SOLUTION BRIEF

Trellix Cloudvisory

A SLED solution for cloud misconfigurations

The shared responsibility model

Every CIO and CISO in state, local government, and educational (SLED) institutions has been tasked with prioritizing the use of 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 users with a secure environment from which to operate, their tenants are responsible for protecting their own workloads.

Moving to the cloud provides tremendous upsides for SLED CIOs—agility, elasticity, scalability, and resiliency. However, the gradual erosion of the traditional perimeter multiplies the enterprise risk.

The players

Securing the enterprise falls to three teams that each have a unique focus, speak their own language, and work at appropriate speeds. The security team focuses on both protecting the network perimeter from external threats across traditional threat vectors (email, network, endpoint) and monitoring their internal teams.

In contrast, the cloud infrastructure team administers access to cloud services and optimizes the footprint of their IaaS. Finally, the DevOps team defines and administers strict development timelines as they push the boundaries of automating application delivery and business optimization.

Given the operational framework, the security team often loses visibility into both infrastructure and DevOps team activities. This disparity means teams are no longer working in harmony toward the SLED institution mission. Security teams can’t be the enabler of business objectives.

Elevated enterprise risk

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

Typical security challenges

SLED institution CIOs and CISOs want to move their workloads to the edge. 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. State and local environments must adhere to several standards in addition to National Institute of Standards and Technology, such as Federal Information Security Management Act and, depending on their mission, Health Insurance Portability and Accountability Act, HITECH, and Payment Card Industry Data Security Standard. Unfortunately, for most environments this is a manual and onerous audit process.

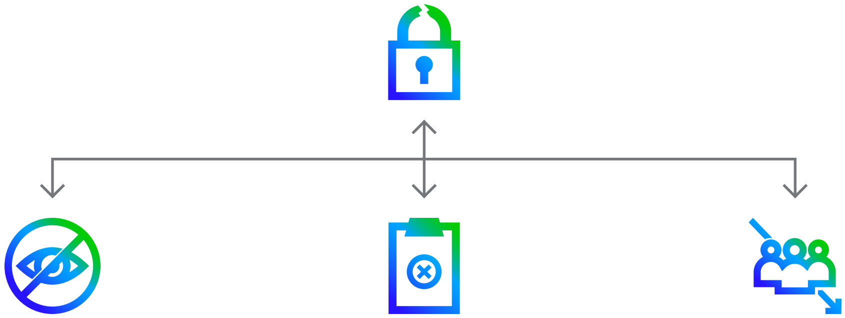

Figure 1. SLED challenges include visibility issues, compliance requisites, and a shortage of skilled staff

Additionally, there’s limited expertise in both traditional cybersecurity and cloud infrastructure roles. Finding and retaining talent who possess both those skill sets can be daunting and expensive. Ultimately, SLED institution CISOs find themselves in a vicious cycle: train staff on more advanced skills and then try not to lose them to other organizations.

The options

SLED institution 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 cloud expertise, costs can be 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 job market, a 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 might find it difficult to prevent their talent from leaving to greener pastures.

The solution

SLED institution CISOs need continuous visibility across their cloud and containerized environments and a way to give their teams information on how to remediate misconfigurations. Such a capability not only provides an audit trail but also offers a framework for protecting cloud environments.

Trellix Cloudvisory offers SLED institution 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.

The solution 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.

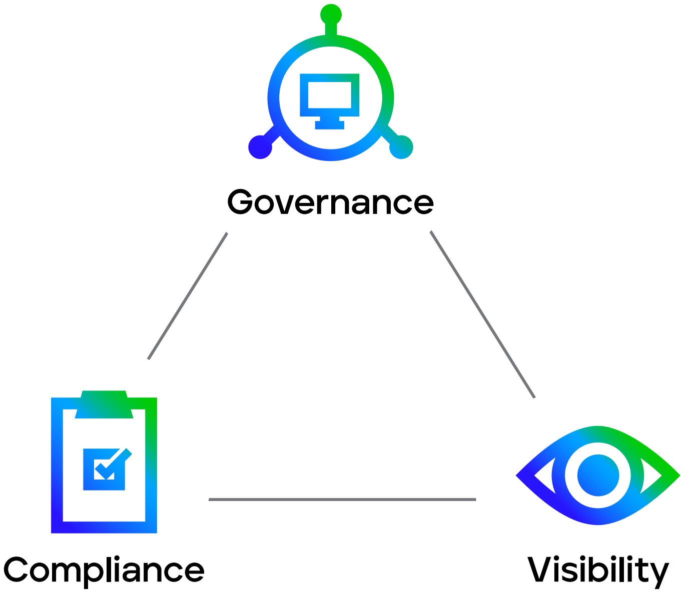

Figure 2.
CISOs must balance governance, compliance, and visibility across their IT environments

The Cloudvisory difference

At the end of a shift or a busy week, the security team 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 intelligence learned from dealing with cloud cyberattacks, Cloudvisory can help SLED institution CISOs transition from cloud compliance to cloud protection. With time and effort, good processes will help them progress from protecting to defending to cyber resilience.

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

Machine learning

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

Intelligent microsegmentation

Cloud-native governance of microsegmentation policies via cloud-native firewalls and security controls

Multicloud, native support

Cloud-native visibility, compliance, and governance support for OpenStack and Kubernetes in addition to public cloud providers such as AWS and Azure

Orchestrated remediation

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

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.