Solution Showcase

Closing the Hybrid Cloud Security Gap with Cavirin

Date: June 2018 **Author:** Doug Cahill, Senior Analyst

Abstract: Most organizations are operating hybrid clouds comprised of on-premises and public cloud infrastructure platforms hosting an array of new and legacy technologies including bare metal servers, virtual machines, and application containers. Such heterogeneity, along with the ongoing shift of server workloads to public clouds, has complicated cybersecurity objectives headlined by a visibility gap. The lack of visibility into cloud-resident assets is part of a broader cloud security readiness gap, the delta between the degree to which companies have already adopted cloud services and their ability to secure that use. IT and cybersecurity professionals need to close both gaps with strategies and solutions that move at the speed of the cloud. The Cavirin CyberPosture Intelligence for the hybrid cloud risk and security management platform provides a set of visibility and control capabilities that allows organizations to automate security policy across their hybrid cloud data centers to reduce a growing attack surface area and assure compliance with industry regulations.

The Realities of Securing Hybrid Clouds

More organizations are leveraging the elasticity of public cloud platforms to gain agility in an increasingly competitive business environment. The cybersecurity charter of mitigating risk is complicated by the resulting expansion of the attack surface, a diversity of asset types to be protected, and a culture of moving at the speed of DevOps.

The Shift of Workloads to Public Clouds Creates a Visibility Gap and New Perimeters

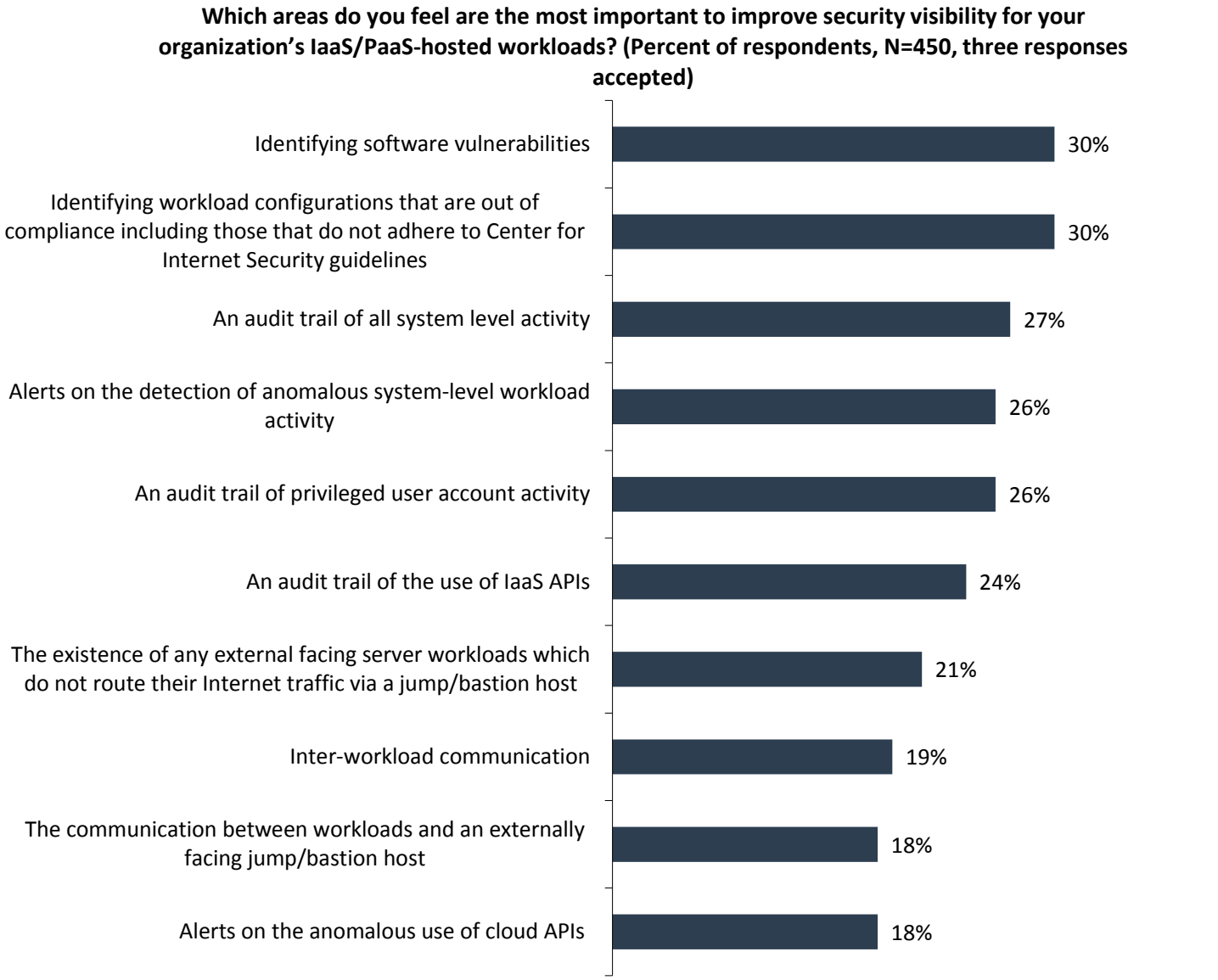
An oft-heard refrain that captures a common concern about securing public cloud platforms is a lack of visibility. The root cause for this perspective is the shift of server workloads to public clouds that challenges the definition of the network perimeter and the persistence of workloads. According to research conducted by ESG, businesses plan to increase the number of workloads they have deployed in a public cloud platform. In fact, while 26% of respondent organizations state that 31-50% of their production workloads run on public cloud infrastructure services today, 40% of organizations expect to be running 31-50% of their workloads in the public cloud 24 months from now.[1]

Network-based approaches to gain visibility are ill-equipped to provide the same level of instrumentation for workloads running in public cloud platforms. ESG's research highlights the fact that this shift of workloads has created a set of visibility concerns centered around the ability to vet software and configuration vulnerability and auditing and alerting on intra- and inter-workload activity (see Figure 1).

Network-based approaches to gain visibility are ill-equipped to provide the same level of instrumentation for workloads running in public cloud platforms.

[1] Source: ESG Master Survey Results, *Trends in Hybrid Cloud Security*, March 2018. All ESG research references and charts in this solution showcase have been taken from this set of master survey results unless otherwise noted.

Figure 1. Improving Security Visibility for IaaS/PaaS-hosted Workloads



Source: Enterprise Strategy Group

The Many Dimensions of Hybrid Clouds Creates Complexity

While the use of public cloud environments is broad-based, these new technologies will coexist with existing elements of the traditional customer-managed data center, resulting in multiple dimensions that need to be secured.

Application Containers Are Creating a Heterogeneous Mix of Server Workload Types

Application containers are an increasingly prominent dimension of hybrid clouds, with 56% of organizations having already deployed containers to production and another 24% planning to do so in the next 12 months. Since they are employed for both new and legacy applications and deployed on-premises and in public clouds, applications containers will share those environments with virtual machines and bare metal servers. According to ESG research, while the blend of containers will

expand from 19% today to 33% in 24 months, respondents noted that 41% of their server types will be VMs and 26% will still be bare metal servers in the same timeframe.[2]

Multi-cloud Adoption Is Creating a Heterogeneous Mix of IaaS Platforms

ESG research also reveals that many organizations are adopting a multi-cloud strategy. Of those organizations that indicated that they are consuming IaaS services, 81% are doing so from more than one provider.[3]

Closing the Cloud Security Gap

The discussion about hybrid cloud security appropriately starts with an overview of what is fundamentally different about the public cloud infrastructure portion of a hybrid cloud. A foundational cloud security construct is the shared responsibility model, which depicts the division of labor between the cloud service provider (CSP) and the subscriber, highlighting how IT and cybersecurity professionals should approach closing the cloud security gap. With that demarcation in mind, IT and cybersecurity professionals should then consider the following best practices.

Employ a Workload-centric Approach

The shift of workloads to public clouds creates a new perimeter, a server workload perimeter that, in turn, requires a workload-centric approach. Such an approach must include gaining visibility via the following best practices:

- Continuously update an inventory of all types of on-premises and cloud-resident workloads.
- Assess the risk profile of all server workloads to enable security and compliance uses cases.
- Reduce the attack surface area by identifying and remediating software and configuration vulnerabilities.
- Audit and alert on anomalous system activity and inter-workload east-west communications.

Unify Across the Dimensions of the Hybrid Environment

The modality for securing hybrid clouds is clearly changing. While 70% of organizations who participated in ESG research stated that they employ different controls for securing public cloud resources and on-premises VMs and servers, the same percentage of respondents shared that they intend to unify controls for all server types across public cloud(s) and on-premises environments within the next two years. And with good reason—a unified approach to workload security independent of server type and location assures consistency of policy, improving an organization's cybersecurity posture across its hybrid cloud.

> …a unified approach to workload security independent of server type and location assures consistency of policy…

Automate Security via DevOps

The challenge of managing the complexities of multidimensional hybrid clouds is exacerbated by an ongoing acute shortage of resources, with 51% of organizations citing a problematic shortage of cybersecurity skills.[4] These dynamics make automating the introduction of security controls an essential element of a hybrid cloud strategy and is likely why 40% of ESG research participants are evaluating security use cases that leverage DevOps processes. Such "DevSecOps" use cases include:

- Identifying workload configuration and software vulnerabilities before deployment to production.
- Applying preventative controls and those that can detect anomalous activity and more.

[2] Source: ESG Brief, *The Growth in the Use of Application Containers*, May 2018.
[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[4] ibid.

Automating Continuous Hybrid Cloud Security with Cavirin

Cavirin's CyberPosture Intelligence employs a pragmatic methodology to automate a workload-centric approach for the hybrid cloud.

Risk-based Visibility via CyberPosture

Cavirin's CyberPosture is a CISO-focused risk and cybersecurity assessment framework that leverages the intelligence provided by the underlying Cavirin platform. CyberPosture reflects the relative state of security, risk, and compliance based on factor-driven quantitative scoring systems. The key variables that contribute to these scores include vulnerability and configuration assessments, monitoring, alignment with cybersecurity and compliance audit frameworks and benchmarks, and more. Historical scores are retained and displayed on a timeline so CISOs can view and manage the status of their organization's cybersecurity posture in data intervals.

A Pragmatic Methodology-based Automation Framework

Cavirin's repeatable automation framework is a methodology comprised of four intertwined and repeating phases (see Figure 2).

Figure 2. Cavirin's Automation Framework

Source: Enterprise Strategy Group

Protect

Cavirin reduces an organization's attack surface area by comparing server workload configurations against industry standard benchmarks such as those defined by the Center for Internet Security (CIS), AWS, and operating system vendors and by identifying known software vulnerabilities.

Monitor

The Monitor phase of Cavirin's automation framework provides continuous assessments of server workloads by detecting anomalies so IT and cybersecurity professionals can be forewarned of drift against a "golden" CyberPosture score.

Respond

To automate taking action on any drift detected in the Monitor phase, the Cavirin platform prioritizes response plans based on maximizing CyberPosture scores (inversely proportional to risk). A prioritized remediation gap report enables improvement of the CyberPosture by minimizing the remediation actions required, thereby saving time and resources.

Predict

As organizations affect changes based on Cavirin's response plans, the platform predicts the impact of those changes on CyberPosture, thus closing the loop from change management to security posture. By leveraging and analyzing via machine learning data collected from the prior three stages, Cavirin can help organizations predict future security issues and provide actionable insights and recommendations to improve their cybersecurity posture.

DevOps Friendly

Cavirin integrates with DevOps continuous integration and continuous delivery (CI/CD) tools to automate the functionality enabled by the four phases of the platform's methodology. Oft referred to as "DevSecOps," automating security via DevOps improves the cybersecurity posture of an organization's hybrid cloud workload footprint by integrating security in development, test, and production environments. For example, Cavirin's Protect phase functionality can automate the hardening of server workloads before deployment to production while the Monitor and Respond phases secure workloads at run time in production.

The Bigger Truth

The strategic imperative to leverage the agility of the cloud has created a readiness gap that IT must close by retooling cybersecurity processes, skills, and technologies. The complexities inherent in the multiple dimensions of today's hybrid cloud data centers have made such adaptations challenging, with effectiveness and efficiency too often mutually exclusive outcomes. However, an organization's cybersecurity, compliance, and efficiency objectives can be realized by leveraging automation and a unified approach to hybrid cloud security. Organizations will need to employ purposeful solutions, designed for the dimensions and scale of hybrid clouds, to unify and automate cybersecurity. Cavirin's hybrid cloud security platform supports the heterogeneous nature of hybrid clouds and provides a DevOps-oriented automation framework that allows businesses to integrate security as an immutable component of their IT infrastructure.