FIREEYE™

SOLUTION BRIEF

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 a path to utilizing public cloud infrastructure-as-a-service (IaaS). While public cloud service providers (CSPs) such as AWS, 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 upsides for SLED CIOs—agility, elasticity, scalability and resiliency. However, the gradual erosion of the traditional perimeter multiplies the ways in which enterprise risk can enter the equation.

The Players
The role of securing the enterprise falls to three separate teams that each have a unique 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 loses visibility into both the infrastructure and DevOps team activities. This disparity ensures all teams are no longer working in harmony towards the State, Local Government and Education institution mission. Security teams cannot 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 flaws to a wide range of users. Even within AWS GovCloud, for example, 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 (DIB).

Some teams may also open the environment up to additional risk by bringing in code in unvetted container images pulled from repositories like GitHub.

Typical Security Challenges
Every SLED institution CIO and CISO wants to move their workloads out 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 their data. In addition to NIST standards, state and local government environments must adhere to several other standards such as FISMA and, depending on their mission, HIPAA, HITECH and PCI-DSS. Unfortunately, for most environments this is a manual and onerous audit process.

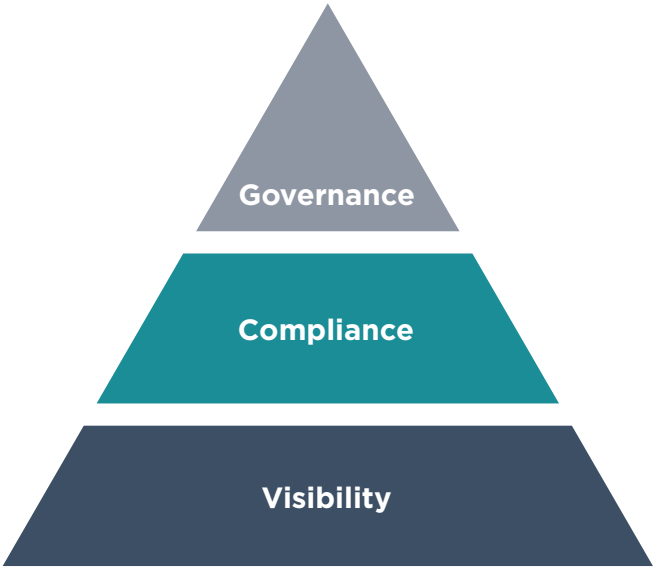
Additionally, there is a finite amount of expertise in both traditional cyber security and cloud infrastructure roles. Finding and retaining talent that possess both of those skillsets can be daunting and expensive. Ultimately, SLED institution CISOs will find themselves in a vicious cycle: they must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

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 their problem 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. Once the auditors walk out the door, the CISO 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 currently tight hiring 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, the CISO will likely be unable to prevent their talent from leaving to another organization.

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 would not only provide them with an audit trail, but also allow them a framework to begin to protect their cloud environments. FireEye 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.



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
A complete set of (artificially) 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

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

Orchestrated Remediation
Orchestrated remediation of compliance failures & governance of desired-state security policies

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

At the end of a shift or a busy week, security 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 Mandiant intelligence learned on the frontlines of cyber attacks in the cloud, Cloudvisory can help SLED institution CISOs transition from cloud compliance to cloud protection. With time and effort, good processes will let them progress from protecting to defending and from defending to cyber resilience.

To learn more about Cloudvisory, visit **www.fireeye.com/products/cloudvisory.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.