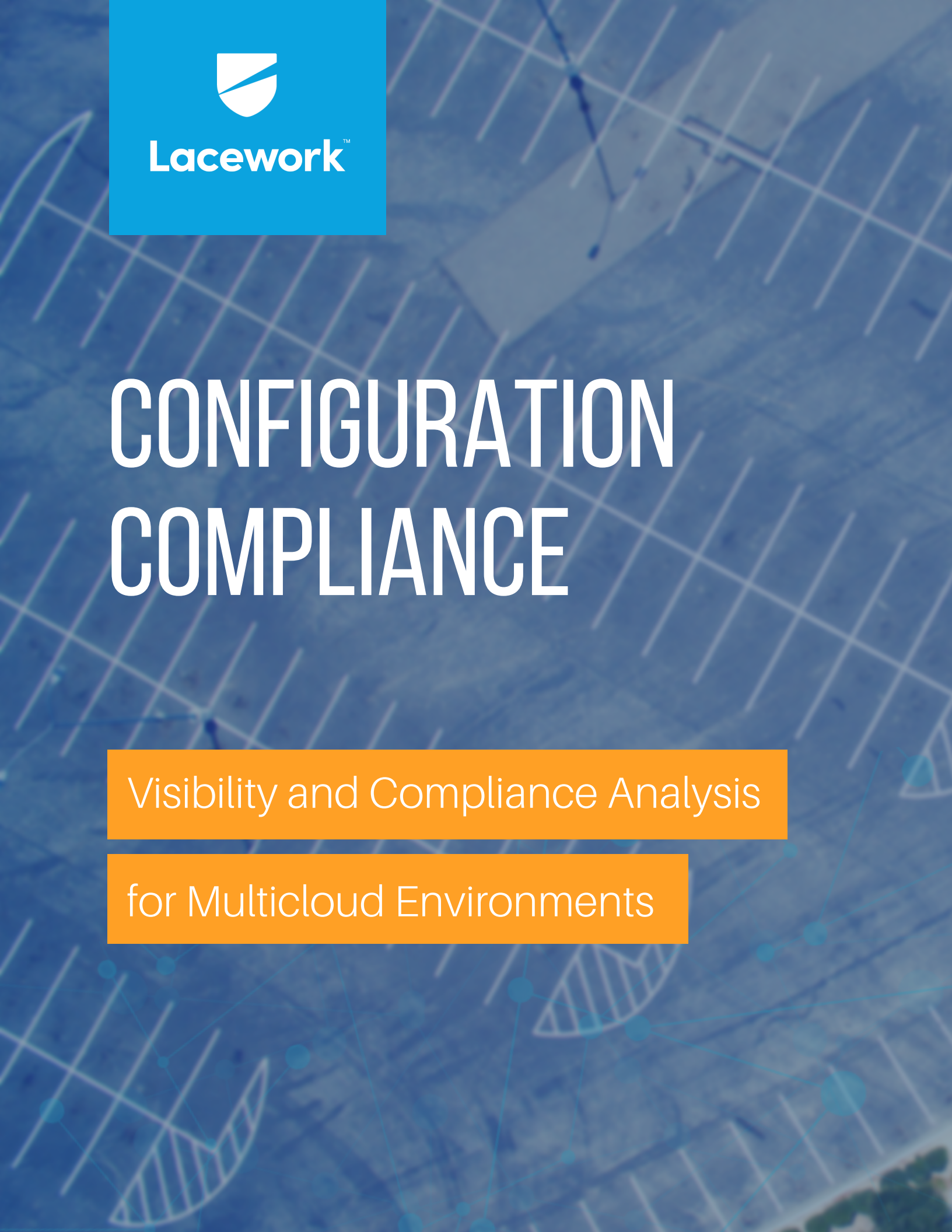
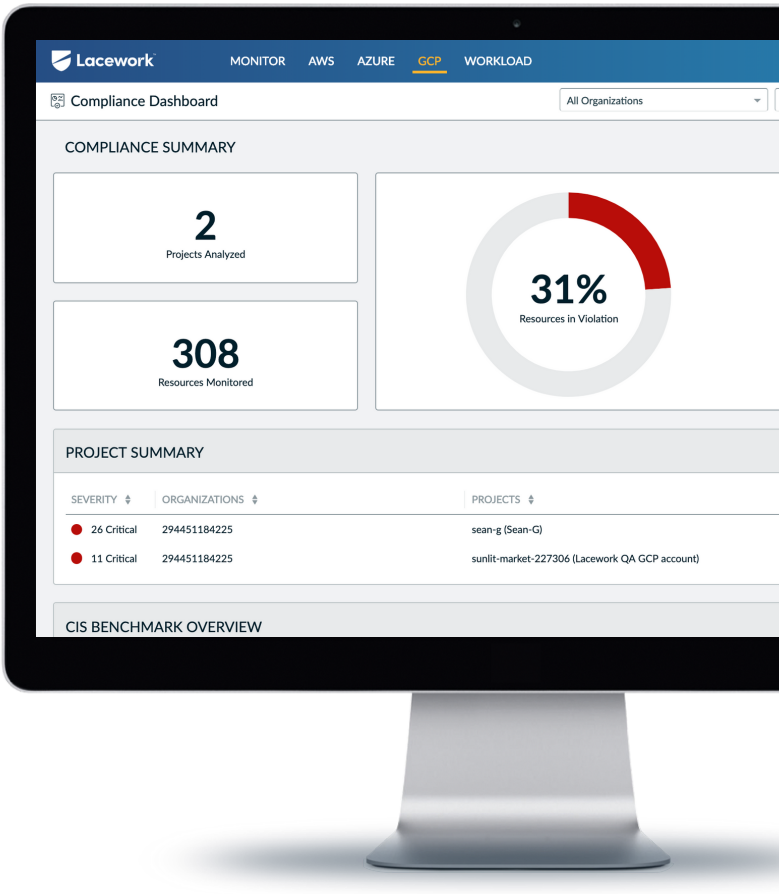

Lacework™
CONFIGURATION COMPLIANCE
Visibility and Compliance Analysis
for Multicloud Environments

CONFIGURATION COMPLIANCE

Visibility and Analysis for Compliance in Multicloud Environments

Lacework delivers deep visibility for configurations across all of an enterprise's cloud accounts and workloads so organizations can ensure compliance with industry, governmental, and institutional standards. Operating on multiple cloud platforms can increase the threat vector of the overall infrastructure and add complexity to an already challenging task. Lacework operates as a comprehensive, centralized solution to identify, analyze, and alert on configuration issues.

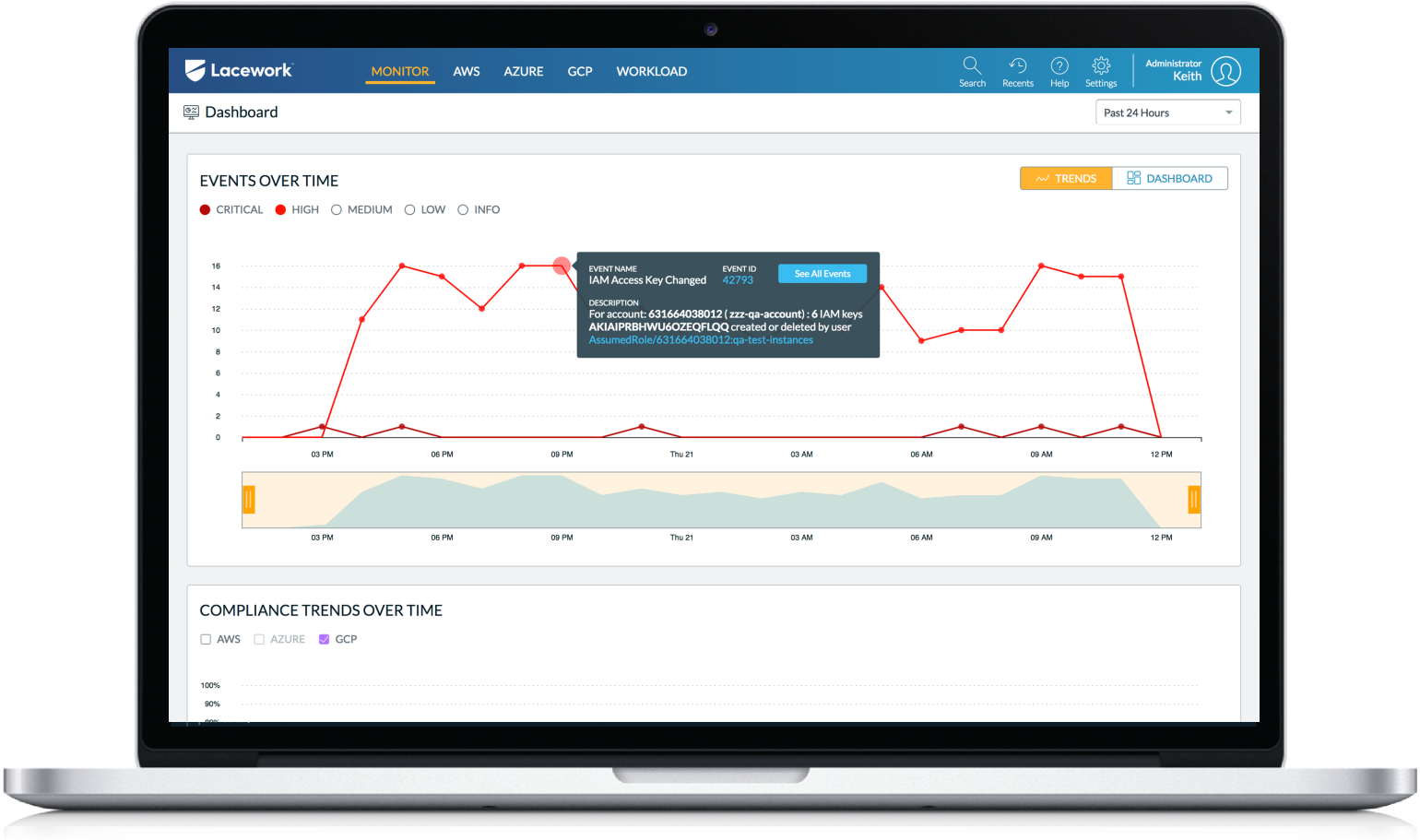


Complexity is an enemy of security; a unified view is essential to simplify the complexity of having multiple configurations. Lacework does this across AWS, GCP, and Azure by bringing multiple clouds into one portal. This means no logging into different disparate tools to evaluate your stance. It is a single pane of glass to audit all of your cloud platform configurations.

Further, as configurations change Lacework will monitor and alert any time a configuration goes out of compliance. This ensures that security and compliance teams immediately become aware of issues so they can be fixed before data and cloud resources are compromised.

IDENTIFY CONFIGURATION ISSUES

- Find Identity and Access Management (IAM) vulnerabilities, including root account, password requirements, and usage of MFA.
- Check for logging best practices enable log files across regions, and enable that log files are validated and encrypted.
- Monitor critical account activity such as unauthorized API calls and use of the management console for unauthorized purposes.
- Confirm secure network configurations, including limiting access to vulnerable ports, enforcing “least access” privileges, and checking for the use of flow logging.



TRACK CONFIGURATION CHANGES CONTINUOUSLY

- Daily re-audit to maintain compliance and protection.
- Monitor account activity for abnormal activity, even when that activity is technical authorized.
- Receive customizable alerts when items change from compliant to non-compliant.

ONGOING MONITORING OF ACTIVITY

- Detection and alerting of activity on all cloud platform resources, such as new activity in a region, activation of new services, or changes to access control lists.
- Changes to users, roles, or access policies.
- Access or customer master key tampering.
- Reduce alert fatigue with customizable alerts and reports that eliminate repetitive or irrelevant results.

CONFIGURATION MANAGEMENT

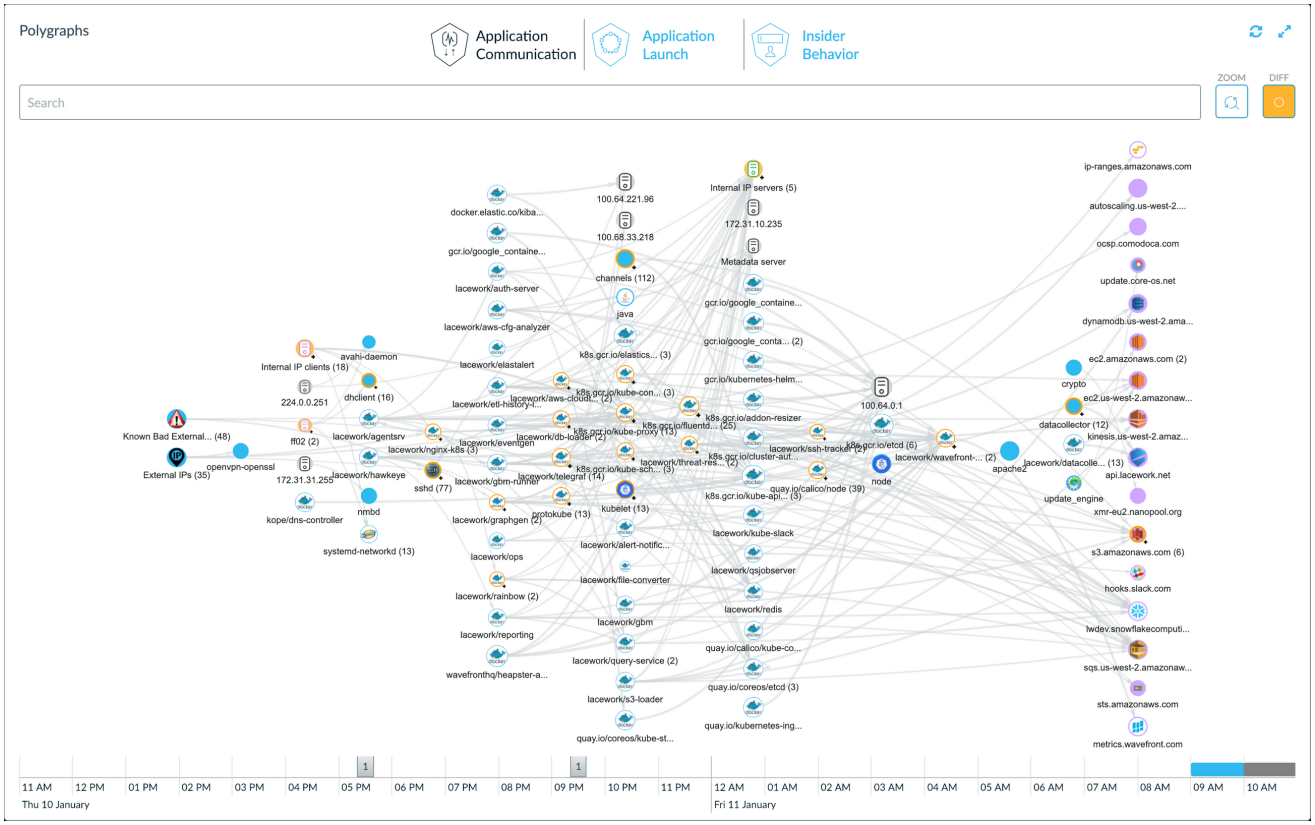
Lacework checks across the industry accepted CIS Benchmark for secure configurations for cloud accounts and workloads. Additionally, Lacework includes supplemental checks for common compliance frameworks like PCI-DSS, SOC 2, HIPAA, and others.

Using Lacework, compliance and security teams have continuous analysis and historical reporting available so they can understand what is being checked, where problems exist, an analysis of the problem, and the steps needed to remediate the misconfiguration. The product supplies links directly to the resources in question to reduce the time to remediate.

The Lacework solution is built to detect behavioral anomalies, so even if configurations meet required standards, unauthorized use or abnormal activity is detected and alerted on. This ensures that organizations are aware of issues that might go undetected by solutions that only identify non-conforming compliance rules.

THE POWER OF POLYGRAPH

Lacework's foundation is Polygraph, a deep temporal baseline built from collecting high fidelity machine/process/users interactions over a period of time. The Polygraph is used to detect anomalies, generate appropriate alerts, and provide a tool for users to investigate and triage issues.



Fundamentally, the Polygraph technology dynamically develops a behavioral and communication model of your services and infrastructure. The model understands natural hierarchies (processes, containers, pods, machines, etc.) and aggregates them to develop behavioral models. A behavioral model is, in some sense, the essence of how a customer's infrastructure operates. With this model, Polygraph monitors your infrastructure for activities that fall outside the model. In addition, the Polygraph continually updates its models as your data center behavior changes.

SECURITY VISIBILITY

Get deep observability into your cloud accounts, workloads, and microservices to give you tighter security control.

THREAT DETECTION

Identify common threats that specifically target your cloud servers, containers, and IaaS accounts so you can action on them before your company is at risk.

ANOMALY DETECTION

Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts that represent a security risk or an IOC.

HOST COMPLIANCE

Achieve compliance for SO2 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS).

CONFIGURATION COMPLIANCE

Spot IaaS account configurations that violate compliance & security best practices the could put your company at risk.