IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Radware

Digital transformation is changing the control points that are available to security practitioners. Applications are emerging as critical control points to understand and manage risk.

Understanding the Next Security Control Points: Applications and Workloads

September 2021

Written by: Christopher Rodriguez, Research Director

AT A GLANCE

KEY STATS

According to IDC, the hybrid cloud workload security market is forecast to grow at a rate of 19% by 2025.

KEY TAKEAWAYS

In IDC surveys, "lack of sufficient tools" was considered the predominant reason for breaches in cloud environments. Applications are emerging as critical security control points that provide unique contextual information about behavior, intent, and authenticity.

Introduction

Digital transformation is unlocking exciting new strategies such as extensive customer insights, tailored messaging, and precision targeting. This transformation will look different for every organization in some aspects but generally starts with the use of powerful, scalable, and flexible cloud computing environments. Unfortunately, with new computing environments come a whole new slew of vulnerabilities and risk concerns.

As a result, the security industry is at a critical juncture as new technologies and frameworks rush to fill the defensive gaps introduced by digital transformation. These approaches vary from extending traditional security technologies to the cloud to developing more specialized security tools for unique use cases. However, transformation is rarely so straightforward. While new and existing security technologies play vital roles in the next-generation security architecture, IDC finds that the transformation era offers a strategic opportunity to realign security tools and practices for superior security outcomes.

Digital transformation is changing the control points that are available to security practitioners to enforce policy and mitigate risk. While technologies such as firewalls and virtual private networks (VPNs) continue to play a foundational role, security professionals require broader visibility, deeper context, and fine-grained controls. As part of this evolution, the application is emerging as a critical control point to understand and manage risk. This IDC Technology Spotlight provides an insight into the advantages of a converged application and workload security strategy as well as best practices.

Benefits of Aligning Security Strategy with the Application Control Point

Applications are emerging as a critical control point that offers unique visibility into user behavior, device telemetry, data sensitivity, and underlying infrastructure to determine and mitigate risk. The strategy to align and coordinate security controls around the application and workload, in a seamless, frictionless manner, offers key benefits for the transformant IT organization.

Applications Provide Fine-Grained Security Control

The network is the original security control point, and network telemetry is widely considered a reliable source of truth. However, security tools that lack visibility into the application layer are oblivious to many types of incidents, including ransomware, phishing, bots, and Layer 7 distributed denial-of-service (DDoS) attacks. Thus, the trend has been to add more application layer visibility into network security tools. For example, legacy firewalls based on IP addresses, ports, and protocols reigned for decades before giving way to next-generation firewalls with application layer visibility, control, and threat detection. The next generation of security solutions, such as zero trust network access, allows organizations to implement and monitor application-specific controls.

The goal of security tools is more application layer visibility, but this objective is sometimes hampered by the privacy or performance requirements associated with proxies or inspection of encrypted traffic. The adoption of cloud computing has helped alleviate these performance concerns. Cloud adoption has also encouraged more integrations as well as new technologies such as containerization and serverless. DevOps teams design applications as modular compilations of microservices and APIs that enable speed, agility, scalability, and portability in order to take full advantage of the cloud. As a result, applications are more interconnected than ever and in ways that are challenging to map or visualize.

Now there is both the need and the opportunity to implement finer-grained controls, including a shift to focus protection around applications. Web application firewalls (WAFs) are designed to meet the specific security needs of applications exposed to the rigors of demanding web users and online threats. As a result, the WAF market is also evolving and is now referred to as web application and API protection (WAAP). These solutions allow security controls to be implemented at the inter-application level or even the API level for greater security control.

Cloud Infrastructure Is Another Threat Surface of the Application

The booming popularity of cloud computing means that many applications are hosted remotely in public or hybrid clouds, outside of the organization's direct realm of influence. This trend, combined with the shift to work from home (WFH) and work from anywhere (WFA), is driving an urgent search for new security control points. Under the shared responsibility model, cloud providers are responsible for security *of the cloud,* while customers are responsible for security *in the cloud*. For example, AWS is responsible for securing the datacenters, physical systems, and virtualization platform, leaving customers to secure the virtual machines, virtual networks, applications, data, and workloads.

For applications deployed in a datacenter, the security architecture can be expansive, including firewalls, intrusion prevention systems, VPNs, and WAFs. Layers of security software would be used to ensure that software is free from vulnerabilities and patched as well as to protect servers and endpoints against malware and other threats.

The importance of securing cloud infrastructure is the same whether workloads are in the cloud or on premises. However, cloud computing inherently limits visibility and control. Instead of the myriad security controls in place in a datacenter, identity and permissions are the only controls available to IT organizations. Overall, cloud infrastructure protection involves several areas of security, including locking down identity context to prevent unauthorized access, eliminating cloud security misconfigurations, and fortifying the cloud's overall security posture.

Trends in Application and Cloud Workload Security

The security industry is changing rapidly to cope with the complexities introduced by new technologies. Complexity challenges traditional network security tools and introduces new security gaps for clever cybercriminals to exploit.

The Rise of Multicloud Complexity

Cloud providers now offer essential security capabilities to help lower barriers to adoption. However, these cloud-provided security tools vary widely in terms of capabilities and controls, and disparities in policies or protections are emerging. The challenge is exacerbated as IT organizations expand to more and new cloud environments. Hybrid cloud and multicloud have become the rule rather than the exception. DevOps teams work in the environment that best supports their projects and speed to market. As a result, organizations are required to protect multiple cloud platforms.

However, complexity is the enemy of security — every cloud has its own capabilities, APIs, management, and reporting. Relying on the native tools of each individual cloud environment can result in "security silos," with each cloud platform having its own security bubble, with disparate security tools, varying levels of protection, and inconsistent reporting. This makes it nearly impossible to detect sophisticated threat actors that understand how to evade a particular security tool.

Furthermore, the use of the cloud has demonstrated the limitations of porting over on-premises tools as virtual appliances. Accordingly, some new "cloud-native" technologies have emerged, including containerization and serverless. These technologies have specialized security requirements and deployment options that account for factors such as the ephemeral nature of containers.

Developments in the Threat Landscape Require Frictionless Security

Threat actors continue to find new means to bypass perimeter-based protections such as hiding malware and phishing attempts in encrypted traffic that force businesses to make a difficult choice between performance and privacy or threat detection. In 2020, the threat landscape grew more severe still — ransomware and supply-chain attacks shut down cities, infrastructure, security companies, and government agencies alike. The success of these attacks highlights the growing need for segmentation, advanced analytics for rapid detection, and automated response.

As of 2021, cybercriminals continue to pioneer novel techniques to steal data, commit fraud, or perform other illicit activities for profit. As these threats emerge, IDC is noting the growing adoption of a few key control points in the next generation of cybersecurity architecture to achieve greater security efficacy. The application is a key control point that offers valuable and unique insight into malicious, suspicious, or unwanted activities. Applications provide insight into user behavior (what action is the user attempting to perform?). This context is vital to determine and control risk because behavior-based detection is a fundamental requirement for detection of elusive or sophisticated attackers. Applications are designed to perform specific and well-defined functions; application-centric security is required to ensure against design mistakes or logic gaps that static security testing tools miss.

In tandem, organizations are increasingly adopting agile software development methods and implementing continuous integration/continuous deployment (CI/CD) models. As the development process becomes faster and more seamless, the downside is that gaps in protection start to emerge. Organizations must integrate security into the application development process — a "shift left" to advance security from the deployment stage to the development stages. Subsequently, security must be as frictionless and automated as possible, ensuring that defenses are up to speed and adapted to any changes in the application, code, or underlying operating environment.

Growing Focus on Holistic Application Protection

Application protection is a well-established practice area, from security testing applications to WAF. However, the nature and composition of applications, as well as the underlying infrastructure, have changed. New technologies have emerged to address complexities and new attacks. Ultimately, application protection in the age of hybrid clouds requires a holistic

approach that combines protection against application vulnerabilities and exploits and security of the underlying cloud infrastructure. This security strategy must be comprehensive, consistent, and pervasive — with security extending to everywhere that cloud workloads, applications, and components are deployed. Comprehensive visibility and control are key to enabling the advanced analytics and automation required to address advanced persistent threats as well as specialized threats such as bots and fraud.

A holistic application protection practice must combine several key requirements:

- **Complete application protection.** WAF, API protection, bot management, and DDoS mitigation are examples of foundational and extended application security use cases. These capabilities offer an additional context of behavior that complements the previously mentioned cloud infrastructure protections. For example, an authenticated user generating excessive HTTP GET responses may indicate an account takeover attack.
- **Protection of cloud infrastructure.** Given that the cloud inherently offers limited controls and visibility, there remains a core set of controls that are essential factors for an effective application/workload security practice. For example, identity context is key to limiting access to known, approved users. Similarly, cloud security posture management (CSPM) solutions can mitigate accidental misconfigurations that criminals are constantly looking to exploit.
- **Cross-cloud coverage.** Cloud workloads and applications require consistent security across multiple environments and threat surfaces as a single solution with uniform protection that is agnostic to the underlying platform.
- **Frictionless, adaptable security.** To support agile development practices and CI/CD processes, application security can no longer be an afterthought. Instead, security must become integrated within the application development process. Seamless integration requires automated algorithms that can identify changes to the application and automatically adapt security policies accordingly.

Importantly, this trend toward holistic application protection aligns with the broader industry trend of a focus on business value. IT buyers are looking for security tools that offer value, which does not strictly translate to price-performance considerations but instead addresses several concerns such as ease of use, time to detection, completeness, and future proofing. Legacy security paradigms that are burdensome, forcing developers to slow down and think about security as a final hurdle in the development process, or an afterthought are quickly becoming outmoded. Enterprises require frictionless security solutions that deliver business value via automation for rapid time to detection and efficient threat mitigation.

Considering Radware

Radware offers a variety of solutions for application delivery and protection across datacenters as well as private and public cloud protection. The Radware security portfolio includes WAF, API protection, bot management, and DDoS mitigation. These products are offered as hardware appliances, software, or software as a service and include Radware ERT services.

Radware Enables Holistic Application and Workload Security

A key benefit of Radware Cloud Application Protection solutions is the integrated approach to Pervasive Application Edge Defense (PAED). PAED is an application-centric approach to cybersecurity that emphasizes the need for holistic, cloud-native security solutions that address the inexorable link between applications and underlying infrastructure. The Radware solution aligns closely with PAED strategy principles by emphasizing the need for comprehensive protection of both the application surface and the underlying cloud infrastructure.

For example, Radware application protection defends applications and APIs against application-level vulnerabilities, while Cloud Native Protector secures underlying cloud infrastructure security concerns of identity, configurations, and malicious access.

Application Protection Solutions for Anywhere Deployment and Key Use Cases

Cybercriminals do not care where applications are deployed. For many attackers, the cloud represents a new frontier to explore for security gaps. While cloud providers are diligent about securing the cloud infrastructure, the rush to the cloud has left many gaps open for attackers to find, given enough time and opportunity. Similar to their on-premises counterparts, applications deployed in the cloud continue to face familiar threats such as SQL injection, DDoS, and zero-day vulnerabilities. These applications are also exposed to emerging threats such as bots or API abuse.

To protect these applications, Radware offers multiple security tools, spanning all deployment models to provide essential security and advanced capabilities across all environments, such as:

- **Web Application Firewall (WAF).** WAF protection based on a positive security model, with multiple deployment options, including cloud/SaaS, physical/virtual appliance, or directly within Kubernetes pods for containerized applications
- **API Protection.** Ability to enforce authentication and defend against API misuse, abuse, and exploits
- **Bot Manager.** Detection of sophisticated bots; fine-grained control of bot ecosystem
- **DDoS Protection.** Protection for applications and infrastructure against volumetric, stateful, and application layer attacks

The positive security model uses behavioral algorithms to automatically establish baselines of legitimate user behavior and automatically tailor security policies accordingly. Through this model, Radware Application Protection solutions provide greater security efficacy against unknown and zero-day attacks, streamline operations, and reduce overhead required for configuring and adapting security policies to dynamic application changes.

Cloud Infrastructure Protection Options

The delineation of security responsibilities between provider and customer is well established, though occasional confusion or oversights continue to occur. Radware addresses key cloud infrastructure protection requirements such as identity management, data security, and application protection. Radware Cloud Native Protector capabilities include:

- **Cloud Security Posture Management (CSPM).** Radware CSPM defends against misconfigurations in cloud platforms, applications, and workloads.
- **Cloud Infrastructure Entitlement Management (CIEM).** CIEM manages permissions and authentication issues to ensure least privilege access so that applications are exposed only to the limited set of users who require access to perform their job duties.
- **Cloud Threat Detection and Response (CTDR).** CTDR provides rapid time to detection of malicious or suspicious activity as well as automated response options to mitigate threats before extensive data loss or damages occur.

» **Visibility and Control.** Cross-cloud visibility and control are fundamental requirements for protection of applications, workloads, and components deployed and integrated across multiple cloud environments.

Challenges

Radware has a deep understanding of the application with a long history of expertise in application security. However, cloud infrastructure protection is a newer area, and Radware is still in the process of building a reputation for quality and expertise. The obvious side note here is that cloud is largely "new" for the security industry as a whole. Applications and workloads, in the context of the unique demands of the cloud, are emerging spaces that have yet to be completely defined. The single greatest hurdle will be educating the market. To the extent that Radware can evangelize the importance of the PAED strategy, the company can have a tremendous influence on driving superior security and, thus, satisfaction for customers.

Conclusion

In the wake of digital transformation, new environments, and changing technologies, the application is quickly emerging as a key control point for security visibility, enforcement, and decisions. However, a mature application security strategy requires a holistic, cloud-native approach that incorporates the unique security requirements of cloud infrastructure.

In the wake of digital transformation, the application is quickly emerging as a key control point for security visibility, enforcement, and decisions.

About the Analyst

Christopher Rodriguez, *Research Director*

Chris Rodriguez leads IDC's Network Security Products and Strategies program covering technologies designed to secure today's complex enterprise networks. The IDC Network Security Products and Strategies practice covers specific functions including firewall/UTM, IDS/IPS, VPN, DDoS mitigation products, cloud security gateway, messaging security, web security, and web application firewall.

MESSAGE FROM THE SPONSOR

Organizations are no longer migrating to the cloud; they're already there. Application deployment is becoming increasingly diverse, resulting in majority of organizations deploying applications across hybrid environments, with applications deployed across public clouds, private clouds, and physical data centers. This leads to challenging application security environment with constantly emerging new threat vectors, longer threat surfaces, challenges in integration with continuous development processes, and increasing involvement by non-security stakeholders in security considerations of cloud environments.

As a result, organizations must deploy a security architecture which is at once comprehensive, consistent, adaptable, and agnostic, to provide consistent, high-level frictionless security with full visibility across all assets at all times.

Radware provides a full set of defenses which give organizations the visibility they need into their application security and allows them to take back control of their protection, with no interruption to business activities.

Visit us at www.radware.com to learn more.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com