IDC ANALYST BRIEF
Sponsored by: Oracle

Cloud-native security toolsets with tightly integrated vulnerability scanning services help tenants avoid known exposures within their server's virtual machines and complete application container images.

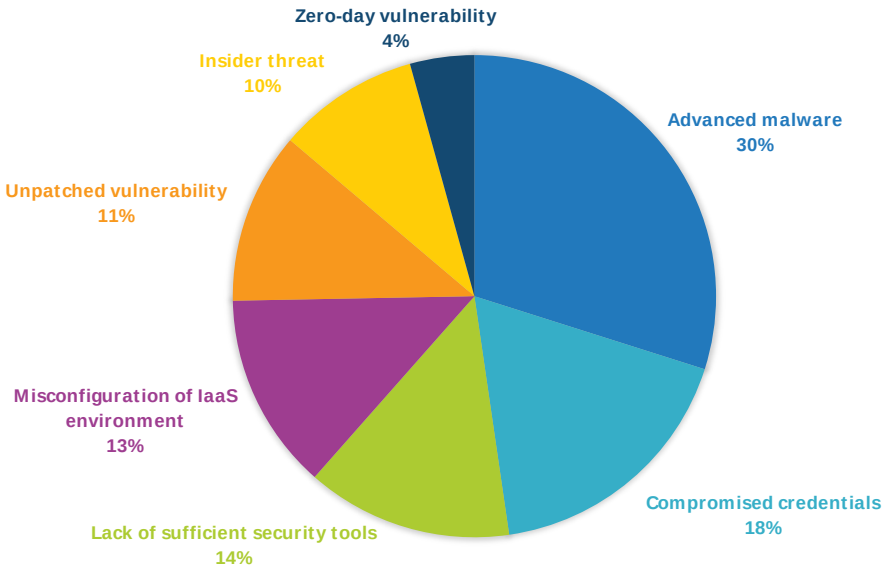
Detecting Vulnerabilities with Cloud-Native Security

July 2021

Written by: Frank Dickson, Program Vice President; Jay Bretzmann, Program Director; Philip Bues, Research Manager

FIGURE 1: ***Breach Factors***

Q ***For the most recent breach of your IaaS environments, what was the predominant factor that resulted in the breach?***



n = 304

Source: IDC's Cloud Security Survey, December 2020

Introduction

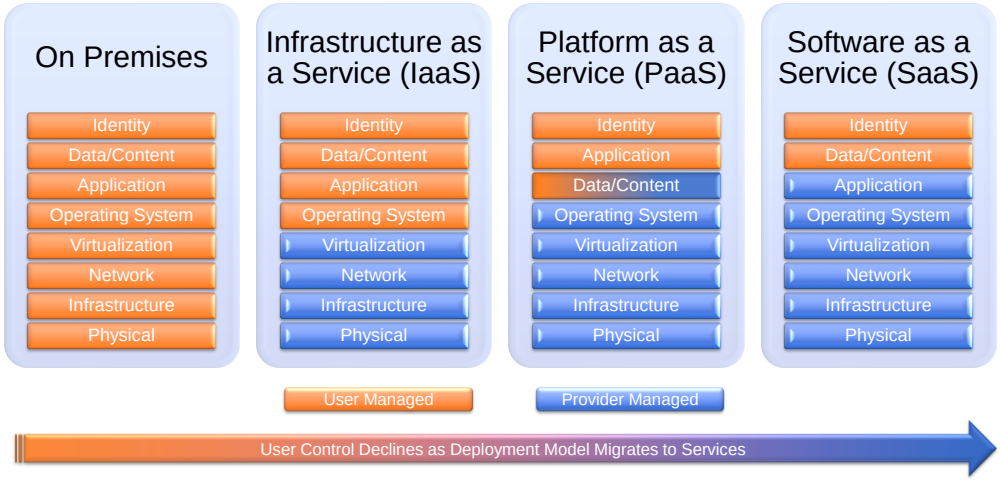
In a recent blog, IDC discussed the topic of cloud-native security as a set of security measures that are an integral part of the cloud offering. As Figure 1 shows, there are sound reasons for having a proactive defense in place. Thus, cloud-native security is a service that the cloud provider offers to application developers, security professionals, and cloud environment owners seeking to realize the benefits of flexibility, choice, and ease of deployment, regardless of where the ownership of security lies in the shared responsibility model (see Figure 2).

The greater cloud security challenges are not found on the provider's side of what's called the shared responsibility model; tenants currently bear an unfair burden.

In any conversation about responsibilities regarding the security of the cloud, as opposed to security in the cloud, it is the cloud provider's responsibility to furnish the security and integrity required to deliver on the cloud's promises of flexibility, choice, and ease of deployment. However, cloud-native integrity cannot stop at the security of the cloud; the greater challenges are not found on the provider's side of the shared responsibility model. Instead, they lie with the consumers of the cloud and addressing what they deploy and run on an infrastructure or as a service.

We've all had a front-row seat to the growing attack surface and the damage wreaked on it by advanced malware threats such as ransomware as a service (RaaS). The fallout includes economic disruptions, information held hostage, exposure of personally identifiable information (PII), and potential compliance liabilities related to GDPR and other regulations. Compliance is particularly relevant for the financial services sector as banks have been disproportionately targeted by cybercriminals. Accelerated by the pandemic, some in-branch services moved to digital platforms and some in-person manual processes shifted to bots, increasing both efficiency and future proofing. However, as digital options increase, security budgets are being cut, which leaves the door open to more exposures. In this new normal, automated cloud-native security services and testing need to be employed and thought of as part of system health.

FIGURE 2: ***IDC's Shared Infrastructure Model***



Source: IDC, June 2020

In fairness, the application owner's side of the shared responsibility model is hard to address. Security professionals can influence the security and integrity of the cloud, but they cannot dictate precise operations. Digital transformation is the conductor that controls business change. Get on the train or get run over by the train; digital transformation does not mind.

Any discussion of cloud-native security (and integrity) must consider how the cloud provider will embed features in its offerings to address some of the conditions presented in Figure 1. For example, in IDC's *Cloud Security Survey* (December 2020), 14% of respondents cited "lack of sufficient security tools" as the reason for IaaS breaches, a factor driving the development and adoption of new cloud-native tools. Security posture also plays a role in controlling and maintaining what customers configure and implement within their compute, networking, and storage instances. The complexities of safely deploying cloud solutions require a posture management solution to help address breaches attributable to a "misconfiguration of IaaS environment," a factor cited by 13% of survey respondents. "Unpatched vulnerability" was also cited as a cause of IaaS breaches by 11% of those surveyed. Addressing these exposures is a complex issue that includes both infrastructure and the application.

IDC recommends "shifting left" beyond configuration and implementation to assist developers and security professionals. Some cloud service providers have developed free vulnerability scanning services (VSSs) based on open source scanning engines that even offer integrations with popular, proprietary tools long used for similar on-premises protections. The services are a safety net against vulnerabilities that may have been inadvertently included as part of newly developed code or that emerged after the application deployment. With a VSS, any detected problems are surfaced and addressed using rules and machine learning to prioritize critical vulnerabilities before they are exploited.

As these services are integrated in cloud instances, they tend to have minimal resource impact. For example, some can leverage a lightweight scanning agent that is embedded into an instance. The embedded scanning engines proactively inspect both host and container images for open source and proprietary code vulnerabilities. To save time on the configuration and upgrade (or maintenance) of these engines and agents, the VSS will automatically handle the details for the customer. Detailed reports and recommended remediation actions will typically be provided per each found vulnerability. The Common Vulnerability Scoring System can be applied to rank the risk of these findings.

A best practice is to scan all container images before they are deployed and then rescan them whenever new CVE information becomes available that applies to a deployed image. Ports, system configuration, and other parameters are also scanned to ensure that nothing is left open. Providers of these services typically strive to offer subsequent reporting that is simple and easy to understand. Depending on the service and once it is configured, results can normally be seen within a day. Some services make results available in an hour. Updated scans can be provided on a daily or a weekly basis, covering attributes such as host vulnerabilities, open ports, and security best practice benchmarks.

Benefits

The primary benefit of a VSS is identifying vulnerabilities before they are exploited. A VSS sits on top of a company's security baseline and patch management process, adding another layer of insulation between the organization and the attacker. A VSS that provides findings to a single pane of glass for a security team to quickly act on is another plus. In some cloud-native solutions, the VSS covers the full gambit of threats and breaches from nation-state attacks to insider threats. Automation is key as internal and external applications are probed and configuration compliance is assessed. However, a VSS also permits manual scanning for targeted operations.

Cloud-native security VSS scanning is application independent. Thus, the service can be used as an independent validation of applications at deployment or applications in runtime.

Additionally, certain cloud-native VSS tools provide a benefit specifically for security or cloud professionals that may not be completely intuitive. Because the VSS is cloud native, scanning is application independent. A security or cloud professional does not need to touch the application or work with application developers to conduct vulnerability scans. Thus, the service can be used as an independent validation of applications at deployment or applications in runtime. Granted, remediation will need to be delegated using the results that are priorities; however, transparency creates communication and trust across all parties.

Considerations

The advantage of cloud-native security is that it is endemic to the cloud, integrating features into the environment and reducing complexity for the user. This benefit gets even better when these tightly integrated features are included by the cloud provider without additional charges. It is also helpful when the cloud provider has a close relationship with the OS vendor, which allows for faster detection and patching of new vulnerabilities. The drawback to cloud-native security measures is that they're often specific to an individual cloud; these tools do not travel from cloud to cloud. Current multicloud strategies diminish their effectiveness.

Conclusion

Cloud-native security is a set of measures innate to the cloud. The integrity created isn't limited to the cloud provider; it also extends to the provider's part of the shared responsibility model. Digital transformation beats the drum to which we all march; reducing complexity and building integrity are shared responsibilities for us all. Thus, embedding security wherever possible is a best practice that everyone should follow.

About the Analysts

Frank Dickson, *Program Vice President*

Frank Dickson is a Program Vice President within IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of security, compliance, risk, privacy, and ethics. Topically, he provides thought leadership and guidance for clients on a wide range of security products, including cloud security, data security, and emerging products designed to protect transforming architectures and business models.

Jay Bretzmann, *Program Director*

Jay Bretzmann is Program Director for IDC Security Products responsible for Identity and Digital Trust and Cloud Security. Jay focuses on identity management, privileged access management, identity governance, B2C identity management, and a multitude of other identity and cloud security topics.

Philip Bues, *Research Manager*

Phil Bues is the Research Manager for IDC Cloud Security. In this role, Phil drives research, provides thought leadership, and advises clients on complex issues including cybersecurity of the cloud and in the cloud. His commentary addresses the benefits and challenges to what's been called the shared responsibility model and how that line may change going forward.

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