Lacework™

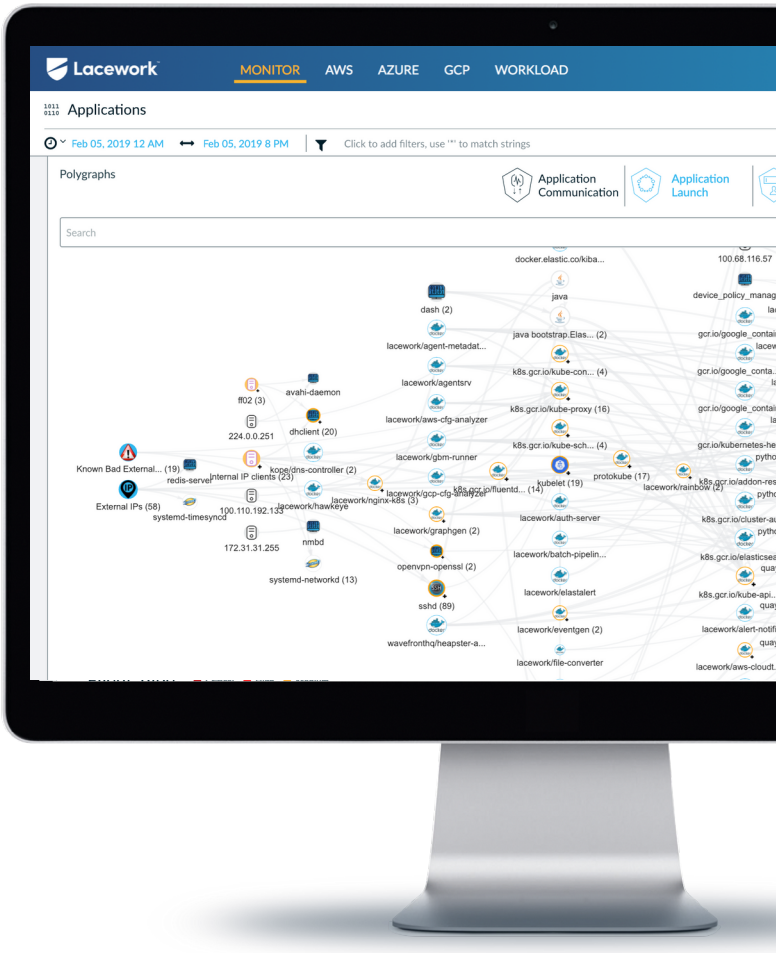
CLOUD ACCOUNT SECURITY

Visibility and Detection of Misconfigurations & Account Vulnerabilities

CLOUD ACCOUNT SECURITY

VISIBILITY AND DETECTION OF MISCONFIGURATIONS AND ACCOUNT VULNERABILITIES

Lacework provides comprehensive security for AWS, Azure, and GCP accounts that provides insights about configuration changes that could lead to threats. At the console level of a cloud environment, an organization can inadvertently apply misconfigurations that could leak data or open up an easy attack surface to a hacker. With continuous updates and broad administrative access happening within cloud environments, account changes are normal. Yet, with increased activity comes increased vulnerability.



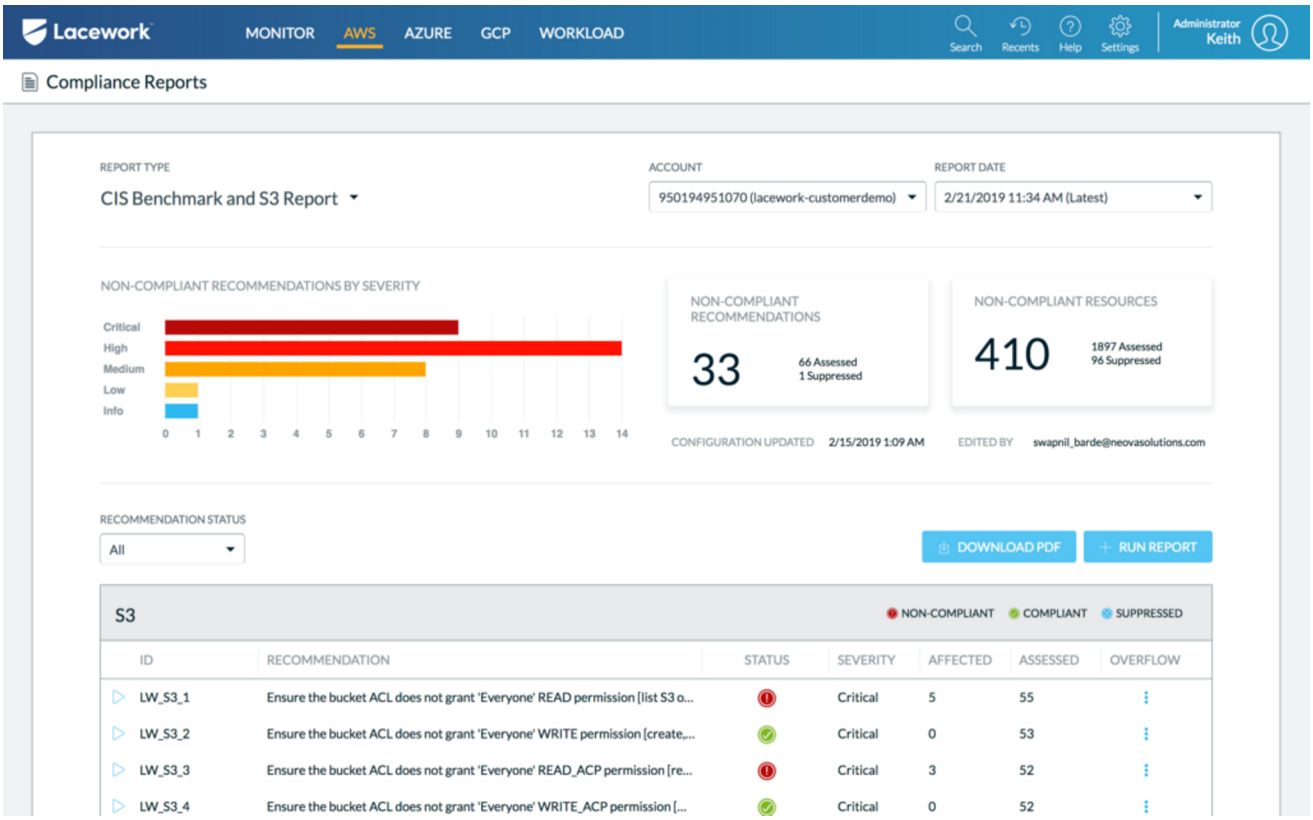
Complexity is an enemy of security; a unified view is essential to simplify the complexity of having multiple configurations. Lacework does this across AWS, GCP, and Azure by bringing multiple clouds into one portal.

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.

Through API integration between with accounts, Lacework looks at all of security-relevant configurations and identifies where the organization is passing or failing certain security best practices for these particular configurations. These checks are run continuously, and security teams receive automated alerts about any configuration changes that violate security compliance. Among the myriad of issues that Lacework is looking for, it is able to identify things such as:

- S3 buckets in AWS that are misconfigured and left publicly open
- Security groups allowing unrestricted access to SSH
- IAM users that don't have MFA enabled
- Security groups that are misconfigured
- New regions are being spun up specifically for Bitcoin mining

Data from the cloud accounts is ingested, and Lacework applies machine learning to logs to generate high fidelity alerts on any behaviors or events that could be an indicator of compromise at the account resource level. Lacework also proactively alerts on any security misconfigurations at the time they occur.



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.

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 SOC 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.