Vendor Landscape: Cloud Workload Security Solutions, Q3 2017

New CWS Functionality Offers Better Breach Detection, Granular Control, And More Cloud Integration

by Andras Cser

September 1, 2017

Why Read This Report

As businesses continue to adopt both infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) cloud platforms, S&R pros struggle to protect their organization's valuable data while minimizing the threat surface of cloud and hybrid cloud workloads. Cloud workload security (CWS) solutions provide automated and layered controls to secure configurations, network, applications, and storage of hybrid cloud hypervisors and workloads. This report provides S&R pros with an overview of the CWS vendor landscape, critical selection criteria, and key vendor differentiation.

Key Takeaways

Forget Manual Cloud Workload Security: Automate

Because of the ephemeral nature of cloud workloads and the increased speed for software delivery, manual security configuration no longer works. S&R pros must find centralized, automated, and auditable ways to monitor and secure cloud workloads reliably.

CWS Solutions Now Monitor IaaS APIs And Guest Operating Systems

Most CWS vendors now offer both agentless operation and agent-based operation, with agent-based operation covering IaaS APIs. Adequate and multilayered IaaS workload file integrity monitoring, network security, and application binary protection requires the use of both agentless and agent-based features of the CWS solution.

Vendor Landscape: Cloud Workload Security Solutions, Q3 2017

New CWS Functionality Offers Better Breach Detection, Granular Control, And More Cloud Integration

by Andras Cser
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie

September 1, 2017

Table Of Contents

Related Research Documents

Create Your Cloud Security Technology Strategy And Road Map

Forrester Data: Cloud Security Solutions Forecast, 2016 To 2021 (Global)

Market Overview: Cloud Workload Security Management Solutions — Automate Or Die

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

You Can't Secure Cloud Workloads With Manual Tools, Traditional Tech

Firms have adopted cloud in earnest. According to Forrester Data, 52% of North American enterprise infrastructure decision makers believe that adopting public cloud is either a high or critical future business priority.[1] This widespread cloud adoption poses unique challenges for S&R professionals responsible for securing workloads in IaaS and PaaS environments. In particular, S&R pros tell us that:

- **Manual breach detection will not work.** The recent OneLogin breach highlights the importance of deep visibility into cloud workloads. In this breach, an attacker stole the AWS administrative console credentials of a OneLogin admin and used them to spin up new, nonproduction instances of the OneLogin identity-as-a-service (IDaaS) backend infrastructure and data. Once these rogue instances were up, the attacker stole the user names and email addresses of IDaaS users in OneLogin's client organizations. It took OneLogin 2 to 3 hours to detect the suspicious activity, and by then the breach was well underway. The breach was particularly painful for OneLogin clients because it exposed sensitive information and undermined their security posture.[2]
- **They need centralized visibility and control over a high volume of workloads.** As technology leaders have migrated workloads to the cloud, the number of workloads has also dramatically increased, and S&R pros struggle to maintain adequate, built-in security configurations at scale. Most of the workloads are ephemeral (they appear and disappear) and number in the hundreds, even thousands, so on-premises, legacy patching, and software delivery tools have a hard time keeping up with oversight and management. S&R pros can't run and control this high number of environments unless they have centralized visibility, asset management, and control of all workloads for compliance and security purposes.
- **They must match the speed of DevOps.** Imbuing security into development and operations (DevOps) processes creates unique challenges. S&R pros must meet aggressive deadlines for setting up the security configuration of hundreds of physical and virtual machines and container-based servers. Separating, segmenting, and tagging multiple environments — such as development, quality assurance, staging, and production — hypervisors, and processes for security purposes also requires automation.
- **Confidentiality, availability, and integrity requirements also apply in the cloud.** Firms are still responsible for the confidentiality, availability, and integrity (CIA) of the data they oversee, whether that data lives on-premises or in the cloud. An integral component of ensuring CIA is detecting changes to workload security configurations, network activity, unusual or excessive activity on the IaaS (e.g., AWS and Azure) console, or unauthorized binary processes running in workloads.
- **Cloud compliance is more complex than ever before.** With the advent of such new cloud services as serverless functions, eCommerce applications, IoT, networking, storage, and audit, visibility into the cloud has dramatically decreased in the past 24 months. However, internal and external auditors are relentless: In addition to industry-norm compliance mandates like ISO, HIPAA, PCI, and SOC, auditors press firms to demonstrate audit of software development life cycles,

DevOps, and business continuity and disaster recovery protocols and to provide proof of visibility into workload configuration and network security. S&R pros struggle to get and maintain an acceptable level of visibility into workloads that meets compliance requirements.

- **Multiple clouds magnify network security challenges.** The network architecture that results from interconnecting multiple IaaS, PaaS, and private clouds creates enormous network security challenges. How will traffic be routed from AWS to on-premises to Azure to Rackspace if the firm uses all three cloud platforms to host workloads? Will the company route inbound traffic to a customer-facing website to the IaaS CSP or to on-premises, and then to the cloud? Understanding and managing the security intricacies of multiple interconnected and changing clouds is not easy, and it's not possible without automation. Moreover, the sharing of responsibilities between the cloud provider and the client change from time to time and between cloud providers — compounding challenges.
- **Traditional on-premises tools are expensive and don't scale well.** Using traditional on-premises commercial off-the-shelf (COTS) and homegrown tools to manage cloud security is hard to scale; it's also hard to calculate costs for because of the continuously changing number of running instances in the cloud. Vendors price these traditional tools per CPU, per server, etc. Cloud workloads require more flexible deployment and pricing methods, such as per instance per hour or per data transferred, and other metered pricing options. As an example, consuming CWS as a marketplace solution as a 15% to 20% additional cost on top of AWS or Azure costs makes procurement easy: The company can purchase CWS from the IaaS provider itself as a monthly line item on its bill.

CWS Detects Compromises, Supports Automation And Compliance

CWS solutions can address many of the security team's toughest cloud workload security challenges. They provide automated and layered controls to secure the configurations, network, applications, and storage of hybrid cloud hypervisors and workloads. Unlike traditional on-premises security solutions, vendors developed CWS solutions specifically to handle the scale, speed, and ephemeral nature of cloud workloads. The solutions are cloud-based themselves, so pricing and deployment also mirror cloud workloads.

CWS Solution Architecture And Key Features

CWS solutions' policy management server is usually available as a SaaS offering. Since DevOps, engineering, security teams, operations teams, and cloud architecture professionals all contribute to CWS purchasing decisions, CWS solutions cover quite a broad swath of functionality areas, but S&R pros should be aware of its general architectural blueprint and the following key features (see Figure 1):

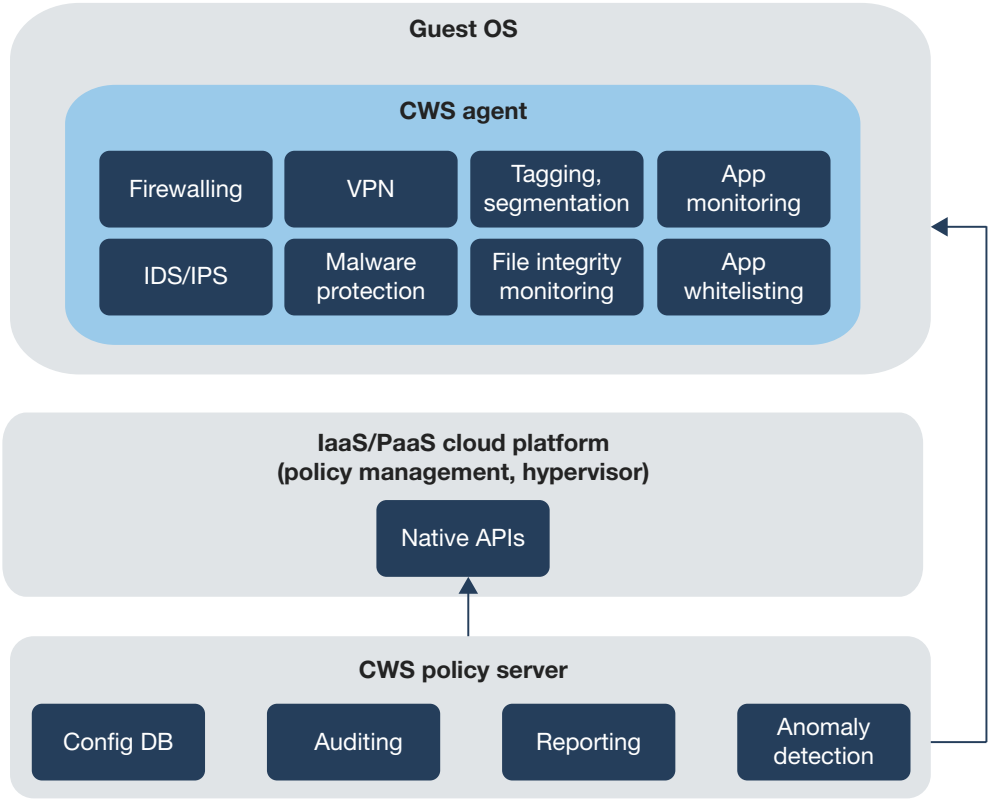
- **Agent-based and/or agentless operation on the infrastructure.** To monitor and control a given workload, a CWS solution either: 1) uses lightweight user or kernel agents in every guest OS it monitors or 2) uses the underlying hypervisor's API to monitor and intercept calls and data flows

between the guest OS and the hypervisor. The benefit of agent-based operation mode is that it can perform a much deeper level of monitoring and interception than the agentless, API-based operation mode. On the other hand, the API-based operation mode does not require constant testing of the agent with new operating systems and kernel versions. API connectivity also provides deeper integration with the IaaS (i.e., AWS and Azure) management console.

- **Tagging and segmenting workloads, hypervisor and container support.** To support large-scale cloud deployments, S&R pros need to know which workload belongs to which environment (development, quality assurance, staging, or production); tagging and segmentation help solve this problem. In private and hybrid cloud environments, CWS solutions should be able to monitor the hypervisor (VMware, Zen, etc.), specifically in how network traffic and disk data flows between the guest OS and the hypervisor, and ultimately the underlying hardware. Container (Docker, Kubernetes, Mesosphere, etc.) support in CWS solutions has to look at and understand data transfer through the container infrastructure, common shared object libraries, and network interfaces of the operating system.
- **File integrity monitoring for change management.** The usual signs of a compromise include changed system configuration files (such as /etc/passwd, /etc/nsswitch.conf, and /etc/hosts on Linux OSS), which in turn profoundly alter the behavior of the guest OS, allowing it to open ports, be accessible to hackers, and serve as a base for botnets. When hackers replace legitimate binary executable files with malicious binary files, it changes the checksum of the binary executable file. Similarly, when a configuration or properties file changes "by itself" on the workload, it's usually a sign of malicious activity.
- **Malware protection, IDS/IPS, firewalling and machine learning for threat detection.** Understanding malware file signatures and scanning the guest OS files to find those signatures is one aspect of malware detection on server workloads. CWS solutions also often provide network security features such as intrusion detection and prevention (IDS/IPS), host-based firewalling, and between workload VPN capabilities on endpoints. Unsupervised and supervised machine learning capabilities help S&R pros create normal activity baselines and then identify any deviance from those baselines.
- **Application binary privilege control, executable whitelisting for privilege managem.** This new feature set made its way into CWS solutions since our last vendor landscape in 2015. CWS solutions can now understand the permissions and normal baseline activity of a binary, such as what kind of privileges a print spooler binary and process needs and uses to perform its job, and can detect any deviations from this baseline. Whitelisting allows system admins to maintain a list of allowable binary fingerprints that can run on the workload.
- **Native API based integration with IaaS consoles and recipe-based solutions.** In order to automate security, S&R pros must bake CWS functionality (agent install and configuration) into the creation and configuration of a workload. To allow for this, the CWS solution should provide integration with recipe-based configuration solutions like Chef, Puppet, and SaltStack to install and

configure its agent. To allow for API-based monitoring and control of IaaS and PaaS workloads, the solution must have: 1) its own APIs for bidirectional integration and 2) productized integration with the AWS and Azure management consoles.

FIGURE 1 CWS Architectural Blueprint



The CWS Solution Vendor Market Is Still Immature And Fragmented

Forrester included 16 vendors that have the largest mindshare with S&R pros and vendors in the CWS market. Forrester found that each vendor offers a unique combination of capabilities of CWS, but no vendor can cover the entire spectrum (see Figure 2 and see Figure 3).

› **Alert Logic provides threat and exposure detection and blocking in a SaaS offering.** Alert Logic offers a security stack, delivered as a service. The solution's capabilities include: 1) assessing workloads/environment for vulnerabilities in software and cloud configurations; 2) detecting active threats to workloads; 3) providing timely escalations to quickly remediate; and 4) blocking application layer threats. The solution requires agents, does not provide file integrity monitoring

(FIM) or any host based firewalls or binary privilege escalation management.[3] Forrester expects that in the future the vendor will: 1) offer integration with additional cloud service providers; 2) improve incident response workflows; and 3) further invest in machine learning for telemetry.

- **Armor offers a single-paned CWS portal with malware protection and file monitoring.** The company has a relatively large user base of 1,200 organizations. The solution provides a single-pane-of-glass view of cloud workloads and comes with 24x7 security operations center support for incident detection and remediation. The agent-based solution covers file integrity monitoring, malware protection, and provides an API for headless integration, but has no VPN or privilege monitoring and escalation management for binaries. The vendor plans to: 1) expand its analytics capabilities to support machine learning in correlating events; 2) support privilege monitoring and escalation; 3) improve incident response and dashboarding/reporting on the portal.
- **AWS integrates its multiple services for CWS functionality.** AWS does not have a single CWS solution; instead, it uses multiple services for CWS functionality.[4] Amazon CloudWatch Logs helps monitor and detect unexpected activity, while Amazon EC2 Systems Manager is a service to collect software inventory, apply patches, and create and configure system images. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. The solution lacks FIM, IDS/IPS, and application binary and privilege escalation management. The vendor plans to: 1) improve Amazon Inspector's assessments; 2) provide Inspector integration with EC2 Systems Manager and CloudWatch events; and 3) improve the AWS web application firewall (WAF).
- **Bitdefender builds its CWS offering on its endpoint protection solution.** Bitdefender GravityZone provides endpoint security for physical, virtual, cloud, and mobile environments running on Windows, Linux, Mac, iOS, and Android systems. For on-premises installations, the vendor delivers as a virtual appliance. The solution provides hypervisor monitoring and process monitoring and requires an agent. It does not provide file integrity monitoring, VPN, AWS, or Azure native integration. The vendor plans to 1) add file integrity monitoring; 2) integrate sandboxing technology; and 3) integrate with Azure Management Console.
- **CloudCheckr checks for cloud workloads for proper configuration.** CloudCheckr provides security configuration and activity monitoring of the IaaS control plane. The vendor starts with running 150 security best practice checks to ensure all appropriate security options and settings are configured properly. The agentless solution does not provide productized support for containers, non-IaaS hypervisor monitoring, malware protection, firewalling, or VPN, but integrates with the AWS and Azure management consoles. The vendor plans to: 1) implement security user behavior analytics (SUBA) and 2) expand mapping of features to compliance mandates.
- **Cloud Conformity provides agentless API-level connectivity to AWS.** The vendor provides a SaaS solution for real-time threat detection, security, compliance, cost management and optimization, and automation. The agentless solution provides an API for connecting to AWS but lacks third-party hypervisor monitoring, malware protection, firewalling, and VPN. The vendor plans to: 1) expand

the solution to the Microsoft Azure and Google Cloud platforms; 2) achieve PCI-DSS and HIPAA certification; and 3) improve machine learning to support a real-time threat monitoring capability that can forecast security risks in advance based on existing user behavior and market trends.

- **CloudPassage offers automated security visibility and compliance monitoring.** CloudPassage Halo provides monitoring and control capabilities for workloads that run in any on-premises, public cloud, or hybrid cloud environment. The agent-based solution has security configuration monitoring; software vulnerability scanning; privileged access management; file integrity monitoring; automated log inspection; log-based intrusion detection; workload traffic discovery; host-based firewall orchestration; and multi-factor network authentication. The solution does not provide Azure console integration, supervised or unsupervised machine learning, or VPN. Forrester expects that the vendor plans to: 1) expand container support; 2) provide IaaS API-based monitoring; and 3) build a new analytics engine based on shared customer data.
- **Dome9 uses IaaS API calls to detect and fix misconfigurations.** The API-based, agentless Dome9 Arc solution is a SaaS-based offering that monitors network assets, assesses their security posture, detects and fixes misconfigurations, models standard policies, protects against attacks and identity theft, and conforms to compliance standards and security best practices in the cloud. The solution provides file integrity monitoring and AWS console integration, but it does not offer productized support for 1) containers, 2) malware protection, 3) app binary privileges and whitelisting, and 4) native productized integration with the AWS console. The vendor plans to: 1) implement compliance and governance for DevOps in its workflows; 2) expand on multicloud strategy; and 3) enhance privileged account management.
- **Evident.io monitors cloud service providers' APIs without agents.** The solution gathers AWS API metadata from each AWS account via the Amazon APIs as often as every 5 minutes (but most commonly every 15 minutes) and feeds this input into the solution's risk analysis engine. The engine then generates a detailed assessment of the security risks, misconfigurations, and vulnerabilities it detects. The agentless solution does not provide file integrity monitoring, malware protection, or IDS/IPS. Forrester expects that the vendor plans to: 1) expand AWS support; 2) support Azure and Google Cloud; and 3) obtain further cloud compliance specifications.
- **Illumio provides the right level of segmentation and tagging of workloads.** Illumio delivers adaptive, granular segmentation that works across data centers and cloud computing environments. The solution can: 1) segment large environments like production and development with a single rule, and/or micro-segment a specific critical, high-value application; 2) define granular policy for control down to the process level; and 3) encrypt traffic between workloads and environments with a single-click policy. The solution does not offer malware protection, IDS/IPS, app binary monitoring and whitelisting, or machine learning. The vendor does not disclose its road map, but Forrester expects user interface improvements and machine learning expansion in baselining activity and workload group memberships.

- **Kaspersky Lab extends malware protection to hybrid cloud workloads.** In addition to its current cybersecurity technologies available for private clouds, the Kaspersky Cloud Security solution provides cloud-assisted AV protection optimized for server workloads, vulnerability assessment and patch management, and application binary monitoring. The solution requires agents, does not provide hypervisor and file integrity monitoring, host-based firewalls, or machine learning. It currently does not integrate with AWS and Azure (however, this is planned). It is not currently certified against PCI DSS and ISO 27001. The vendor plans to introduce: 1) system and file integrity monitoring; 2) firewalling and network segmentation; and 3) exploit prevention.
- **Lacework uses proprietary machine learning to baseline workload activity.** Lacework Polygraph automatically builds and archives a baseline of a comprehensive set of cloud entities and activities. Then it identifies and alerts on deviations from the baseline. The vendor's machine learning techniques aggregate and organize baseline data into behavioral maps, called "polygraphs," that visualize the data from multiple perspectives. The solution lacks generally available file integrity monitoring (it's in beta), VPN between workloads, and PCI DSS and ISO 27001 compliance. The vendor plans to: 1) integrate native IaaS and Windows support; 2) offer the solution on the Azure Marketplace; and 3) expand support for virtual private clouds.
- **RedLock correlates configurations, large user activity, and traffic to detect risks.** The solution enables organizations to manage security and compliance risks across AWS and Google Cloud Platform. It continuously ingests and correlates massive volumes of third-party raw data feeds consisting of configurations, user activities, and network traffic from the cloud environment via APIs to develop its own analytics. The solution enriches the data using machine learning and external data feeds such as threat intelligence and vulnerability scan results to construct a network map that models the resources within the environment. The agentless solution lacks malware protection, IDS/IPS, application control and whitelisting, and PCI DSS and SOC2. Forrester expects that the vendor plans to 1) support Azure; 2) add compliance for NIST, HIPAA, and FedRAMP; and 3) expand enterprise integrations.
- **Symantec offers broad CWS functionality and integrates with AWS and Azure.** Symantec Cloud Workload Protection automates and centralizes security for hybrid cloud workloads to provide a single pane of glass and compliance controls. The solution natively integrates with public cloud APIs to enable discovery, visibility, and elastic protection of AWS and Azure workloads from unknown exploits. The solution provides file integrity monitoring and application binary monitoring and whitelisting. It requires agents and lacks malware protection, SOC2 certification, and machine learning algorithms. The vendor plans to 1) add antimalware; 2) expand container security; and 3) add microsegmentation management visualization and automation.
- **Threat Stack offers smart, behavioral cloud traffic monitoring.** Threat Stack Cloud Security solutions enable customers to monitor and analyze multiple data streams (including Linux host kernel syscall data, Windows events data, file events, network connection logs, AWS service configurations, AWS CloudTrail data, vulnerability notifications, and threat intelligence data) in

real time to inform a rules-based behavioral monitoring and detection model. The solution lacks signature-based malware protection, host-based firewalling, application binary control, and productized support for DevOps tools. Forrester expects that the vendor plans to: 1) increase the scalability of deployments and workflows; 2) improve support for serverless and containerized components; and 3) expand its technology partner ecosystem.

› **Trend Micro covers hybrid cloud, virtualized, and legacy workloads.** Trend Micro Deep Security provides managed SaaS or AWS/Azure marketplace-available automated host-based security for hybrid environments including (physical, virtualized, cloud, and Docker containers) using deep API integration, addressing the security needs of both data center operations and cloud teams. The predominantly agent-based solution lacks VPN, application binary privilege monitoring and privilege escalation, SOC2 certification, and machine learning in behavioral baselining and detection. The vendor plans to: 1) allow for security automation and tool reduction; 2) support serverless and container based architectures; and 3) expand SaaS support for specific regulatory requirements such as SOC2 and HIPAA and data sovereignty requirements such as GDPR.

FIGURE 2 CWS Vendor Capabilities

● Yes ○ No

Solution capabilities	Alert Logic	Armor	AWS	Bitdefender	CloudCheckr	Cloud Conformity	CloudPassage	Dome9
Productized container support	●	○	○	○	○	●	●	○
Agentless functionality	○	○	○	○	●	●	○	○
Hypervisor monitoring	○	○	○	●	○	○	○	○
API connectivity to AWS and Azure	●	●	○	○	○	●	○	●
Workload agents for data collection	●	●	○	○	○	○	●	●
File integrity monitoring configurable for individual files	○	●	○	○	○	○	●	●
Malware protection	●	●	○	●	○	○	○	○
Network-based IDS/IPS	●	●	○	○	○	○	○	○
Host-based firewalling	○	●	●	●	○	○	●	●
VPN between workloads	○	○	○	○	○	○	○	○
Binary control by executable whitelisting	○	○	○	●	○	○	●	○
Policy-based binary privilege escalation	○	○	○	○	○	○	○	○

FIGURE 2 CWS Vendor Capabilities (Cont.)

Productized integration with DevOps tools	●	○	●	○	○	○	●	○
Supports AWS management console APIs	○	○	●	●	●	●	○	○
Supports Azure management console APIs	○	○	○	○	●	○	○	●
Documented API for headless integration	●	●	●	●	●	●	●	●
ISO 27000 native compliance	●	●	●	●	○	○	●	●
PCI native compliance	●	●	●	●	●	○	●	○
SOC2 native compliance	●	●	●	○	●	○	●	●
Unsupervised ML-based risk scoring, exposed to customers	○	○	○	○	○	●	○	○
Supervised ML-based risk scoring, exposed to customers	○	○	○	○	○	●	○	○
Guest OS is independent of the kernel	○	○	●	○	●	●	●	○

FIGURE 2 CWS Vendor Capabilities (Cont.)

● Yes ○ No

Solution capabilities	Evident.io	Illumio	Kaspersky	Lacework	RedLock	Symantec	Threat Stack	Trend Micro
Productized container support	○	●	○	●	○	●	●	●
Agentless functionality	●	○	○	○	●	○	○	○
Hypervisor monitoring	○	○	○	○	○	○	○	○
API connectivity to AWS and Azure	●	○	○	●	●	○	○	○
Workload agents for data collection	○	●	○	●	○	○	○	●
File integrity monitoring configurable for individual files	○	○	○	○	○	●	●	●
Malware protection	○	○	●	○	○	○	○	●
Network-based IDS/IPS	○	○	●	●	○	○	●	●
Host-based firewalling	○	●	○	○	○	●	○	●
VPN between workloads	○	●	○	○	○	○	○	○
Binary control by executable whitelisting	○	○	●	●	○	●	○	●
Policy-based binary privilege escalation	○	○	○	●	○	●	●	○

FIGURE 2 CWS Vendor Capabilities (Cont.)

● Yes ○ No

Solution capabilities	Evident.io	Illumio	Kaspersky	Lacework	RedLock	Symantec	Threat Stack	Trend Micro
Productized integration with DevOps tools	●	●	○	●	●	●	○	○
Supports AWS management console APIs	○	○	○	○	●	●	●	●
Supports Azure management console APIs	○	○	○	○	●	●	○	●
Documented API for headless integration	●	●	●	○	●	●	●	●
ISO 27000 native compliance	○	○	○	○		●	○	●
PCI native compliance	○	●	○	○	○	●	○	●
SOC2 native compliance	○	●	○	○	○	○	○	○
Unsupervised ML-based risk scoring, exposed to customers	○	○	●	●	●	●	○	○
Supervised ML-based risk scoring, exposed to customers	○	○	●	●	○	○	○	○
Guest OS is independent of the kernel	○	●	○	●	●	○	●	○

FIGURE 3 CWS Vendor Business Profiles

Strategy	Alert Logic	Armor	AWS	Bitdefender
R&D spend (as % of annual CWS revenue)	100%*	75%*	5%*	22%
Pricing: CWS solution SaaS policy server	• CloudDefender: $3,990-$28K/ node/month • Threat Manager $550-$7K/ node/month	$200/node/ month	Amazon inspector: $0.03-$0.3/ node/month	$59-10/node/ year
Average annual subscription cost	$30K-$35K*	$50K-$100K*	$12K-$15K*	$850
Pricing: on-premises policy server (pure on-premises deployments)	N/A	N/A	N/A	$37-$1000/ endpoint/year
Pricing: marketplace CWS solution	$0.013/host/hour for the first 50 instances, $.002/ host/hour for 25K+ instances, or AMI-based SaaS billing	N/A	N/A	$0.005-$0.06/ instance/hour
Paying organizations: SaaS CWS in production	4,000	1,100-1,200*	1,000-1,500*	41,300
Paying organizations: marketplace CWS in production	10-15*	0*	100-120*	100
Paying organizations: on-premises CWS in production	0	100	0	10,460
Annual revenues: on-premises	0	0	0	$7.5M
Annual revenues: SaaS	$110M-$115M*	$40M-$45M*	$25M-$30M*	$14.8M
Revenues: geographic splits	• US: 85% • EMEA: 15%	• US+CA: 81%* • LatAm: 0%-1%* • EMEA: 17%* • AP: 2%*	• US+CA: 82%* • LatAm: 0%-1%* • EMEA: 15%* • AP: 3%*	• US+CA: 37.5% • LatAm: 8.3% • EMEA: 34.7% • AP: 4.7%

*Forrester estimates

FIGURE 3 CWS Vendor Business Profiles (Cont.)

Strategy	CloudCheckr	Cloud Conformity	CloudPassage	Dome9
R&D spend (as % of annual CWS revenue)	50%	50%-60%*	37%	45%-55%*
Pricing: CWS solution SaaS policy server	0.75%-2.25% of the spend on the IaaS/PaaS environment	By number AWS account $49/ account/month, $179/account/ month, fixed fee of management: 300-500/month	$0.015-$0.135/node /hour*	Pricing starts at $10/protected asset/month
Average annual subscription cost	$18K	$15K	$300K-$400K*	$60K*
Pricing: on-premises policy server (pure on-premises deployments)	N/A	N/A	N/A	N/A
Pricing: marketplace CWS solution	$3-$96/ instance/hour	N/A	N/A	$0.01/instance/ hour
Paying organizations: SaaS CWS in production	400	42,988	130-150*	210-240*
Paying organizations: marketplace CWS in production	100	0	0*	10-15*
Paying organizations: on-premises CWS in production	0	0	0*	0
Annual revenues: on-premises	0	0	0*	0
Annual revenues: SaaS	$4M	$100K	$15M-$17M*	$2M-$3M*
Revenues: geographic splits	• US+CA: 80%* • LatAm: 1%* • EMEA: 18%* • AP: 1%*	• US+CA: 10%* • LatAm: 0%* • EMEA: 0%* • AP: 90%*	• US+CA: 95%-99%* • LatAm: 0%* • EMEA: 1%-2%* • AP: 0%*	• US+CA: 80%-85%* • LatAm: 0%-1%* • EMEA: 15%-20%* • AP: 0%*

*Forrester estimates

FIGURE 3 CWS Vendor Business Profiles (Cont.)

Strategy	Evident.io	Illumio	Kaspersky	Lacework
R&D spend (as % of annual CWS revenue)	130%-150%*	50%-60%*	20%-30%*	71%
Pricing: CWS solution SaaS policy server	$500-$1,000/ account/month	$300/node/year*	N/A	$0.015/instance /hour, $250/ instance/year
Average annual subscription cost	$71K/year	$300K-$400K*	N/A	$100K-$150K
Pricing: on-premises policy server (pure on-premises deployments)	N/A	$300/node/year*	$250-$300/core/ year, or $30-$50/ desktop/year, or $80-$110/ server/year*	N/A
Pricing: marketplace CWS solution	$500-$1,000/ account/month	N/A	N/A	$0.015-$0.045/ instance/hour depending on size of the instance
Paying organizations: SaaS CWS in production	220	10*	0	5-10*
Paying organizations: marketplace CWS in production	215	0	0	5-10*
Paying organizations: on-premises CWS in production	3	40*	20-30*	0
Annual revenues: on-premises	0	$25M-$28M*	$1M-$2M*	0
Annual revenues: SaaS	$15M-$18M*	$3M-$4M*	0	$500k-$1M*
Revenues: geographic splits	• US+CA: 95% • LatAm: 0% • EMEA: 2% • AP: 3%	• US+CA: 95%-98%* • LatAm: 0%* • EMEA: 2%-5%* • AP: 0%*	• US+CA: 1%-2%* • LatAm: 0%-2%* • EMEA: 95%-98%* • AP: 0%-2%*	• US+CA: 80% • LatAm: 0% • EMEA: 20% • AP: 0%

*Forrester estimates

FIGURE 3 CWS Vendor Business Profiles (Cont.)

Strategy	RedLock	Symantec	Threat Stack	Trend Micro
R&D spend (as % of annual CWS revenue)	70%-75%*	15%-20%*	30%-40%*	34%
Pricing: CWS solution SaaS policy server	$160-$180/ instance/year*	$0.01-$0.06/ core/hour, or $60-$350/ server/year	$100/node/ month	$0.01-$0.06/ instance/hour, or $400/instance/ year
Average annual subscription cost	$45K-$100K*	$30K-35K*	$300K-$400K*	$300K-$400K*
Pricing: on-premises policy server (pure on-premises deployments)	N/A	$246-$1,125/ server/year		$5,600/CPU, $700/server perpetual
Pricing: marketplace CWS solution	N/A	$0.01-$0.06/ core/hour, or $60-$350/ server/year		$0.01-$0.06/ instance/hour, or $400/instance/ year
Paying organizations: SaaS CWS in production	20-25*	20-30*	250	400-500*
Paying organizations: marketplace CWS in production	0	5-10*	0	200-300*
Paying organizations: on-premises CWS in production	0	1,200-1,250*	0	3,200-3,500*
Annual revenues: on-premises	0	$30M-$35M*	0	$100M-$110M*
Annual revenues: SaaS	$1-$2M*	$1M-$2M*	$4M-$6M*	$20M-$25M*
Revenues: geographic splits	• US+CA: 95%-100%* • LatAm: 0%* • EMEA: 0%-5%* • AP: 0%*	• US+CA: 40%* • LatAm: 10%* • EMEA: 20%* • AP: 30%*	• US+CA: 80%-85%* • LatAm: 0%-3%* • EMEA: 10%-15%* • AP: 0%-3%*	• US+CA: 40%-50%* • LatAm: 3%-5%* • EMEA: 20%-25%* • AP: 25%-30%*

*Forrester estimates

Recommendations

Address Vulnerabilities At Configuration Time To Reduce User Impact

When implementing additional CWS solutions in a complex environment where workloads can live in the cloud or on-premises, and travel between, S&R professionals should:

- **Automate and secure config, operations, and code delivery with minimal changes.** CWS implementations should not require change of the code delivery pipeline and software development life cycle (SDLC) from development organizations. It is a good idea to: 1) address known vulnerabilities in the code base preproduction; 2) patch the workload at build and config time; and 3) test IaaS/container configurations against CSP best practices to avoid misconfigurations.
- **Ensure admins have only need-to-know access to the CWS tool and its configuration.** OneLogin could have prevented its recent breach with a more effective least privileges model. Be sure that configuration recipes, network blueprints and interconnectivity, and app-to-app credentials (passwords) are managed centrally in a privileged identity management tool integrated with the CWS solution and that you regularly audit and review access of all admin users.
- **Combine IaaS API- and workload OS-level CWS for multilayered defense.** API-level CWS functionality is a great tool to keep a running inventory of workloads. It can also monitor activity and traffic between workloads and between a workload and the cloud platform. Using the agent-based CWS functionality, you should also watch what's happening in the workload: how processes are running, how configuration files are changing, what communications are taking on the network interfaces, and how the workload reads and writes data to storage via the hypervisor.

Supplemental Material

Survey Methodology

The Forrester Data Global Business Technographics® Infrastructure Survey, 2016 was fielded in June and July 2016. This online survey included 3,503 respondents in Australia/New Zealand, Brazil, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Endnotes

[1] Source: Forrester Data Global Business Technographics Infrastructure Survey, 2016.

[2] Source: Brian Krebs, "OneLogin: Breach Exposed Ability to Decrypt Data," Krebs on Security, June 1, 2017 (https://krebsonsecurity.com/2017/06/onelogin-breach-exposed-ability-to-decrypt-data/) and Devin Coldewey, "OneLogin admits recent breach is pretty dang serious," TechCrunch, June 1, 2017 (https://techcrunch.com/2017/06/01/onelogin-admits-recent-breach-is-pretty-dang-serious/).

[3] The solution does not require agents for exposure, vulnerability and asset visibility, and cloud log ingestion; however, it does require agents for network-based threat detection.

[4] AWS is a platform that offers more than 90 services that provide some components of CWS functionality. For example, securing IaaS (EC2) is different from securing an RDS database instance, and is different from securing IoT devices. Serverless architectures don't need firewalls, for example, whereas EC2 instances do. AWS security interweaves the AWS platform and uses a common SDK, one management console, one CLI, and a common policy language.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

139051