Trellix

SOLUTION BRIEF

Trellix Cloudvisory

A federal solution for cloud misconfigurations

The shared responsibility model

Every CIO and CISO in the US federal government has been tasked with prioritizing a path to utilizing public cloud infrastructure as a service (IaaS). While public cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform provide their users with a secure environment from which to operate, their tenants are responsible for protecting their own workloads.

Moving to the cloud provides tremendous advantages for federal CIOs—agility, elasticity, scalability, and resiliency. However, the gradual erosion of the traditional network perimeter multiplies the ways in which enterprise risk can enter the equation.

The players

The role of securing the enterprise falls to three teams that each have their own focus, speak their own language, and work at different speeds. Security teams are focused on both protecting the perimeter from external threats across traditional threat vectors (email, network, endpoint) and monitoring their internal teams.

In contrast, cloud infrastructure teams are tasked with administrating access to cloud services and optimizing the footprint of their IaaS.

Finally, the DevOps team is held to strict development timelines as they push the boundaries of automating application delivery and business optimization.

Ultimately, the security team often loses visibility into both the infrastructure and DevOps team activities. This disparity ensures all teams are no longer working in harmony towards the federal mission. Security teams can't be the enabler of business objectives.

Elevated enterprise risk

Simple misconfigurations and mistakes in the cloud carry added gravity as well. One simple change to a port, protocol, or service can expose your vulnerabilities to a wide range of users. Even within AWS GovCloud, for example, federal customers can expose their crown jewels to those within state and local governments, as well as members of the defense industrial base. Some teams may also open the environment to additional risk by bringing in code in unvetted container images pulled from repositories like GitHub.

Typical security challenges

Federal CIOs and CISOs want to move their workloads to the edge. However, while they may be effectively protecting their perimeter, they may not be as resilient when it comes to defending their disparate cloud environments. Limited visibility is only a symptom of the larger problems they face.

To protect their workloads, they must first focus on the regulatory compliance frameworks that govern how each organization protects its data. In addition to National Institute of Standards and Technology, federal environments must adhere to several other standards such as Federal Information Security Management Act, Defense Information Systems Agency Security Technical Implementation Guides, and depending on their mission, Health Insurance Portability and Accountability Act and Payment Card Industry Data Security Standard. Unfortunately, for most environments this is a manual and onerous audit process.

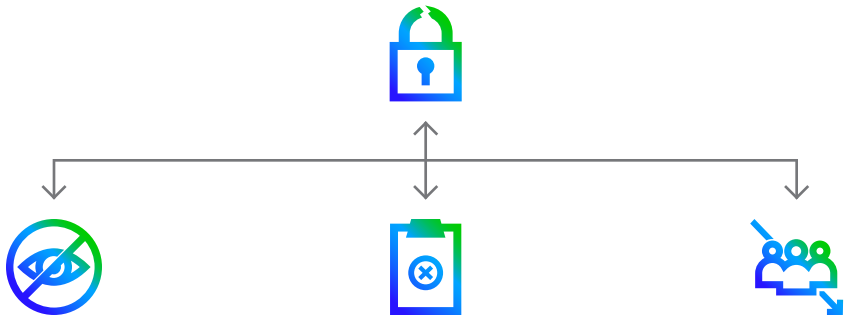

Figure 1. SLED challenges include visibility issues, compliance requisites, and a shortage of skilled staff

Additionally, there is a finite amount of expertise in both traditional cybersecurity and cloud infrastructure roles. Finding and retaining talent that possess both of those skill sets can be daunting and expensive. Ultimately, federal CISOs find themselves in a vicious cycle: they must train staff in more advanced skills only to have them leave the organization for other opportunities.

The options

Federal CISOs often find themselves trying to decide whether to outsource the auditing of their disparate cloud environments. If they choose to outsource to a large consulting firm with a bench of cloud expertise, costs can be quite high for a compliance report that only represents a brief snapshot of their environment suspended in time. After the auditors walk out the door, CISOs must still identify how to address any security concerns that were flagged. If they don't put plans of action and milestones in place to correct misconfigurations, risk to the enterprise can compound quickly.

Should they choose to deal with this process internally, they must train their virtualization or security administrators. In the current tight hiring market, a cleared virtualization administrator with certifications for AWS, Azure, and Google Cloud Platform might see their market value double in a matter of weeks. With a finite budget, CISOs will likely be unable to prevent their talent from leaving to other organizations.

The solution

Federal CISOs need continuous visibility across their cloud and containerized environments, and a way to give their teams information on how to remediate misconfigurations. Such capabilities would not only provide them with an audit trail, but also allow them a framework to begin to protect their cloud environments.

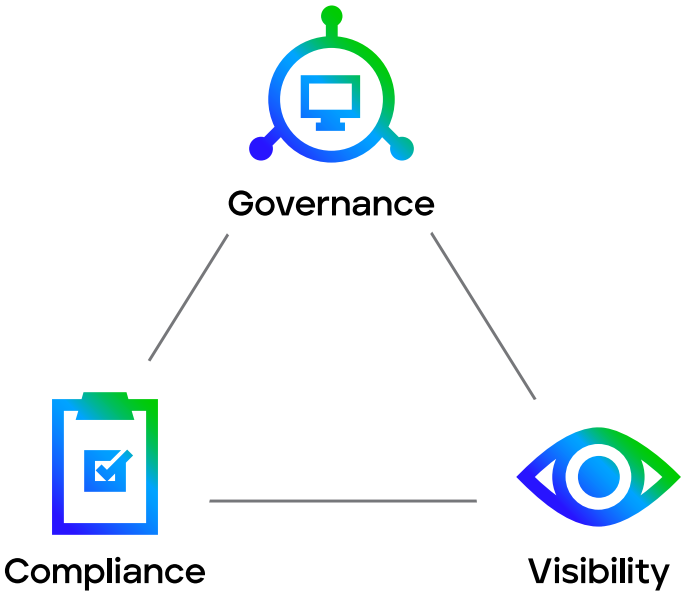

Figure 2.
CISOs must balance governance, compliance, and visibility across their IT environments

Trellix Cloudvisory offers federal CISOs a control hub for cyber resiliency in the cloud. Cloudvisory provides organizations visibility into cloud assets, real-time auditing of compliance frameworks, and governance of cloud infrastructure.

This allows their security personnel to effectively speak the same language as their infrastructure and DevOps counterparts. Clear communication leads to consistent expectations between teams, resulting in mission success.

The Cloudvisory difference

Machine learning

Offers a complete set of intelligent tools that work together to empower cloud security posture improvement

Intelligent microsegmentation

Governance of microsegmentation policies is provided via cloud-native firewalls and security controls

Multicloud native support

In addition to public cloud providers such as AWS and Azure, Cloudvisory supports cloud-native visibility, compliance, and governance for OpenStack and Kubernetes

Orchestrated remediation

Cloudvisory orchestrates remediation of compliance failures and governance of desired-state security policies

Agentless monitoring and execution

Agentless monitoring of all network flows across multiple cloud providers and accounts

At the end of a shift or a busy week, security teams can remediate their infrastructure back into a hardened and compliant baseline. Should anomalous behavior introduce added risk to the enterprise, the security team can effectively step in to limit the threat in real time.

By applying built-in intelligence gleaned from addressing cyberattacks in the cloud, Cloudvisory can help federal CISOs and their teams transition from cloud compliance to cloud protection. With time and effort, good processes will help organizations progress from protecting to defending, and from defending to cyber resilience.

To learn more about Trellix Cloudvisory, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

Copyright © 2022 Musarubra US LLC 052022-01