CASE STUDY

Protegrity grows compliance posture and gains visibility into multicloud environments

PROTEGRITY

Challenges

- Address blind spots by meeting compliance goals
- Monitor cloud sprawl and growth model with increased visibility into AWS, Google Cloud, and Azure environments
- Reduce operational costs by choosing a single comprehensive platform

Solutions

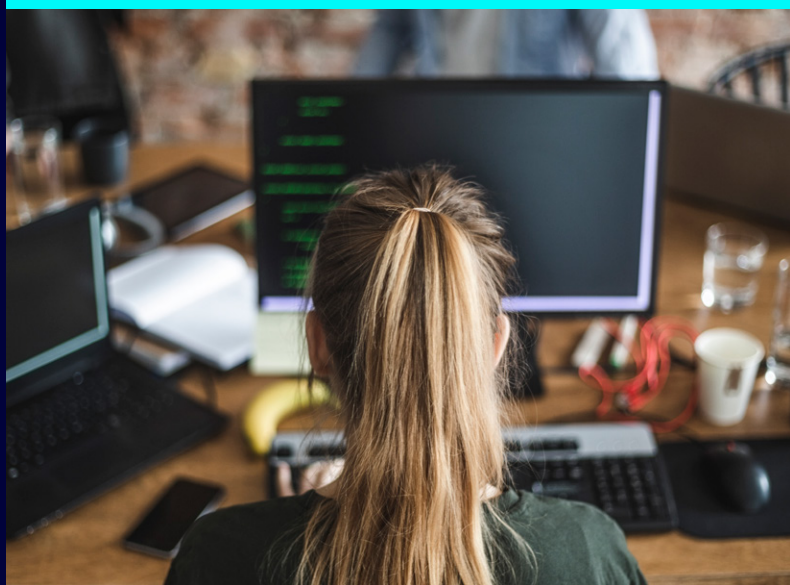
- Received enhanced risk and compliance reporting
- Integrated Lacework with Protegrity DevOps pipeline and containerized strategy, gaining increased transparency
- Transitioned seamlessly from trial to full deployment with on-demand training and support

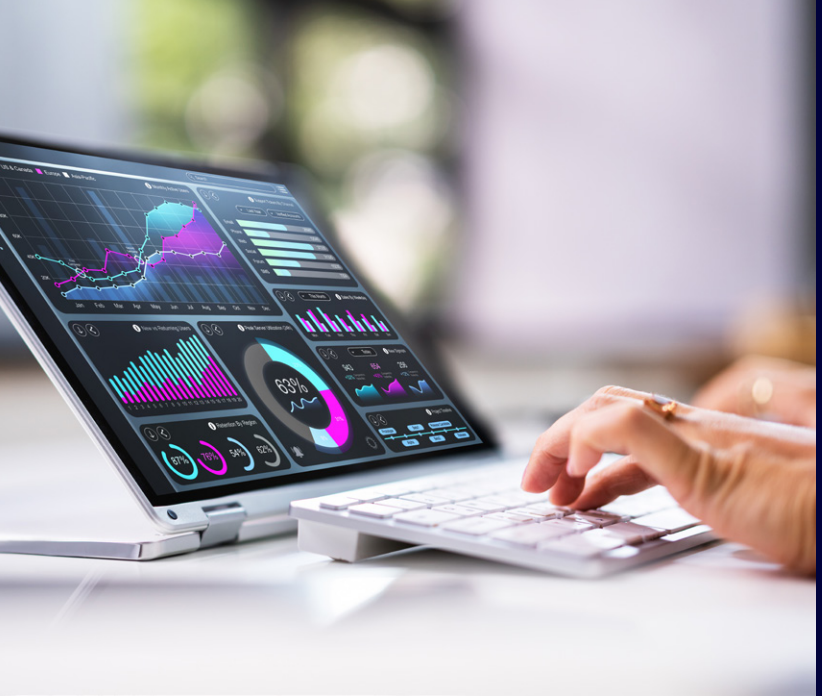
Results

- Stopped compromises with increased visibility into multicloud environment
- Demonstrated compliance to customers with improved reporting capabilities
- Saw a 10x drop in alerting from production areas

"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





> I was impressed that Lacework offered the entire CIS Benchmarks suite and also provided monitoring for ISO, HIPAA, PCI, NIST, and SOC controls."
>
> GOUTAM CHATTERJEE, SENIOR APPLICATION AND CLOUD SECURITY ENGINEER, PROTEGRITY

About Protegrity

Protegrity aspires to protect the world's most sensitive data — whatever it is and wherever it resides at any given moment. Their platform frees businesses from the constraints typically associated with the access and fine-grained protection of sensitive data, so they can have the confidence to create better customer experiences, make intelligent decisions, and fuel innovation. With their core product development based in India and Sweden, plus locations in the United States for sales, HR, and finance teams, Protegrity is a global company.

Scott Ingram, Protegrity's Director of Information Security, is responsible for the company's overall security and compliance. He oversees everything from a security and compliance standpoint, from the research and development division to the shared service areas of finance, accounting, HR, and IT. Working alongside Ingram is Goutam Chatterjee, Senior Application and Cloud Security Engineer. Chatterjee heads a number of security functions at Protegrity, including their vulnerability management system, penetration testing program, and security testing and reporting.

Protegrity is a true multicloud organization, using services from all three major cloud providers — Amazon Web Services (AWS), Google Cloud, and Microsoft Azure — and supporting their security initiatives with a containerized strategy on Kubernetes. "This strategy is vital to our software delivery model of containers and microservices," explains Ingram. "Our customers with highly sensitive data want the assurance of proactive monitoring and patching before, not after."

Challenges

When the Protegrity team started looking for a cloud security provider, it was important that they find a multicloud solution. Two major security objectives underpinned their search. First, they needed strong compliance reporting. "I'm tasked with achieving ISO 27001 certification, and when I went through our different cloud environments, we had a major blind spot," says Ingram. "So, I went to market to find a solution."

Their second priority was to increase visibility into their environments. "It's really hard to monitor our cloud sprawl or our growth model from different tools," states Ingram. Using various tools also meant that they had to consider the operational expense in this area. With these objectives in mind, Protegrity started their Lacework journey.

> "Before Lacework, we did not have a record of how many AWS or Google Cloud accounts were outside of our network, and now we are able to track that, which is a big change. Because of that visibility, we've stopped compromises from happening."
>
> GOUTAM CHATTERJEE, SENIOR APPLICATION AND CLOUD SECURITY ENGINEER, PROTEGRITY

Solution

Before they started trialing Lacework, the Protegrity team developed several criteria for success. "We wanted to see what the Lacework risk and compliance reporting looked like for our AWS and Google instances," says Ingram. Since they were already satisfying compliance standards including CIS Benchmarks, explains Chatterjee, "we were also looking at how Lacework presented different compliance varieties. I was impressed that Lacework offered the entire CIS Benchmarks suite and also provided monitoring for ISO, HIPAA, PCI, NIST, and SOC controls." Beyond compliance, states Ingram, "We were working to integrate security into the DevOps pipeline and extended detection response, so we wanted to see if Lacework could help us in these areas. It successfully hit its mark, allowing us to review our exposure and see how to fix it without false positive fatigue."

Protegrity was ready to deploy Lacework after a successful trial. "Deployment was really seamless," says Ingram. "When we did the proof of concept, the platform was set up for integration. Then, Lacework brought in a team to help us push to production." They received on-demand training while learning the platform – and the support from Lacework has continued ever since. According to Chatterjee, "Whenever we need the Lacework team, they are available, whether that's via chat, in the form of a meeting, or for a quick training."

Protegrity looked at three different vendors, but Lacework stood out from start to finish. "Lacework shined for three reasons: its maturity model, the initial proof of concept, and the run phase support model," Ingram says.

> **"Lacework shined for three reasons: its maturity model, the initial proof of concept, and the run phase support model."**
>
> SCOTT INGRAM, DIRECTOR OF INFORMATION SECURITY, PROTEGRITY

Results

Increased visibility and FIM capabilities

Having visibility into cloud environments is crucial to preventing breaches. "Before Lacework, we did not have a record of how many AWS or Google Cloud accounts were outside of our network, and now we are able to track that, which is a big change," says Chatterjee. "Because of that visibility, we've stopped compromises from happening." As Protegrity continues to grow their remote workforce, visibility will only become more important. "If there are a large number of hits, it's directly proportional to the attack surface, which will be bigger," Chatterjee continues. "But Lacework is helping us track this."

Lacework has also been useful to Chatterjee for its file integrity monitoring (FIM) abilities. "Whenever a file is being changed, whether it's being written or modified, Lacework will log it and highlight it into the dashboard," says Chatterjee. "That's helped us piece together what happened and uncover important changes."

Improved compliance reporting

Since implementing Lacework, the Protegrity team has seen a marked improvement in their ability to address compliance issues. "We've seen a shift in items that were heavily noncompliant before," says Chatterjee. "Now we are on track, thanks to Lacework." Adds Ingram, "Lacework identified major blind spots across our cloud environments, which is leading to Protegrity's successful ISO 27001 certification."

As security experts, Protegrity has an obligation to demonstrate compliance to their customers. "Our customers will ask what we're doing for compliance in our cloud environments, and Lacework helps me with that communication," explains Ingram. "Instead of just showing them a checkbox of what we're doing to satisfy compliance, I can give them a full storyboard."

With an active regulatory environment, Protegrity pays close attention to new regulations and updates to existing standards, and they're confident that their partnership with Lacework puts them in a good position to meet what comes next. For example, recent changes to the ISO 27001:2022 standard call for information security requirements for the use of cloud services, configuration management controls, and anomalous activity monitoring. With coverage from Lacework, Protegrity will be able to prove compliance across the new controls. "Proving compliance with the new ISO 27001:2022 controls will be straightforward with Lacework," says Ingram. "Many of the controls are right in the Lacework wheelhouse, so this will be simple for our team."

> "Our customers will ask what we're doing for compliance in our cloud environments, and Lacework helps me with that communication. Instead of just showing them a checkbox of what we're doing to satisfy compliance, I can give them a full storyboard."
>
> SCOTT INGRAM, DIRECTOR OF INFORMATION SECURITY, PROTEGRITY

Working across teams

Prior to adopting Lacework, Ingram and Chatterjee brought teams across their organization into the proof of concept and demo processes. "I wanted to make sure that all the core teams — development, DevOps, cloud development, IT — knew that Lacework wasn't only for security," says Ingram. "Initially, they thought it was just another tool. Now, these teams are heavily utilizing Lacework in their production environments." Protegrity's security team also used Lacework to mature some of their development, test, and production areas. Says Ingram, "When we would bring findings from the benchmarks to each department, we saw a 10x drop in alerting from our production areas." For a number of teams at Protegrity, Lacework is making a big impact.

> "Whenever we need the Lacework team, they are available, whether that's via chat, in the form of a meeting, or for a quick training."
>
> GOUTAM CHATTERJEE, SENIOR APPLICATION AND CLOUD SECURITY ENGINEER, PROTEGRITY

A productive partnership

By working closely with the Lacework team, Protegrity has been able to take advantage of the product's many offerings. At one point, recalls Ingram, "we brought a challenge to Lacework with how we set up the design of a new technology. Initially, we thought this would be a blocker, and we'd have to wait for development cycles. But the Lacework team jumped in immediately and developed a fix for us on the spot. They did fantastic work."

Lacework also stood out to Protegrity for its maturity and roadmap. When they adopted Lacework in 2020, it was already heavily matured in AWS, Ingram's core area. "With Lacework, there was full transparency about the future pipeline," recalls Ingram. "When I spoke to other vendors, I didn't get that communication, but Lacework gave me a roadmap of where they were going." When the Protegrity team made specific asks of Lacework, says Ingram, "My voice was listened to. Lacework would give me biweekly updates about what was changing in the console, so I was part of the roadmap, receiving full communication." As Lacework continues to mature and add new features, this communication and transparency will stay constant.

Schedule a demo today

PROTEGRITY

Protegrity aspires to protect the world's most sensitive data — whatever it is and wherever it resides at any given moment. Their platform frees businesses from the constraints typically associated with the access and fine-grained protection of sensitive data, so they can have the confidence to create better customer experiences, make intelligent decisions, and fuel innovation. With their core product development based in India and Sweden, plus locations in the United States for sales, HR, and finance teams, Protegrity is a global company.