SOLUTION BRIEF

Achieving ISO 27001 Compliance with Lacework

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.

As with any independent audit, the most difficult part of achieving ISO 27001 certification is the audit process itself. The ISO 27001 standard is flexible and allows companies leeway on how they meet the guidelines. It's necessary to gather a lot of evidence both before and during the audit and to ensure compliance on an ongoing basis. If your organization has never achieved ISO 27001 before, you also face the unknown cost and risk of preparing for the independent audit and potentially going through an internal audit to make sure the independent audit is successful, but both are time-consuming and expensive.

Lacework can help with ISO 27001 audits by easily providing a comprehensive view of your cloud environment and mapping ISO 27001 controls to the cloud security controls monitored by Lacework. Lacework reports can be run at any point in time to review compliance against your multicloud and multi-account environment, allowing your compliance team and cloud team to work together to ensure continued compliance to ISO 27001. Additionally, Lacework reports can be run and reviewed over different time periods, so any compliance drifts can be reviewed and investigated. Lacework also facilitates the auditing process: 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 provides a platform that saves you time and money by preventing issues before the audit and by reducing the evidence gathering time during the audit by leveraging just one platform to easily track configuration changes, find vulnerabilities, and detect threats. We also provide a consolidated view to all team members who might not otherwise have access to your Google Cloud management console.

Lacework can help with ISO 27001 audits by easily providing a comprehensive view of your cloud environment and mapping ISO 27001 controls to the cloud security controls monitored by Lacework.

Lacework's unique ISO 27001 advantage

Lacework acts as a "flight recorder" for your environment, collecting and organizing relevant data. We enable organizations to easily meet auditors' evidence gathering requests, drastically reducing the amount of time required for your security or compliance team. In addition, we track this data over time so that you can always go back and review changes to ensure better control of your environment.

USE CASES

Lacework's cloud security platform

The Lacework platform contains many features that will help streamline 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.

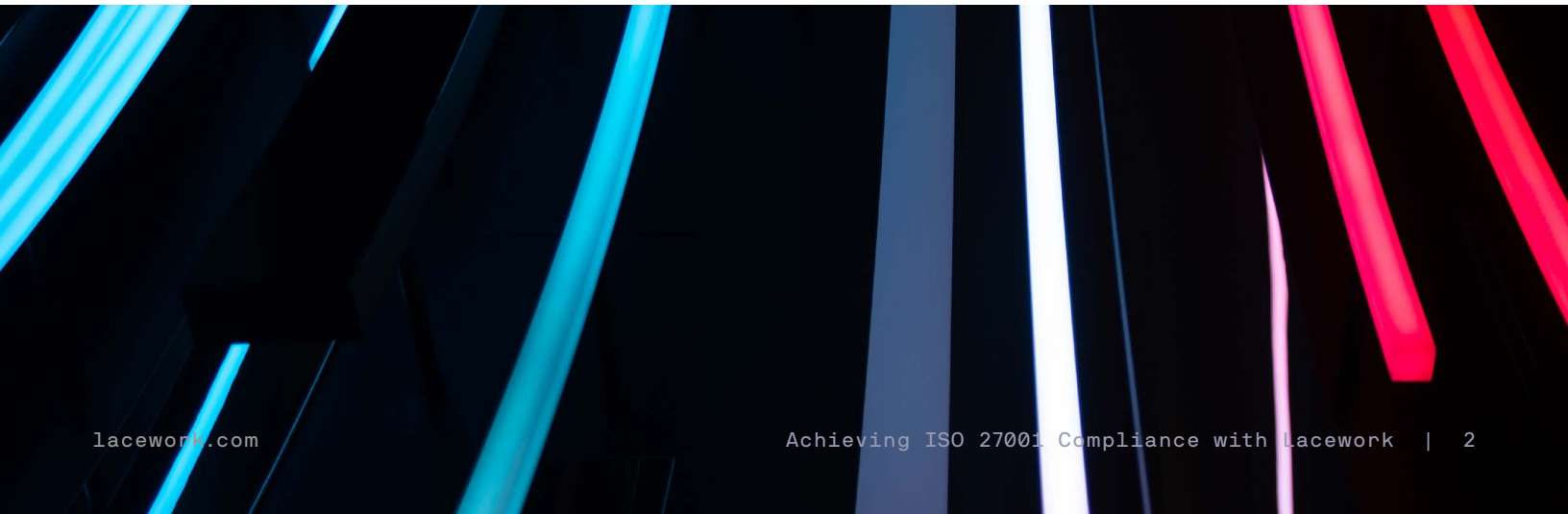
Host intrusion detection system (HIDS)

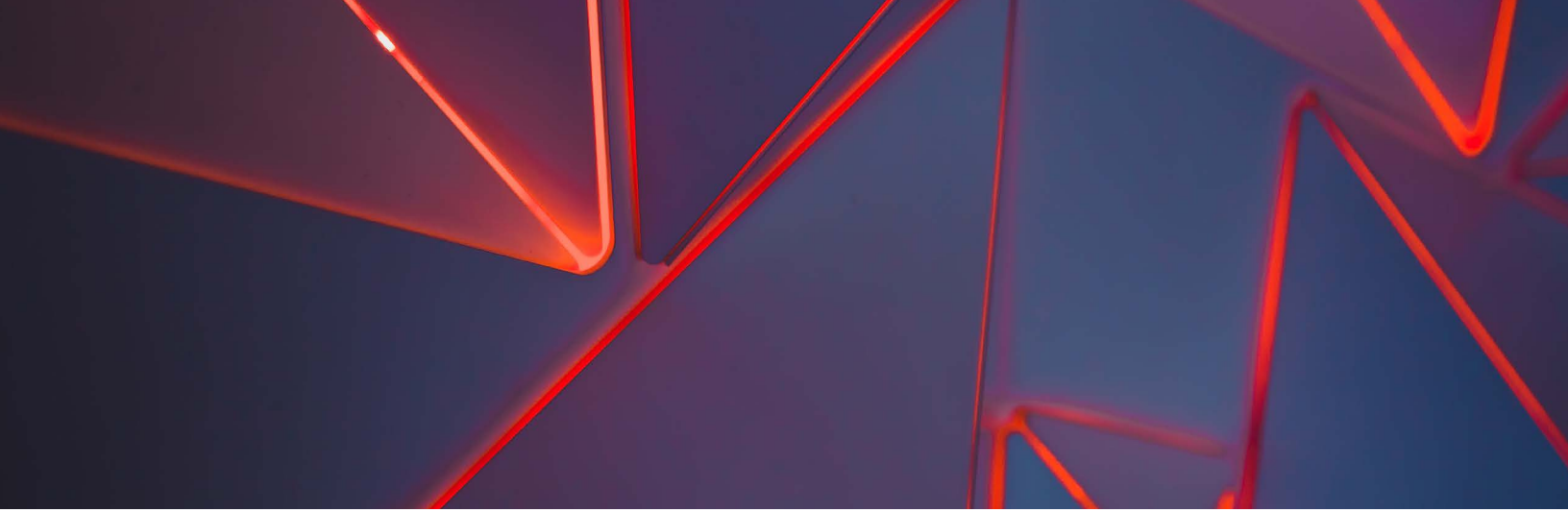
Lacework acts as a host-based intrusion detection system (HIDS) where an agent is loaded into various types of Linux workloads to gain visibility into changes in baseline behaviors. Lacework can also monitor Kubernetes-based workloads as well as files within containers and VMs.

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.

A user can run a compliance report at any time to see the compliance status on an hour-by-hour basis.





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 their 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.

Communication and information

Lacework's compliance dashboard provides an overview of your organization's compliance posture across all your accounts. It also 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. Plus, it displays how your organization's cloud configurations are mapped to specific ISO 27001 criteria, showing which need to be addressed and fixed. With our one-click reporting, you can stop aggregating reports from multiple systems, and start responding to auditors instantly.

Lacework monitors all cloud events, configurations, and behavioral activities on the cloud, offering you a complete view of your entire cloud ecosystem.

Mapping required security controls

ISO 27001 compliance requirements	ISO 27001 control numbers	Lacework platform
Organization of Information Security	A.6.2.2 - Teleworking	Included
Access Control	A.9.1 - Access Control A.9.2 - User Access Management A.9.4 - System and Application Access Control A.9.4.3 - Password Management System	Included
Operations Security	A.12.1.2 - Change Management A.12.4.1 - Event Logging A.12.4.3 - Administrator and Operator Logs A.12.6.1 - Management of Technical Vulnerabilities	Included
Communications Security	A.13.1.3 - Segregation in Networks A.13.2.1 - Information Transfer Policies and Procedures A.13.2.3 - Electronic Messaging	Included
Systems Acquisition, Development and Maintenance	A.14.1.2 - Securing Application Services on Public Networks A.14.1.3 - Protecting Application Services Transactions A.14.3.1 - Protection of Test Data	Included
Compliance	A.18.1.3 - Protection of Records A.18.1.4 - Privacy & Protection of Personally Identifiable Information A.18.1.5 - Regulation of Cryptographic Controls	Included

Ready to chat?

Request a demo