SOLUTION BRIEF

Achieving ISO 27001:2022 compliance

Supply chain and third-party risks pose some of the biggest challenges in the field of security. How can an organization demonstrate to its customers that it is trustworthy enough to handle their data? One solution is to adhere to an industry-standard framework such as the ISO 27001 standard — one of the most common international certifications for information security. For the latest changes to the standard, which is now updated to ISO 27001:2022, Lacework has you covered.

As with any independent audit, the most difficult part of achieving ISO 27001 certification is the audit process. The ISO 27001 standard is flexible, allowing companies leeway on how they meet the guidelines. Organizations must gather lots of evidence both before and during the audit to ensure compliance on an ongoing basis. If your organization has never before achieved ISO 27001, you also face the unknown cost and risk of preparing for the independent audit. This potentially includes going through an internal self-audit to make sure the independent audit is successful. All of this can be time-consuming and expensive.

Lacework can make ISO 27001 audits easier by quickly providing a comprehensive view of your cloud environment and mapping ISO 27001 controls to the cloud security controls monitored by Lacework. At any time, you can choose to run a report that shows exactly how your cloud environment implements ISO 27001 controls, which you can then provide to an auditor. Lacework reports can also review compliance against your multicloud and multi-account environment, allowing your compliance and cloud teams to ensure continued alignment with ISO 27001. Additionally, Lacework reports can be run and reviewed over different time periods, so any compliance drifts can be reviewed and investigated. By preventing issues before the audit and reducing the evidence-gathering time during the audit, Lacework saves organizations time and money.

> **Lacework identified major blind spots across our cloud environments, which is leading to Protegrity's successful ISO 27001 certification."**
>
> SCOTT INGRAM,
> DIRECTOR OF INFORMATION SECURITY
>
> PROTEGRITY

Using Lacework features

The Lacework Polygraph® Data Platform contains many features that will help you on your journey to ISO 27001 compliance, including:

Asset management

Track your cloud resources with the Lacework resource management function. You can edit the resources summary to show different information, including Resource Name, Account ID, Account Alias, Service, Type, Status, etc. You can also export the resource summary to a CSV file, which you can use as evidence of your organization's cloud asset inventory.

Logging and monitoring

Automated monitoring and reporting throughout the development lifecycle helps ensure that you're compliant from day one. Lacework monitors all cloud events, configurations, and behavioral activities on the cloud, offering you a complete view of your entire cloud ecosystem. The events dashboard gives an overview of all events that have been logged in your environment. Event records include a description of why the event was triggered, which account was responsible, what API was affected, and the source IP address. Lacework also enables you to send high-fidelity contextual alerts to your SIEM solution.

Vulnerability scanning

By managing vulnerabilities and compliance continuously, you can mitigate risk as it is introduced into your cloud infrastructure. Lacework automatically and continuously scans your organization's cloud environment for vulnerabilities, which we communicate via alert channels configured by the admin user. The Lacework Vulnerability Assessment summary shows a list of all identified vulnerabilities and rates them based on criticality. You can then export the report to a CSV file to share with auditors.

Host-based intrusion detection system (HIDS)

Lacework acts as a host-based intrusion detection system (HIDS) where an agent is loaded into various types of workloads to gain visibility into changes in baseline behaviors. Lacework can also monitor Kubernetes-based workloads, as well as files within containers and VMs.

> "Within just two months of using Lacework, we significantly improved compliance across our environment. Lacework has had a huge impact on our compliance posture."
>
> NABIL MISSOUM,
> DEVSECOPS ENGINEER
>
> AB Tasty

Compliance over time

Lacework allows for tracking of compliance standards over time. A user can run a compliance report at any time to see the compliance status on an hour-by-hour basis. This enables tracking of compliance status to see what has changed and who changed it.

Communication and information

Stop aggregating reports from multiple systems and start responding to auditors instantly with one-click reporting from our compliance dashboard. This dashboard provides an overview of your organization's compliance posture across all your accounts and groups the ISO 27001 technical controls into a readable PDF or CSV format. The report covers areas such as identity and access management, logging and monitoring, networking, and general security. The report also displays how your organization's cloud configurations are mapped to specific ISO 27001 criteria, showing which need to be addressed and fixed.

Threat intelligence

Lacework uncovers both known and unknown threats across your cloud environment through a combination of threat intelligence and behavior-based threat detection. Lacework gathers information from cloud audit logs and running workloads to find compromises in your cloud accounts and runtime environment.

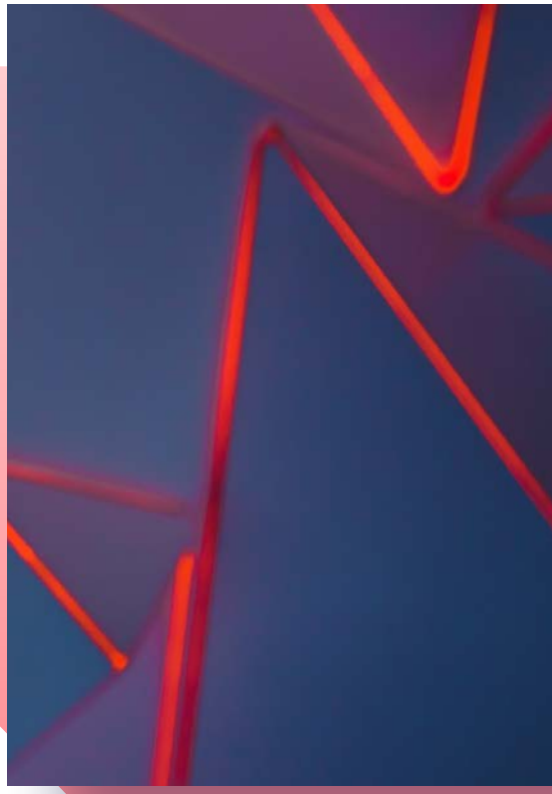
Secure coding

Lacework Infrastructure as Code (IaC) Security integrates into your code repository to scan for security misconfigurations in your IaC prior to the infrastructure being deployed. Lacework can also integrate with your software development life cycle (SDLC) process to scan for vulnerabilities in your containers before they are deployed to production. To help automate security for your Kubernetes environment, you can utilize the Lacework Admission Controller to set container security policies and stop vulnerable containers from being deployed.

Securing your cloud services

Lacework helps organizations secure their use and management of a single or multicloud environment by identifying threats, vulnerabilities, misconfigurations, and unusual activity across cloud accounts, workloads, containers, and Kubernetes.

> "Lacework is a one-stop shop for security and compliance."
>
> GOPI KRISHNAMURTHY,
> VICE PRESIDENT OF PRODUCT
> AND ENGINEERING
>
> CLARINESS



Mapping required security controls

ISO 27001 compliance requirements	Polygraph® Data Platform
Compliance reporting/configuration assurance	Included
User and entity behavior analytics (UEBA)	Included
Container and Kubernetes security (HIDS and vulnerability detection)	Included
Intrusion detection (hosts, containers, and Kubernetes)	Included
Anti-malware (hosts, containers, and Kubernetes)	Included
Vulnerability scanning (hosts and containers)	Included

Ready to chat?

Request a demo