5 Challenges to Keeping Application Environments Secure

Application Protection in the Age of Hybrid Clouds Requires a New Approach to Security

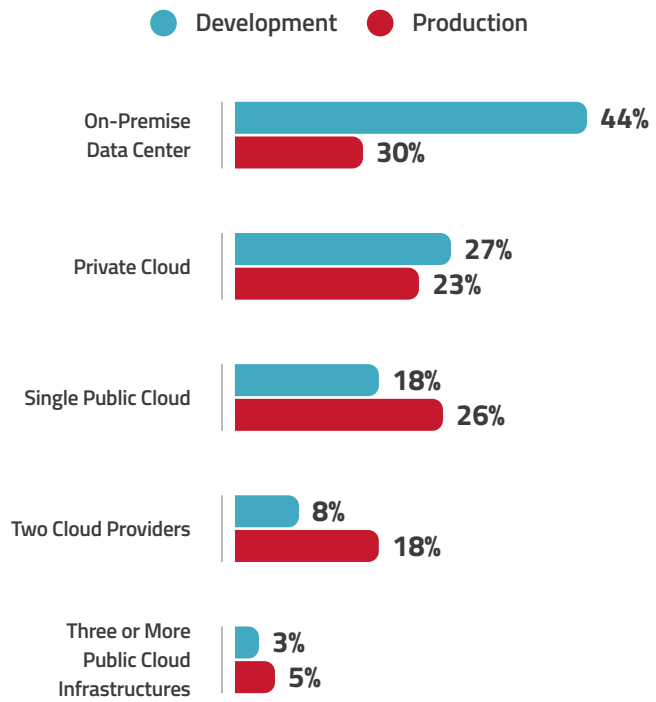
From sophisticated e-commerce engines to cloud-based productivity solutions and personal tools on mobile phones, applications are how things get done. In the information age, applications exchanging, processing and analyzing data are critical to staying ahead of the competition.

The need for application agility has driven an increase in cloud adoption. According to Radware's *The State of Web Application* and *API Protection*[1] report, 70 percent of production web applications now run in cloud environments.

Moreover, it has resulted in application development and deployment becoming increasingly diverse, resulting in the majority of organizations dealing with hybrid, heterogeneous environments that span public clouds, private cloud and on-premise data centers. According to the aforementioned report, the development of applications occurs primarily within a company's on-premise data centers or private clouds (see chart). Seventy-one percent of application development occurs either on-premise or in private clouds, while the remaining balance is mostly housed in single public cloud environments.

When it comes to applications released to production, nearly half of organizations that deploy in applications in public clouds deploy them across multiple environments. The remainder of companies deploy them across private clouds or on-premise data centers.

Where Applications Are Housed for Developments Versus Production



Lastly, the overwhelming majority of organizations do not trust the security offered by their public cloud providers. According to Radware's *C-Suite Perspectives: Accelerated Cloud Migration but Lagging Security* report,[2] 73 percent of organizations "do not completely trust" the security provided by their cloud vendors.

1. The State of Web Application and API Protection report
2. C-Suite Perspectives: Accelerated Cloud Migration but Lagging Security report

radware

The 5 Critical Challenges

Maintaining control, consistency and security of these hybrid environments has never been more challenging. Emerging attack vectors, agile software development/DevOps and multi-cloud deployments have conspired to create an environment where data is left vulnerable and the digital experience is left undermined.

Organizations now face five key challenges for securing hybrid environments.

1 **EMERGING THREAT VECTORS**

Hackers are continuously refining existing and developing new attack vectors that circumvent existing protections. This exposes applications and cloud environments to attacks and data breaches.

2 **BROADER THREAT SURFACE**

In the past, organizations had direct control over the backend infrastructure of the application; only the customer-facing side of the application was exposed externally. In a cloud environment, both the application surface and the application infrastructure are exposed. Both require protection.

3 **AGILE SOFTWARE DEVELOPMENT AND DEVOPS CULTURE**

The primary driver of cloud migration is the need for increased application development agility. The catalyst for this is agile development and DevOps processes that speed the development and enhancement of applications, but often leave security as a secondary priority. Applications might be changing more frequently, but must be kept secure nonetheless.

4 **MULTI-CLOUD DEPLOYMENTS**

Per the aforementioned statistics, companies now deploy applications across on-premise, hybrid and public clouds. This broadens the threat surface, convolutes the implementation of coherent security policies and further complicates the task of cloud security because organizations are now required to protect multiple cloud platforms, each with its own capabilities, APIs, management and reporting.

5 **OWNERSHIP BY NON-SECURITY STAKEHOLDERS**

Although security staff are commonly tasked with protecting cloud environments, they frequently have no authority over the choice or management of cloud environments. According to *C-Suite Perspectives: Accelerated Cloud Migration but Lagging Security*, in 92 percent of organizations, decisions about cloud platforms are made by stakeholders other than security staff.

Frictionless Security at the Pace of Innovation

Security strategy must start with visibility and control and address application security holistically, consistently, anywhere. However, organizations struggle with gaining control.

According to *The State of Web Application and API Protection* report, 31 percent of respondents anticipate that their organization's most significant application security concerns over the next two years will be maintaining a coherent security policy across heterogeneous environments. Nearly as many respondents believe that their most significant concern will be gaining visibility into the security events impacting their organization.

These statistics underscore one of the key overarching issues of application security: despite the implementation of new security technologies, organizations continue to struggle with maintaining visibility and consistency of security policies across the heterogeneous collection of platforms, infrastructures and technologies. To ensure coherent, comprehensive cybersecurity in an environment that is as diverse as it is evolving, organizations must begin thinking about security differently.

APPLICATION AND CLOUD SECURITY ARE CONVERGING

Why? Because application protection in the age of hybrid clouds requires a holistic approach that combines protection against both application vulnerabilities and exploits, as well as security of the underlying cloud infrastructure.

ORGANIZATIONS REQUIRE FRICTIONLESS SECURITY THAT CAN SUPPORT THE PACE OF INNOVATION ORGANIZATIONS NOW DEMAND

Security needs to be frictionless and automated to ensure defenses are up to speed and automatically adapt to changes to either the application or cloud environment while not becoming a roadblock to innovation and change.

Securing this out-of-control environment requires a security strategy that delivers visibility and control and addresses application and cloud security holistically, consistently and anywhere.

Here are six key security capabilities to keep applications and hybrid environments secure:

1 **ADAPTIVE AND AUTOMATED SECURITY**
leveraging behavioral-based and machine-learning algorithms to proactively manage frequent changes to the application, their underlying environments, new security threats and more.

2 **HOLISTIC, AGNOSTIC APPLICATION PROTECTION**
across all environments — providing 360-degree application protection for both the application surface and the cloud application infrastructure.

3 **FRICTIONLESS**
Integrated as much as possible with the development cycle and does not interfere with business processes. It needs to be adaptive so it can change with the frequent changes to applications and the underlying deployment platform. As application development and deployment processes become more agile, security must be tightly integrated with the application development process. This seamless integration must rely on automated algorithms that can identify changes to the application and automatically adapt security policies.

4 **CONSISTENCY**
Uniform, state-of-the-art security for applications everywhere to enable the same level of holistic protection agnostic to the application infrastructure, whether it be private or public clouds.

5 **A BROAD RANGE OF SOLUTIONS**
that provide multiple deployment options, including cloud services, software and hybrid.

6 **VISIBILITY AND CONTROL**
via security and development dashboards that provide actionable analytics, automation and customized controls.

Learn How Radware Provides Frictionless Security at the Pace of Innovation ▸

Contact Us ▸

radware