Invest Implications: ‘5 Things You Must Absolutely Get Right for Secure IaaS and PaaS’

Published: 16 June 2020    ID: G00469682

Analyst(s): Frank Marsala

To implement a comprehensive cloud security strategy, Gartner recommends that security and risk management leaders responsible for infrastructure security deploy access management, encryption, ZTNA, CSPM and SIEM.

Company Impact

AKAMAI TECHNOLOGIES, INC. (NASDAQ:AKAM); ALPHABET INC. (NGS:GOOG); AMAZON.COM, INC. (NGS:AMZN); AQUA SECURITY SOFTWARE INC.; BITGLASS, INC.; Broadcom Corporation (NGS:BRCM); CISCO SYSTEMS, INC. (NASDAQ:CSCO); CLOUDFLARE, INC. (NYSE:NET); CROWDSTRIKE HOLDINGS, INC. (NASDAQ:CRWD); CYBERARK SOFTWARE LTD (NASDAQ:CYBR); Dell Technologies Inc. (NYSE:DELL); F5 NETWORKS, INC. (NASDAQ:FFIV); FORGEROCK, INC.; FireEye (NGS:FEYE); IBM Corp. (Berlin:IBM); Illumio, Inc.; Imperva, Inc.; MICROSOFT CORPORATION; NETSKOPE, INC.; OKTA, INC. (NASDAQ:OKTA); PALO ALTO NETWORKS, INC. (NYSE: PANW); Ping Identity Corporation (NASDAQ:PING); QUALYS, INC. (NASDAQ:QLYS); RAPID7, INC. (NASDAQ:RPD); SAILPOINT TECHNOLOGIES HOLDINGS, INC. (NYSE:SAIL); SPLUNK INC. (NASDAQ:SPLK); Tufin Technologies; ZSCALER, INC. (NASDAQ:ZS)

Investment Implications

- Using on-premises security architectural patterns in public cloud infrastructure as a service (IaaS)/platform as a service (PaaS) will result in inefficient and ineffective deployments.

- To implement a comprehensive IaaS/PaaS security strategy, Gartner recommends that security and risk management leaders responsible for infrastructure security should:
  - Get identity and access management (IAM) permissions right by using cloud-native controls to maintain least-privilege access to sensitive data.
  - Encrypt all data at rest using customer-controlled keys.
  - Use zero trust network access (ZTNA) and microsegmentation to reduce risk and contain breaches.
Scan continuously for unsecure configurations using cloud security posture management (CSPM) tools.

Capture and analyze all logs using cloud-native threat detection and enterprise security information and event management (SIEM) tools.

IAM: In the public cloud, identity plays a more prominent role by acting as a perimeter for protecting workloads and replacing traditional network edge controls.

Security and risk management leaders should control access to data using cloud-native approaches such as granular role-based access, privileged access management (PAM), privilege trimming and multifactor authentication (MFA).

Gartner also recommends enterprises use access management (AM) and identity governance and administration (IGA) tools to monitor privileges and consolidate user directories.

Encryption: Security and risk management leaders must ensure data stored in the public cloud is protected at rest using strong encryption and an effective key management strategy that enables data encryption with customer-controlled keys.

Key management systems offered by all major cloud service providers (such as Amazon Web Services [AWS] Key Management Service and Azure Key Vault) should be implemented using well-defined policies and standards. Essential features, such as autorotation, strictly defined access policies and service integration are critical for maintaining control of your data.

ZTNA: Microsegmentation and zero trust network access principles should be implemented when configuring cloud infrastructure. Combined with strong IAM and robust encryption, these principles form the foundation of the cloud infrastructure protection hierarchy.

Secure cloud network access is evolving from traditional point-to-point VPN implementations toward the dynamic technologies necessary to meet the demands of modern digital business.

Gartner also advises clients to consolidate network tooling, such as secure web gateway (SWG), cloud access security broker (CASB) and microsegmentation software, to as few vendors as possible. This reduces complexity by simplifying tool integration and minimizing staff training overheads.

CSPM: CSPM tools continuously manage cloud risk through the prevention, detection, response and proactive identification of misconfigured cloud infrastructure. CSPM tools should be used to continuously scan for incorrectly configured cloud resources, such as overly permissive storage access (Amazon Simple Storage Service buckets, Azure Blob Storage or Google Cloud Storage), network access or user permissions.

CSPM tools should not replace existing tools for protecting web applications. Web application firewall (WAF) and web application and API protection (WAAP) technologies should be used to ensure cloud workloads have strictly defined and monitored access to external and internal API endpoints.
Also, alerts should be enriched by inspecting the content of data stores using tools such as Amazon Macie, Azure Information Protection and Google’s integrated Cloud Data Loss Prevention.

SIEM: Cloud platforms provide multiple enhanced logging mechanisms compared with on-premises deployments. Fine-grained IAM logs, enriched network logs and artificial intelligence tools that provide insights into known malicious workload patterns provide new opportunities for threat detection in the public cloud.

Start by enabling logging in every region and for every service, including network flow logs. It is essential that these cloud-specific log sources are collected with enterprise SIEM tools and analyzed to increase visibility and mitigate risks in IaaS/PaaS workloads.

Logging in the cloud has many differences to on-premises deployments and it is important that you make full use of the cloud-native capabilities provided by the cloud service provider. Cloud-native tools, such as AWS GuardDuty and Microsoft Security Center, should be used to monitor for indications of workload compromise. For organizations using multiple cloud providers, third-party cloud workload protection platforms should be used to provide a singular view of all cloud deployments.

Leading cloud providers are offering native SIEM tools to leverage their integration capabilities and expertise in analyzing large-scale datasets. AWS has also shown initial signs of entering this space with the launch of Security Hub; however, due to limited functionality, it is not a recommended alternative at present.

Organizations without adequate SIEM/security orchestration, analytics and reporting capabilities suitable for cloud workloads should use a cloud-native tool, such as Microsoft Azure Sentinel, and plan to migrate from legacy systems. If this doesn’t fulfill your requirements due to multicloud workloads or functionality gaps, then use third-party solutions, such as Splunk, IBM QRadar or Rapid7 Insight.

What to Watch

AM vendors have started to add more “light” IGA capabilities, and IGA vendors are increasingly adding more PAM functionalities to their products. Converged IAM platforms will be the preferred method for IGA, AM and PAM going forward.

Pure-play IGA vendors, such as SailPoint, will have to contend with converged platform competitors such as Okta as it targets the mid-market. At the same time, pure-play PAM vendors, such as CyberArk, will have vendors like SailPoint as competitors for PAM “light” in the mid-market.

MFA is a required feature of an AM deployment. Adaptive access techniques rely on MFA should the risk of the transaction require additional authentication. By 2024, the use of MFA for application access through AM solutions will be leveraged for over 70% of all application access, up from 10% today.
In our “Solution Comparison for Cloud MFA Services,” Cisco and Ping Identity are rated well. RSA is fairly well rated, followed by Okta and Microsoft.

Cloud-based SWGs protect users wherever they are, regardless of whether they are currently working in a company office, traveling or teleworking.

Zscaler and Symantec are in the Leaders quadrant of our “Magic Quadrant for Secure Web Gateways.” Cisco, McAfee and Forcepoint are in the Challengers quadrant.

It is “mostly true” that ZTNAs are the next-generation VPNs. Modern enterprise apps generally have REST APIs, bringing them into the scope of service delivery platform (SDP). However, legacy applications and complex protocols are generally not suitable for SDP tunneling. If an organization’s application protocol mix consists of mainly generic applications with no or few REST-based APIs, then SDP is not the right technology for the organization at this time.

ZTNA vendors: Cisco (Duo Beyond), Perimeter 81 (Software-Defined Perimeter), Pulse Secure (Pulse SDP), Unisys (Stealth), Zscaler (Zscaler Private Access), Akamai (Enterprise Application Access), Cato Networks (Cato Cloud), Cloudflare (Cloudflare Access), Okta (Okta Identity Cloud), Symantec (Luminate Secure Access Cloud)

Where a CASB is used for remote access, additional corporate controls can be enforced by using an AM tool. Also, Gartner strongly encourages all enterprises to pilot and deploy MFA for any kind of remote access. Phone-as-a-token authentication is very suitable here. Interest in CASBs is intense, and customer adoption is rapid — driven by enterprises of all sizes embracing the cloud as the default starting point for new projects and the next step for updates and enhancements to existing applications.

Microsoft, McAfee, Netskope, Symantec and Bitglass appear in the Leaders quadrant of the most recent Magic Quadrant for this space.

The rapid adoption of cloud services, along with an increasing number of cloud infrastructure and platform services, has created an explosion in complexity and unmanaged risk. IaaS providers deliver basic configuration and risk assessment capabilities, but only address their own services. Most enterprises will require hybrid, multicloud capabilities.

Sample CSPM vendors: Bitglass, Check Point Software Technologies, CloudPassage, CipherCloud, DivvyCloud, Fugue, Lacework, McAfee, Netskope, Palo Alto Networks, Sophos, Symantec, Threat Stack, Turbot, VMware.

Gartner predicts that, by 2023, more than 30% of public-facing web applications and APIs will be protected by cloud WAAP services, which combine distributed denial of service protection, bot mitigation, API protection and WAFs.

WAAP vendors: Akamai, Cloudflare, Radware, Imperva.

The competitive dynamics of the SIEM space will be interesting over the next few years. Such dynamics could be impacted by the emergence of extended detection and response products, which are beginning to demonstrate security operations productivity with alert and incident correlation, as well as built-in automation. Also, competitive intensity could be impacted by the maturity of Microsoft Azure Sentinel and AWS Security Hub.
Leading SIEM vendors: Splunk, IBM, Rapid7, Exabeam, Securonix and Dell RSA.

Get the full story
This content is part of a larger body of research on this topic.

5 Things You Must Absolutely Get Right for Secure IaaS and PaaS
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp