiple cloud providers and on-premises systems, making it difficult for IT organizations to optimize security operations and ensure consistent protection for all applications. That challenge is only increasing — up to 90% of new enterprise applications will be designed and built to be cloud native by 2022. With the growing popularity of microservices design principles, aggressive development practices called continuous integration and continuous delivery (CI/CD), and code reuse, applications are becoming more numerous as well.

More applications, emerging technologies, and changing computing environments require a realignment of security practices to ensure a successful and secure move to the 3rd Platform. This white paper outlines the threats and challenges targeting applications today as well as new techniques and solutions for defending applications and application programming interfaces (APIs).

New Technologies and Threats Escalate Risk

As technology changes, cybersecurity practices have tightened, requiring the security industry to collectively rethink and redefine the ideal control points for cybersecurity. Gradually, the industry is converging on applications, users, devices, and data as the key cybersecurity control points. Web applications are particularly important — web applications enable businesses to interact with all types of users, including employees, customers, and partners. Understandably, web applications are a growing target for attackers. In addition, new technologies such as APIs and threats such as bots represent a new landscape of cyberthreats for IT organizations to navigate.

Applications Are Increasingly API Driven

Application development is shifting from massive monolithic applications to smaller component services that are assembled into composite applications. These application components are more scalable, portable, and modular, enabling CI/CD practices. Application programming interfaces have emerged as the most appropriate method to connect these applications and application components. APIs standardize and streamline the process of exchanging data with an application. The benefits of API adoption include the ability to provide predictable, predefined, and regulated communications between applications.

API adoption has accelerated in recent years, especially as APIs provide the means to coordinate communications from applications to other applications and Internet of Things (IoT) devices. The ProgrammableWeb API database now includes over 22,000 APIs and grew at a 30% higher rate in 2019 compared with the previous four years.[1] IDC estimates that by 2022, 90% of new applications will be developed as cloud-native applications, with agile methodologies, and based on a hyperagile API-based architecture (see *IDC FutureScape: Worldwide IT Industry 2020 Predictions,* IDC #US45599219, October 2019). Threat actors have identified APIs as a new threat vector and are increasingly directing attacks toward APIs or probing for vulnerable APIs.

Encryption Is Everywhere

Encryption is a fundamental technology that facilitates business transactions; governments and enterprises have long recognized the value of their data and the need to obscure this data from prying eyes. However, a broader cultural shift has occurred as well, as data privacy and security have gained importance globally. Now, most web traffic is encrypted, and the amount of HTTPS traffic continues to increase each year.

However, encryption has proven to be a double-edged sword as threat actors now use encrypted communications streams to obscure their activity and evade defenses. Typically, internet traffic passes through a number of security devices and inspection points that peer into various levels of the packet to check for threats. However, encrypted traffic must first be unencrypted before it can be inspected. The process of unencrypting traffic is compute intensive and adds latency. Essentially, encryption challenges IT organizations to consider how and where to inspect encrypted traffic without impeding network performance. An organization may require the ability to pass traffic through multiple security tools while needing to avoid decrypting the traffic more than once.

Modern Threats Use Automation

The threat landscape is further amplified by the use of automation to amplify attacks. In particular, bots are used to automate attacks of all kinds and all severity, ranging from anticompetitive (such as data scraping or inventory blocking/hoarding) to outright malicious (fraudulent purchases/transfers or account takeover).

Note that not all bots are malicious; bots are used for benign or beneficial purposes such as web indexing or for sharing data with partners. Blocking benign bots can be problematic – for example, blocking Googlebot can effectively delist a site from Google search results, making it difficult for customers to find product information. This fact introduces more complexity into the security equation.

[1] More information is available at https://www.programmableweb.com/news/apis-show-faster-growth-rate-2019-previous-years/research/2019/07/17.

It is not enough to identify a bot, and risk assessment and management must be based on the intended effect and the actual effect of the bot's programming. For example, bot activity that is not malicious but is disruptive or unintentionally malicious (e.g., skewed metrics or reduced performance) is likely to be considered unwelcome by business leaders. Likely, IT organizations will have to navigate a minefield of considerations outside the scope of "maliciousness" when determining what bot activities to police.

In addition, risk posture will vary tremendously from industry to industry and business to business. For example, data scraping may present a nuisance to one organization but could rise to the level of existential threat for online communities oriented around user-generated content. In the latter case, content scraping can lead to the loss of intellectual property, and automation can drive users away from the afflicted site in droves. In retail, bots can be used to gather data, such as pricing and inventory data, from competitors. Bots lend these operations a massive level of scale that can overwhelm smaller competitors, with Diapers.com representing a cautionary tale of uncontrolled price scraping becoming a business killer.

The 3rd Platform Challenges Traditional Application and API Security Models

The DX trend is converting businesses into digital innovation factories. According to *IDC FutureScape: Worldwide IT Industry 2020 Predictions* (IDC #US45599219, October 2019), "by 2025, nearly two-thirds of enterprises will be prolific software producers with code deployed daily." The adoption of 3rd Platform technologies including innovation accelerators such as big data and analytics and cloud is key to enabling digital transformation. But the rapid adoption of new technologies has opened new threat vectors for cybermiscreants and presents logistical challenges for security operations (SecOps) teams to address. Traditional security practices are hampered or complicated by legacy tools that hinder speed or lack visibility. Similarly, the growth in application development yields a concomitant explosion of logs and data that challenges security operations center (SOC) teams. These challenges will require a commensurate advance in security tool capabilities as well as an architectural realignment to meet the demands of DX.

Legacy Tools Hinder SecOps Teams

DX is driving an explosion in the number of applications; by 2023, over 500 million new digital applications and services will be developed and deployed using cloud-native approaches. Code reuse, new tools, more developers, CI/CD, and aggressive application development are accelerating innovation and improving business outcomes. However, applications have become more complex, and aggressive development practices may propagate vulnerabilities and increase risk. Of course, attackers have also taken notice and are increasing their focus on applications and application layer attacks. For example, 41% of IDC survey respondents were targeted by a Layer 7 distributed denial-of-service (DDoS) attack in 2018.

For SOCs, the increase in applications and application layer attacks coincides with an unmanageable increase in the number of logs to review and investigate. In a recent IDC survey, only 12% of organizations claimed to be able to review and clear all security alerts, which means that 88% of organizations are leaving some alerts unchecked. The metaphor is well worn but remains applicable: Security analysts are challenged to find "needle in a haystack" indicators of compromise.

Simultaneously, threat actors have honed their craft, becoming more creative and elusive and using automation to test defenses. The static rules used for OWASP Top 10 threats such as cross-site scripting (XSS) and SQL injection have proven susceptible to both false positives and evasion tactics. Legacy tools that generate too many alarms and false positives are considered nuisances, leaving an opening for security teams to miss true positives.

Multicloud/Hybrid Cloud Presents Unique Challenges

Cloud computing has been embraced by businesses of all sizes. In IDC's 2018 *CloudView Survey,* respondents cited "business agility" as the most important benefit of public cloud services. However, the same survey shows that "security" is the top inhibitor to adoption. Cloud adoption has been largely unplanned, driven by end users leaving IT organizations behind. As a result, IT organizations now rely on multiple cloud platforms and a mixture of public cloud and private cloud deployments.

For security teams, enforcing policies and extending protections to cloud environments have proven challenging. Enterprise security teams may attempt to leverage built-in cloud-provided controls, extend existing security deployments to the cloud, or invest in a dedicated solution for a particular environment. Regardless of the approach taken, a consistent challenge for multicloud and hybrid cloud deployments is in integrating the products into a common management platform.

The lack of a single integrated platform hinders the ability to define and enforce policy and requires security teams to manage policies and controls across different consoles and interfaces. This may lead to a loss of security visibility, hampered threat detection, defensive gaps, and inconsistent policy enforcement.
Other challenges arise; for example, application portability and business agility can be hampered by a lack of security coverage, which can add unexpected costs and reduce value from the platform.

New Application Technologies and Practices Challenge Security Models

The nature of applications is changing — the microservices architecture emphasizes applications that are composites of smaller interconnected services, enabling aggressive development and innovation. APIs are the streamlined integration points between these applications and others, defining expected data types, formats, quotas, and requirements, such as identity or access tokens, for efficient and controlled communications.

The nature of APIs highlights a key difference in modern applications: Applications are communicating more with other applications, machines, and devices while communicating less with human end users. Related to the lack of user interface, APIs are often treated differently during the development process or overlooked during the security process. A fundamental misunderstanding of APIs, such as unrealistic expectations for "security by obscurity," can lead to vulnerabilities such as rate-limiting errors, authentication errors, and business logic exploits. In reality, attackers are able to ascertain the usage of APIs, often easily, and will direct well-known application exploits at APIs. APIs that are unprotected by a web application firewall (WAF) are vulnerable to many of the same OWASP Top 10 threats that are routinely directed at websites. In addition, WAFs that lack the ability to parse API traffic may not be able to defend against these attacks properly.

Furthermore, microservices architecture requires security tools that can secure all forms of API communications. Traditional WAFs are designed to secure "north-south" (inbound and outbound) traffic. However, API communications are not categorized strictly as inbound and outbound and may be used to communicate with other application services or internal applications. Therefore, modern security tools must be able to secure "east-west" traffic as well. Security tools that cannot support microservices and APIs introduce blind spots in the security architecture or may present a performance bottleneck.

Modern Application and API Security Requirements

As network technologies change and concepts of a defined, defensible perimeter dissolve, businesses are focusing more attention on the protection of applications and APIs. In this section, IDC identifies requirements for a successful application and API security practice.

Consistent Protection, Visibility, and Control

A modern approach to application security must provide consistent and complete visibility, protection, and control across the many varied environments and technologies used to create and deploy applications. This will require support for multicloud and hybrid environments, including deployment models and technologies. However, truly comprehensive visibility and control will require a common, integrated platform with centralized reporting to ensure consistency in policies, definitions, and enforcement.

Note that the support for traditional models is likely to continue to be a requirement for many years. Enterprise networks tend to be heterogeneous, including a variety of product form factors, brands, legacy systems, acquired systems, and uninterruptible applications performing critical business functions. The criticality and sensitivity of certain business applications ensure that some organizations must continue to protect applications that reside on mainframes and other legacy systems. Modern WAF solutions not only must support new platforms but also should offer deployment options that provide a path for adoption at the unique pace that best suits an individual organization.

Flexible Integration for Comprehensive Protection

As threats and technologies change, security platforms must integrate a broader set of capabilities. Researchers have identified an increase in targeted attack campaigns, directing an array of attacks at their victims, including DDoS attacks, bots, and zero-day exploits. Security solutions that integrate an array of security technologies into a common platform will allow businesses to build the protection profile that they need to align with their specific and unique set of threats.

Given the breadth and variance of threats, comprehensive protection will require consolidation of multiple security technologies into an integrated platform. Consolidation is a necessary function to make security manageable given that IT organizations are already inundated with point products, consoles, and alerts. Ideally, platforms will be modular, preventing vendor lock-in and enabling SecOps teams to adapt to new threats, emerging technologies, and changing business trends.

Aligned with Applications, Now and in the Future

For efficacy and efficiency purposes, application security should be in line with application and API traffic. A modern WAF solution must be designed with API protection in mind, and as a priority, rather than an afterthought. APIs must be defended against many of the same threats that target application front ends but also require the ability to parse API traffic such as JSON and XML formats.

IDC notes that the application delivery controller (ADC) has proven to be an ideal platform for delivering application and API protections. ADCs are already in line with application communications, providing functions such as load balancing, acceleration, server health monitoring, network address translation (NAT), and SSL offload. By combining WAF, API Gateway, bot protection, and ADC, IT organizations can achieve the benefits of application performance and reliability. In addition, the combination is clearly advantageous when factoring in the need to decrypt traffic for security inspection. ADCs already perform SSL offload, typically using specialized hardware or optimized software to speed up the process. Inserting content inspection by ADC at this stage adds scale and minimal latency compared with performing this function separately and requiring either an additional hop or burdensome decryption efforts.

Ultimately, application and API protection solutions should offer flexible deployment options. Every organization is currently on a unique stage of its journey to the cloud, and buyers require options that support their business and security objectives. For example, businesses can emphasize simplicity and ease of use or maximize scalability requirements depending on how containers are deployed.

Designed for Cloud

The cloud offers benefits, such as high performance, scalability, and elasticity, that have spurred rapid adoption. However, increased cloud adoption has forced application architecture and technologies to evolve as well, and security solutions must evolve accordingly. WAF vendors must adapt or build their products to support these characteristics in order to protect and extend customer value. To this end, modern WAFs must support cloud-native technologies such as containers and emerging practices such as CI/CD. For example, service mesh and container deployment models can enable the east-west visibility required to detect advanced threat lateral movement and insider threats.

Modern WAFs must be able to support enterprises that rely on multiple cloud services as well as hybrid environments spanning cloud and on-premises datacenters and private clouds. In particular, enterprise organizations are likely to have hundreds or thousands of applications of varying criticality and risk tolerance deployed across multiple or hybrid cloud environments. First, enterprises cannot afford to have security blind spots regardless of where applications live. Next, SecOps must be able to implement a rule change and ensure that protections are propagated across all cloud environments instantly. This can be achieved only by a solution offering "single pane of glass management" compared with the laborious and error-prone method of attempting to monitor threats and manage policy across multiple dashboards, each with differing capabilities and unique interfaces to learn.

In addition, a WAF solution that is designed to operate with multiple cloud environments and hybrid deployments offers the benefit of portability with operational consistency. Portability enables WAF protections to follow applications across all computing platforms, which enables businesses to adapt to new trends, such as service reliability, pricing changes, and performance.

Analytics and Automation

Threats are becoming more numerous, elusive, and sophisticated, while the attack surface becomes broader and more complex. Static WAF rules are no longer sufficient against modern threats, and behavior learning capabilities are necessary to protect against zero-day attacks that bypass static defenses. A modern WAF solution must leverage advanced security analytics to detect threats throughout every possible stage of the attack chain. Machine learning is a critical new technology that is required to properly collect and assess the myriad signals, data points, and threat telemetry before distilling them into an actionable set of alerts. For example, analytics may be required to detect bots that bypass common detection methods such as IP reputation and JavaScript challenges. By using telemetry from device sensors, an analytics-based approach can identify devices that are operating without human user interaction, thus indicating bot-related activity.

Analytics is a necessary security capability in some cases where direct inspection may not be possible. For example, it may not always be possible to inspect encrypted traffic, and advanced security analytics may prove useful to identify threats hiding in encrypted traffic. In addition to improved security efficacy, analytics can help security teams work smarter instead of harder — dynamic profiling provides a means to learn a baseline of acceptable, normal application behavior and then block behaviors that appear malicious with automated rule creation.

Ultimately, a modern approach to application security must extend protection, consistently, to wherever an application resides and across the many technologies that applications now use. But the ability to detect and block emerging threats will require defenses that are no longer static: Modern application security must be dynamic and automated, providing the advanced security analytics necessary to detect zero-day attacks and threats that scour for vulnerable APIs, employ encryption to hide, or use automation for scale.

Considering Citrix

The drastic and rapid advancement of cloud and application technologies and development practices has forced security tools to adapt as well. Security companies are rushing to adapt their products to the demands of the new technologies and emerging threats facing modern applications and APIs. IDC has identified the Citrix solution as meeting the needs for modernized security.

The Citrix Platform Approach Provides Comprehensive, Flexible Protection

The Citrix approach to application security is focused on its ADC with integrated security, which performs numerous application performance, security, and management functions including load balancing, acceleration, server health monitoring, WAF, API Gateway, and bot protection. Citrix ADC is already in the path of application traffic, improving performance and ensuring reliability, and thus is a natural integration point for security. For example, Citrix ADC performs SSL offload, allowing SecOps teams to inspect application traffic in one pass instead of performing decryption multiple times. Visibility into SSL/TLS-encrypted traffic can also be extended to adjacent security technologies such as intrusion detection systems/intrusion prevention systems (IDS/IPS) and next-generation firewalls (NGFWs).

The Citrix application security portfolio is expansive, delivered as a single, comprehensive security platform. Citrix ADC combines traditional WAF protections with anti-DDoS, firewall, antibot, SSL inspection, API security, and authentication to enable comprehensive protection. As an optional component in Citrix ADC, the offering is integrated but allows flexibility in adoption. Businesses do not need to invest in the full suite of functionality but can address immediate security concerns and then adapt as threats evolve. Deployment flexibility enables businesses to address security requirements while assuaging business concerns about cost.

Citrix Supports Heterogeneous Environments, Including Cloud

Citrix offers multiple deployment options to support cloud and virtualized environments, including virtual appliances (VPX), VPX for AWS, VPX for Azure, VPX for GCP, bare metal (BLX), and containers (CPX). A Citrix ingress controller (CIC) enables flexibility in Kubernetes container deployment and management. For example, a unified ingress deployment for Kubernetes clusters allows for simple inbound protection and multitenancy, while a two-tier ingress model allows networking teams to deploy and manage ADC and WAF functions and developers to write their own container security policies separately. Citrix also supports service mesh and Istio deployments, allowing networks to use a sidecar pattern to define policies for both inbound and inter-container traffic.

Importantly, Citrix offers hardware appliances for datacenters and private clouds. High-performance hardware appliances support application repatriation and applications that cannot move to the cloud for privacy or regulatory concerns.

The Citrix platform is designed for consistency across these multiple deployment options, with a single console to manage policy, view alerts, and generate reports. This approach provides portability and consistency of protection across heterogeneous environments featuring multiple cloud platforms, private cloud, and traditional datacenters.

Citrix Designs for Modern Applications, Including APIs

APIs are rapidly gaining recognition as important threat vectors. The ability to support APIs is key to gaining east-west security visibility, supporting microservices architecture, and enabling CI/CD practices. Citrix offers API security as part of its ADC or as an API Gateway. The solution enables API security through a combination of authentication/authorization, encryption, analytics, and rate limiting. Citrix API security enables businesses to extend WAF protections to vulnerable APIs, including bot management technologies and machine learning capabilities to identify abuse or anomalies in API communications.

The Citrix API Gateway offers additional options and can be deployed as a container, a virtual instance, or an appliance. The API Gateway delivers key integrations with OpenAPI Specification (OAS)/Swagger and other DevOps tools. The Citrix API Gateway can also be deployed in the Kubernetes environment both as a north-south gateway and in a service mesh deployment.

Citrix Analytics Defends Against Advanced Threats

Citrix WAF leverages numerous techniques to defend against threats, including IP reputation, signatures, rate limiting, and behavior learning. In addition, Citrix leverages machine learning capabilities in its Citrix Analytics System (CAS) platform to defend against data loss or data theft and advanced and elusive security threats. Citrix advanced analytics is required to detect more sophisticated threats, such as encrypted threats, or bots that can evade JavaScript challenges. For example, Citrix can identify and block bots engaging in credential stuffing attacks by monitoring dwell time and authentication attempts. The example is oversimplified: Citrix uses numerous factors including user agent, screen resolution, browser attributes, and other behaviors to identify bots.

Similar types of behavior analytics are useful to identify and block application layer DDoS attacks, including identifying and blocking anomalous and DDoS activity directed at APIs. For example, CAS supports application performance, which can help defend against "low and slow" application layer attacks that are designed to be imperceptible to network layer defenses such as Slowloris.

Challenges

Bot operators are highly motivated to outfit their bots with new evasion tactics. Citrix has developed an array of bot detection capabilities but acknowledges a need to further develop advanced bot detection capabilities as of the time of the writing. For example, adding machine learning to enable user biometrics validation may be required to detect bots that can emulate user web browsing to bypass browser-based detections.

Conclusion

Innovative and cutting-edge applications have proven to be key to digital transformation as businesses vie for digital dominance. As a result, applications, platforms, and development practices are locked in a cycle of rapid technological change. Threats change and adapt as well. A modern web application security platform must adapt to these changes by delivering a consistent, coherent protection posture across all types of computing environments at scale, supported by advanced analytics for the detection of elusive and complex threats.

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

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com