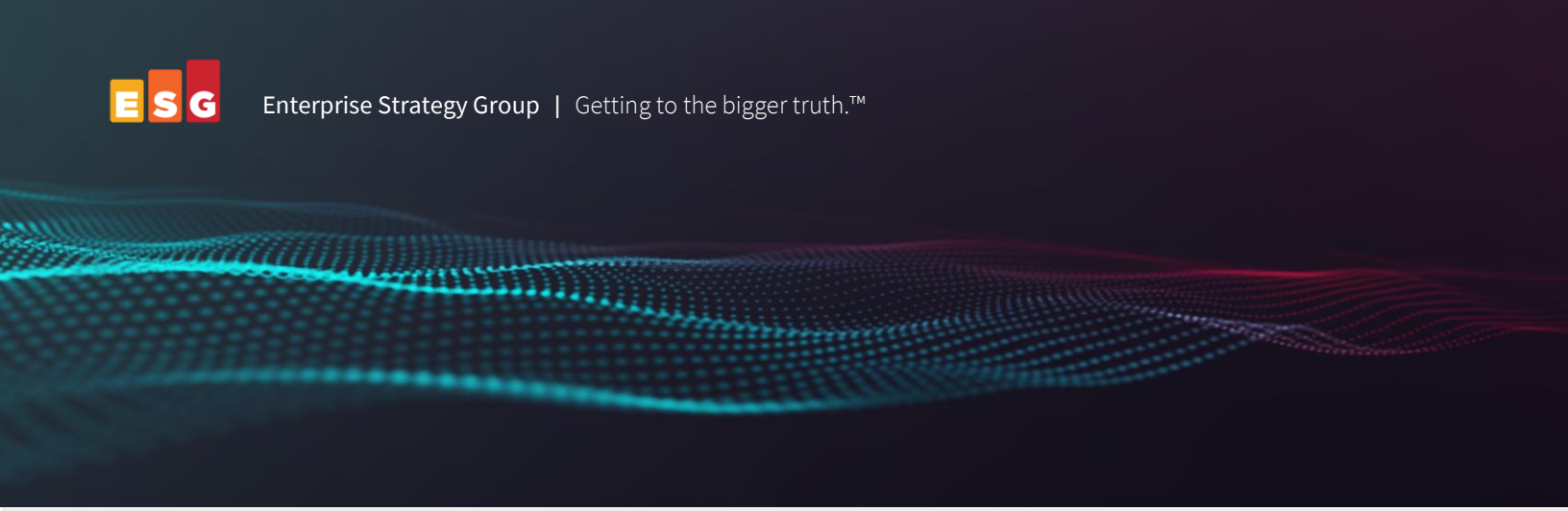


ESG WHITE PAPER

Adopting a Web Application and API Protection Service with Citrix

By John Grady, ESG Senior Analyst

April 2021

This ESG White Paper was commissioned by Citrix and is distributed under license from ESG.

Contents

Executive Summary

The modern application landscape has become fragmented. While applications are more likely than ever to be built on microservices and hosted on public cloud platforms, many legacy applications continue to reside in the data center. At the same time, the threat landscape continues to evolve to utilize multiple avenues of attack, including APIs, automated bots, and availability-based attacks. Traditional, on-premises-based, and siloed tools were not designed for the dynamic, distributed application environment most enterprises support today.

As a result, cloud-delivered web application and API protection platforms, also called WAAP, have emerged. These solutions converge web application firewall, distributed denial of service, bot management, and API protection into a single, cloud-delivered solution. While these tools certainly promise better efficiency, effectiveness cannot be sacrificed in the process. Organizations investigating WAAP should consider solutions providing not only effective security, but also scalable architectures; centralized, intuitive management to promote ease of use; and coverage across all application types and locations. The Citrix Web Application and API Protection service (CWAAP), powered by machine learning, provides this type of cloud-delivered, comprehensive application security, and coupled with Citrix ADC-based application and API security solutions for on-premises and cloud deployments, provides organizations a variety of options for securing applications across their environments.

Organizations investigating WAAP should consider solutions providing not only effective security, but also scalable architectures; centralized, intuitive management to promote ease of use; and coverage across all application types and locations.

The Fragmented Application Landscape Leads to Security Challenges

Businesses today rely on applications to support their employees, engage with customers, and ultimately, drive revenue. As a result, most organizations support tens, if not hundreds, of applications. These may be procured from software providers or developed internally, but many are critical for business operations. Yet while changes to application composition and location have helped drive this increased scale, it also creates challenges from a security perspective.

Applications Span Many Locations and Architectures

The shift to cloud is well documented and yet continues to be overly simplified at times. Organizations deploy applications on public cloud platforms to achieve better scale, agility, and cost optimization. Yet at the same time, many applications continue to reside on-premises. This may be due to architectural considerations, performance concerns, compliance mandates, or simply how the migration of different applications to the cloud is prioritized over time.

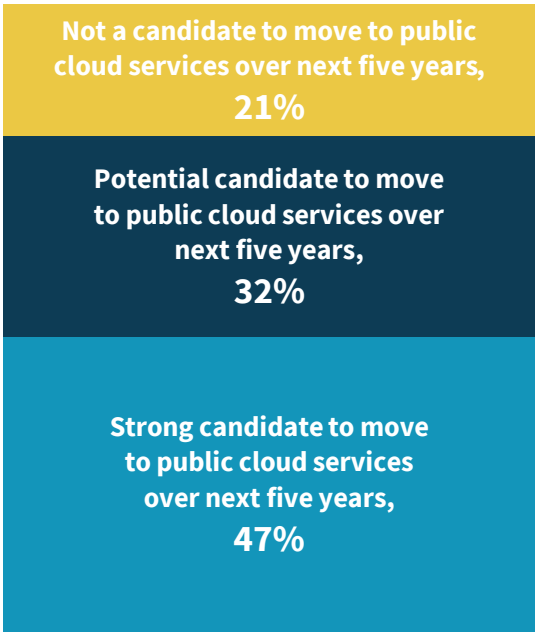
Organizations deploy applications on public cloud platforms to achieve better scale, agility, and cost optimization, yet they may keep applications on-premises due to architectural considerations, performance concerns, compliance mandates, or simply how the migration of different applications to the cloud is prioritized over time.

Whatever the reason, ESG research has found that 21% of current on-premises applications will not be candidates to shift to the public cloud, even in five years' time (see Figure 1). Additionally, nearly one-third (32%) of applications are only

considered *potential* candidates to move to the cloud, further highlighting the fact that on-premises infrastructure will not be fully replaced any time soon.[1]

Figure 1. Likelihood of On-premises Applications to Move to Cloud

Think about all of the applications and workloads that your organization currently runs in your on-premises data centers. What percentage of these workloads are/aren't candidates to move to public cloud services over the next five years? (Percent of respondents, N=664)



Source: Enterprise Strategy Group

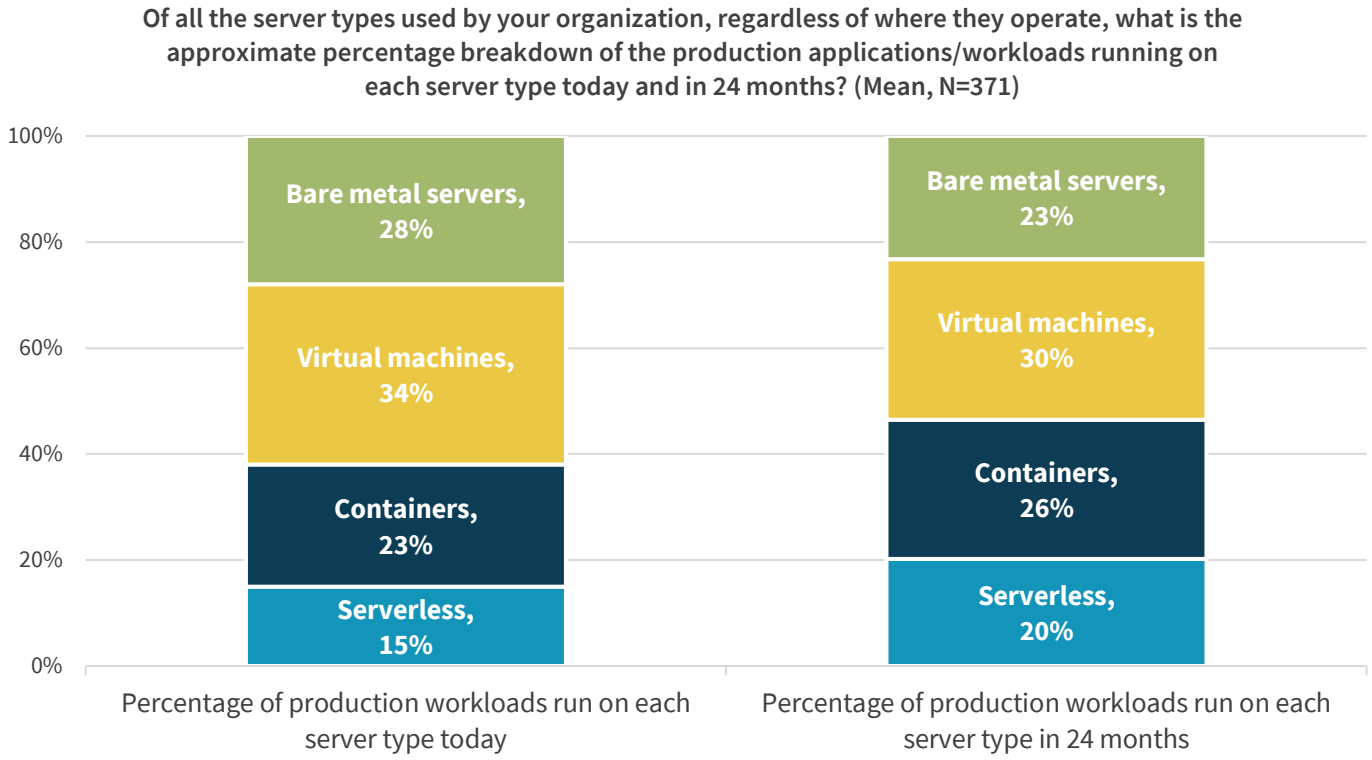
Interconnectivity and Heterogenous Application Composition Is Now the Norm

The adoption of agile application development methodologies such as DevOps, enabled by microservices-based architectures, has been one of the predominant technology trends of the last few years. Relatedly, the use of APIs has increased dramatically not only to connect microservices internally, but also to facilitate information sharing across a variety of third parties through application ecosystems. The result is that, rather than a contained set of siloed applications, organizations now must manage and secure an ever-expanding matrix of interconnected services.

These modern architectures offer numerous advantages over traditional approaches, including speed of deployment, agility, scale, and flexibility. However, organizations cannot rearchitect the entirety of their application portfolios overnight. This results in most retaining a mix of application architectures supported by a variety of server workloads. Specifically, ESG research has found that organizations anticipate that, while 46% of their production applications will run on containers or serverless platforms in the next two years, more than half (53%) will continue to run on bare metal servers or virtual machines (see Figure 2).[2]

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.
[2] Source: ESG Research Report, *Leveraging DevSecOps to Secure Cloud-native Applications*, March 2020.

Figure 2. Production Server Workloads are Heterogenous



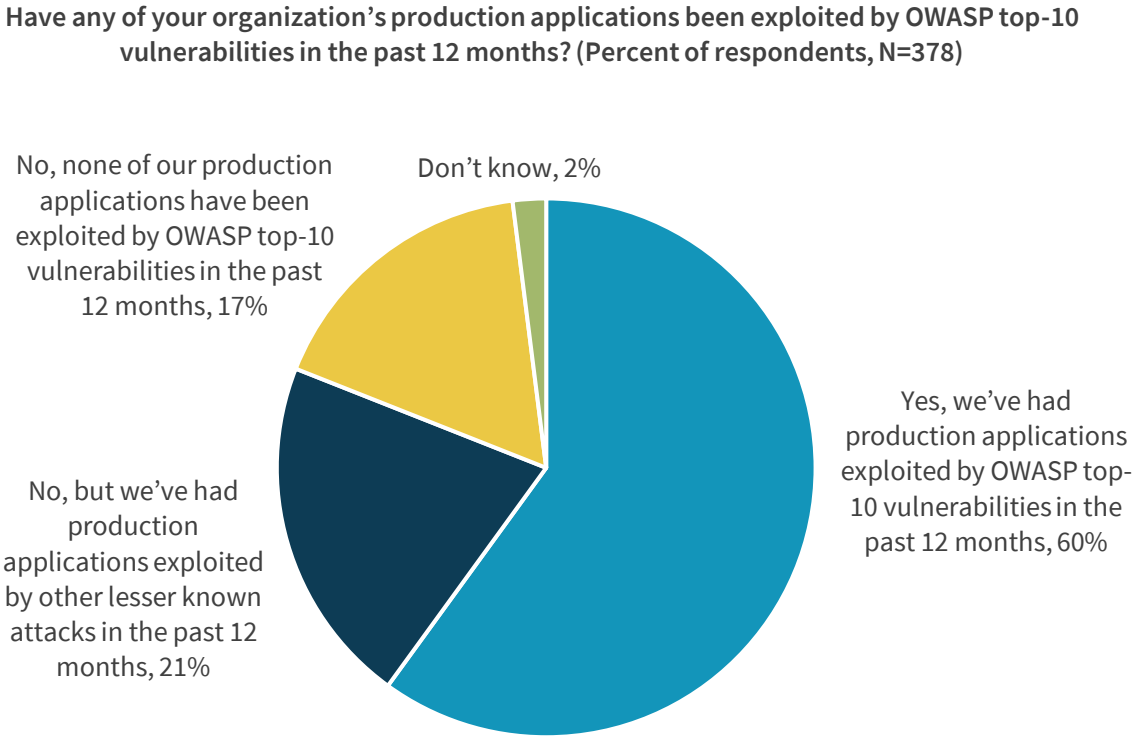
Source: Enterprise Strategy Group

The Security Impact

Cloud migration and evolution of application architectures, coupled with the external threat landscape, have created new challenges with which security teams must contend. In addition to the traditional OWASP Top 10 application threats such as injection, cross-site scripting, and misconfigurations, attackers have evolved their tactics to utilize malware and phishing attacks, website scraping, and credential abuse at scale. Specifically, ESG research has found that 60% of organizations have had production applications exploited by OWASP Top-10 vulnerabilities in the past 12 months, while an additional 21% have been exploited by lesser-known attacks in the same period of time (see Figure 3).[3]

[3] Source: ESG Master Survey Results, *Modern Application Development Security*, November 2020.

Figure 3. Most Have Had Production Applications Exploited by OWASP Top-10 Vulnerabilities



Source: Enterprise Strategy Group

Many of these attacks are carried out by bots, which help attackers dramatically increase the scope of their campaigns and impact the availability of application resources. These attacks often target the APIs supporting microservices-based applications, adding an additional threat vector to already overburdened security teams. Often, attacks follow a multi-pronged approach of targeting different aspects of the application stack with different exploits, probing for the weakest point in an organization's defenses.

Maintaining a consistent security posture to defend against the broad range of malicious activity attackers may utilize across the different cloud platforms and application architectures they support is a daunting task for security organizations that are already understaffed and overworked. Further, the increasing complexity of the regulatory environment due to a heightened focus on user privacy and the resulting mandates such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) add additional considerations organizations must address.

Siloed Security Approaches Cannot Meet Modern Application Demands

Security technologies have historically lagged broader IT transitions, and the application space has been no different. Traditional application security strategies have been centered upon an on-premises hardware or virtual appliance-based web application firewall (WAF), with some organizations layering on additional tools for bot management, distributed denial-of-service (DDoS) mitigation, and API protection on a case-by-case basis.

However, when applications are increasingly likely to reside in the cloud and most organizations are potential targets of campaigns across the attack continuum, this approach ceases to be efficient, and in some cases, effective. Some of the specific challenges that organizations face include:

When applications are increasingly likely to reside in the cloud and most organizations are potential targets of campaigns across the attack continuum, a siloed, on-premises-based approach to application security ceases to be efficient, and in some cases, effective.

- Integrating different application security tools. ESG research has found that 26% of organizations cite the difficulty or lack of integration between different tools as a challenge they face with regard to application security tools.[4] An attacker may initially probe a website for hidden fields before deciding to use bots to target the related APIs with a denial-of-service (DoS) attack. When the tools protecting against each type of attack are siloed, security teams can lose the broader visibility into attack campaigns necessary to protect their application environments.

- Integrating security tools with DevOps processes. While the adoption of DevOps has helped spur greater agility and scale with regards to application development, many organizations continue to grapple with the security implications brought on by this transition. According to ESG research, 19% of organizations cite difficulty integrating security solutions with their DevOps processes as their top application security challenge.[5] Application security is a team sport, and the related tools must support a variety of different personas and processes.

- The impact of the application security skills gap. According to ESG research, 33% of cybersecurity professionals identified application security as one of the areas with the most significant shortage of cybersecurity skills in their organization.[6] While organizations may be able to prioritize security support for tier-1 applications, tier-2 and -3 applications may not receive the same level of attention. Tools that are easily deployed and managed can bridge the gap and provide consistent security across the entire environment.

Key Requirements for Web Application and API Protection Solutions

Recently, a new class of application security tools has emerged that converge WAF, bot management, DDoS, and API protection into a single solution. Commonly referred to as web application and API protection (WAAP), these solutions represent a modernization of application security through a cloud-delivered approach to consistently protect applications wherever they reside. However, convergence alone only solves some of the application security challenges organizations currently face. When considering WAAP solutions, users should look for offerings that provide effective security, a scalable architecture, and ease of use.

Effective, Multi-vector Protection

Many WAFs have offered some level of bot protection and layer 7 denial-of-service prevention for years. Yet these capabilities have remained rudimentary in some cases, unable to protect against attacks from sophisticated bots or layer 4, volumetric DDoS attacks scaling into the terabit per second range. Organizations cannot sacrifice efficacy for consolidation and should continue to demand best-of-breed capabilities as part of a platform approach. In the context of WAAP, this includes:

[4] Source: ESG Master Survey Results, *Modern Application Development Security*, November 2020.
[5] Source: ESG Master Survey Results, *Application and Email Security Trends*, September 2019.
[6] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals 2020*, July 2020.

- Strong signature-based rulesets to prevent OWASP Top-10 exploits and meet compliance mandates.
- Behavioral analysis to detect never-before-seen attacks and support a positive security model.
- Multiple prevention measures to block bots attempting to scrape sensitive information, launch credential abuse attacks, or maliciously consume application resources.
- Mitigation of volumetric DDoS attacks of all types, including ping, flood, application, malformed packets, and others.
- Protection of API endpoints from denial-of-service, malware, authentication, and logic attacks.

Ease of Use

To alleviate the cybersecurity skills shortage and better address the decentralized nature of application security, these solutions must be easy to use. Cloud-delivered solutions remove the need to provision appliances and better match the speed of deployment to which application teams are accustomed.

Centralized and intuitive management and reporting helps to streamline investigation and response, as well as simplify compliance reporting. These solutions should work within DevOps frameworks through integrations with tools such as Chef, Ansible, Puppet, and others to ensure the proper protections are enabled as applications are pushed to production.

Ease of use also encompasses simplified billing and consumption models. Organizations require the flexibility of paying only for what they use through an operational expense (OpEx) model, while at the same time maintaining a level of cost certainty to avoid bill shock.

A Flexible, Scalable Architecture

Finally, to address the modern application landscape, a cloud-delivered web application and API security model is preferred to provide consistent protection for applications of all types across all locations. This requires a global footprint of points of presence (PoPs) to ensure consistent availability and performance wherever the application resides. A cloud-delivered architecture enables security capabilities to scale seamlessly with the application as performance needs dictate and provides a consistent and up-to-date security posture for applications across all locations, whether on-premises or in the cloud. This is especially important from a DDoS perspective in order to mitigate the large-scale volumetric attacks that have become increasingly common.

To address the modern application landscape, a cloud-delivered web application and API security model is preferred to provide consistent protection for applications of all types across all locations.

The Citrix Approach to WAAP

Citrix is well known for its application delivery controller solutions and associated web application firewall capabilities. In 2020, the company introduced the Citrix Web Application and API Protection service (CWAAP). The cloud-delivered service boasts 14 globally distributed PoPs with 12Tbps of scrubbing capacity to deliver consistent security controls across all public cloud and private data center environments and is deployed as a proxy service via DNS or BGP redirection. The solution is billed via a transparent, subscription-based pricing model.

The service combines traditional WAF capabilities to protect against the OWASP Top 10, as well as artificial intelligence (AI) and machine learning (ML) based capabilities to prevent zero-day attacks through a positive security model. CWAAP

mitigates stealthy layer 7 and volumetric DDoS attacks. Bot management uses a variety of detection mechanisms, including signature files and profiles, transaction per second analysis, malicious IP blocking and reputational analysis, device fingerprinting, and bot traps. From an API security perspective, CWAAP protects against JSON and XML-based attacks to protect API endpoints from misuse and abuse.

CWAAP offers a user-friendly, GUI-based dashboard to simplify configuration across multiple environments. The centralized management interface allows corporate security policies to be efficiently distributed across all applications, even through decentralized teams. This single-pane-of-glass console provides visibility over all applications and helps maintain regulatory compliance by ensuring that corporate policies are met and that the correct application security protections are enabled across all environments. Additionally, Citrix offers application and API security solutions for on-premises and cloud deployments through its Citrix ADC solution.

The Bigger Truth

The security space has seen a notable shift towards consolidation and platform-based approaches over the past few years. Secure access service edge (SASE) and extended detection and response (XDR) are two of the most notable examples. Yet, arguably, nowhere is this shift needed more than in application security. The combination of siloed security tools, distributed application locations and architectures, and lack of security skills is a recipe for disaster when attackers understand both the criticality of applications to business operations and the sensitive data to which those applications have access.

With that in mind, the time is right for a new approach to application security in order to improve efficiency and effectiveness. WAAP seeks to provide those benefits, and Citrix's Web Application and API Protection Service delivers the broad range of application security capabilities and attributes required in a WAAP solution.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188