strongdm Now part of Delinea Ironclad

Ironclad Shrinks Attack Surface And Onboarding Time

Using Google groups Integration

Ironclad is leading the charge to free up legal professionals from administrative work. It focuses on turning contracts into business assets, allowing teams to extract valuable information to drive business decisions. By choosing StrongDM, Ironclad freed up its own professionals to focus on improving its product, rather than manually managing infrastructure and user access.

> "The access control has helped us out the most. And with audit logging, it's very easy for the auditors to see what queries are being run by a particular person at a particular time. That granular level auditing–I can't stress enough how big of a win it is.
>
> Ironclad | **Nate Schlitt**, software engineer

Unified Access Reduces Costs and Improves Compliance

Ironclad struggled with two main issues: managing endpoint access and auditing activity. VPNs were expensive from both a budget and maintenance perspective. They required significant effort to maintain, but didn't provide the evidence auditors required to fulfill SOC 2 compliance requirements. Specifically, VPNs were not sufficient to prove that Ironclad prevented unauthorized access to its databases. As Ironclad evaluated options, they needed a solution that could fulfill SOC 2 requirements and support its entire backend stack, including the DBMS from a recent acquisition.

Granular Auditing Improves Visibility

A few employees at Ironclad used StrongDM at previous companies. They recommended it because it was easy to set up–particularly on the Kubernetes side. Ironclad did its due diligence, and their decision-making team of five made a unanimous choice. They chose StrongDM for its ability to conduct granular auditing and grant temporary access to resources. And they liked that StrongDM integrates with G Suite and allows the team to forward logs to Datadog and set up Slack alerts.

Query logging and SSH replay sessions are some of the most useful features, according to Nate Schlitt, Software Engineer. The team can see what the user typed and the commands executed.

"Just being able to see everybody's queries against the database–that granular level auditing, I can't stress enough how big of a win that was," Schlitt said. "Being able to see every user's query, connection access, and network access is fantastic."

Automated Access Speeds Up Onboarding

The most significant benefit for Ironclad has been the time saved onboarding new users. Ironclad uses Google Groups, and when a user is added to the Google Group, they also get automatic access to resources via StrongDM. The team can drag and drop a new user into a role that matches the Google Group, automatically assigning access. This ensures least privilege permissions are assigned by default for all new hires. Before StrongDM, any new accounts and local provisioning had to be manually configured.

With StrongDM, Ironclad reduced the attack surface in two ways. First, the company no longer distributes database credentials to staff. Instead, staff authenticate using Google. As a result, the underlying credentials can't be compromised because they are never stored locally on staff workstations. Ironclad also restricts access to isolated subnets by leveraging StrongDM's egress-only proxy that ensures traffic only communicates with the proxy. This protects the back end systems from unauthorized access.

Best of all, by reducing its administrative overhead with StrongDM, Ironclad now has more time and energy to help legal professionals streamline their own work.