SOLUTION BRIEF

Achieving SOC 2 compliance with Lacework

Lacework helps you achieve compliance and continuously monitor your cloud environments

OVERVIEW

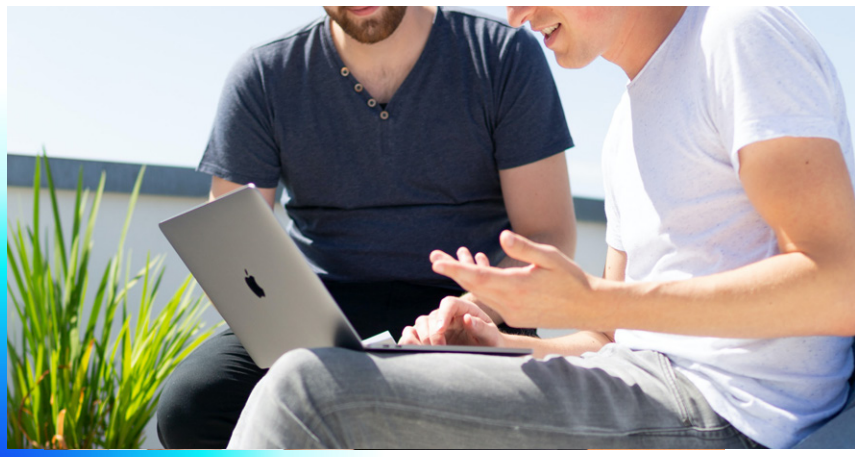
An industry standard

Supply chain and third-party risks pose some of the biggest challenges in the field of security. According to a May 2021 report from SecureLink and Ponemon, 50% of organizations have experienced a breach caused by a third party. How can an organization prove 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 SOC 2 standard, which is one of the most common certifications for information security.

CHALLENGES

Proving SOC 2 compliance

The most difficult part of achieving SOC 2 is having to prove compliance with the framework. Since it's meant to be flexible enough to allow companies leeway on how they meet the guidelines, it's necessary to gather a lot of evidence both before and during the audit. If your organization has never achieved SOC 2 before, you also face the unknown cost and risk of preparing for an audit and potentially going through a pre-audit to make sure the final audit is successful. SOC 2 pre-audits and audits, along with the accompanying need to gather evidence, are time-consuming and expensive.



Key Lacework use cases

- Asset management to track cloud resources
- Automated monitoring throughout development lifecycle
- Continuous vulnerability scanning integrated with alert channels
- Dashboard that visualizes compliance posture
- One-click reporting

OUR APPROACH

Visibility and speed

Lacework can help with SOC 2 audits by easily providing a comprehensive view of your cloud environment and mapping SOC 2 controls to the required cloud security controls. 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 SOC 2. 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 SOC 2 controls, which you can then provide to an auditor. Lacework's platform saves you time and money by preventing issues before the audit and by reducing the evidence gathering time during the audit.

Lacework acts as a "flight recorder" for your environment, collecting and organizing SOC 2-relevant data. We enable organizations to easily meet auditors' evidence gathering requests, drastically reducing the amount of time required for the security team. In addition, we track this data over time so that you can always go back and review changes to ensure better control of their audited environment.

USE CASES

The Lacework advantage

The Lacework platform contains many features that will help streamline your journey to SOC 2 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 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.

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.

Communication and information

Lacework's compliance dashboard provides an overview of your organization's compliance posture across several accounts. It also groups the SOC 2 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 SOC 2 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.

At a glance

Lacework helps with many SOC 2 requirements, including:

- Vulnerability scanning (for host and container)
- Cloud compliance (for multicloud)
- User behavior
- HIDS (for host, containers, and Kubernetes)
- FIM (for host, containers, and Kubernetes)
- Anti-malware (for host, containers, and Kubernetes)

Mapping required security controls

SOC 2 compliance requirements solved with Lacework	SOC 2 control numbers	Lacework platform support
Communication and information	· CC2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Included
Risk assessment	· CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Included
Logical and physical access controls	· CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. · CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. · CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. · CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries. · CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Included
System operations	· CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. · CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Included