strongdm
Now part of Delinea

Modernizing Infrastructure Access Across Enterprise Platforms

How enterprise teams modernize infrastructure access to improve visibility, control, and efficiency with StrongDM.

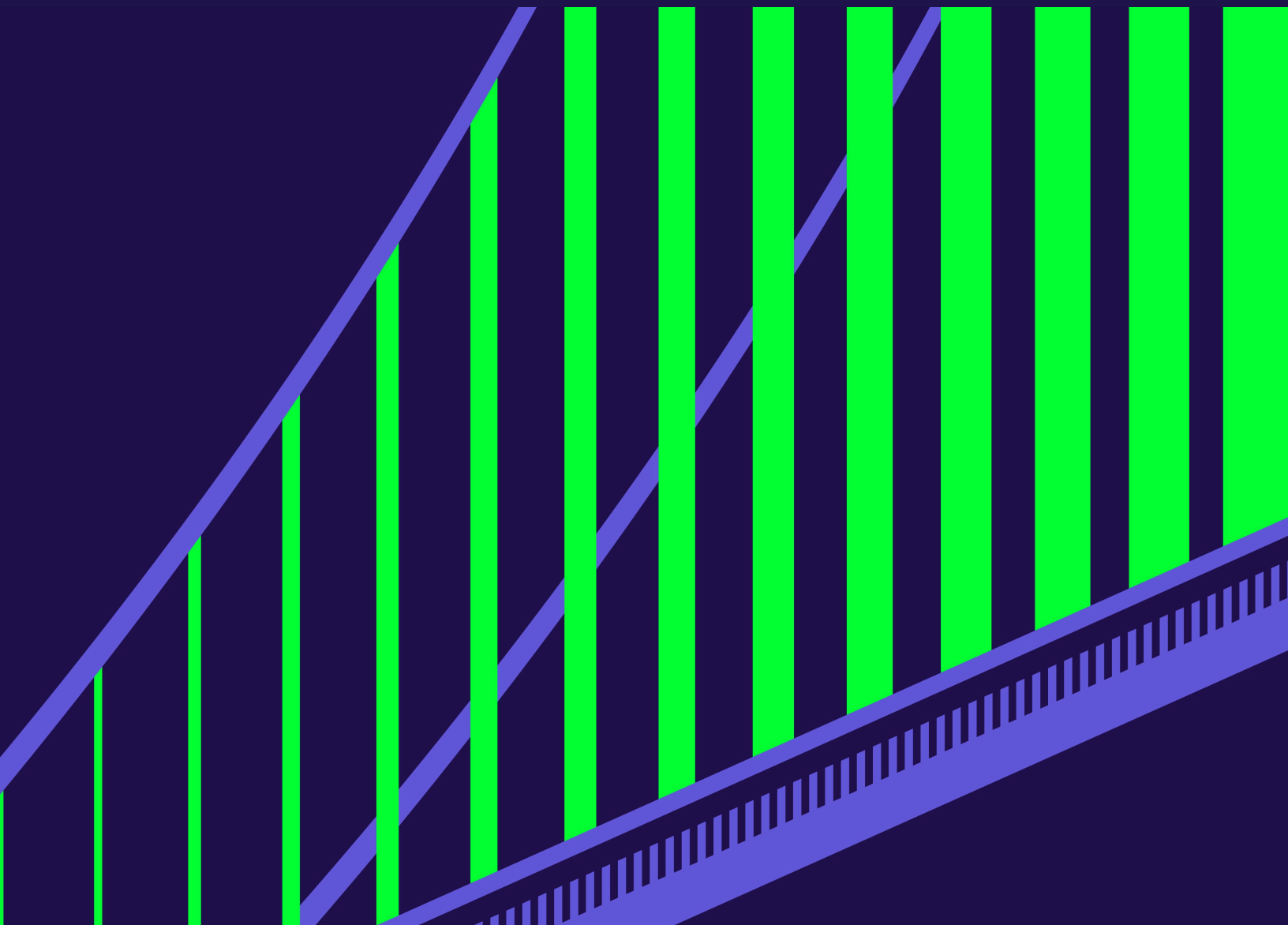


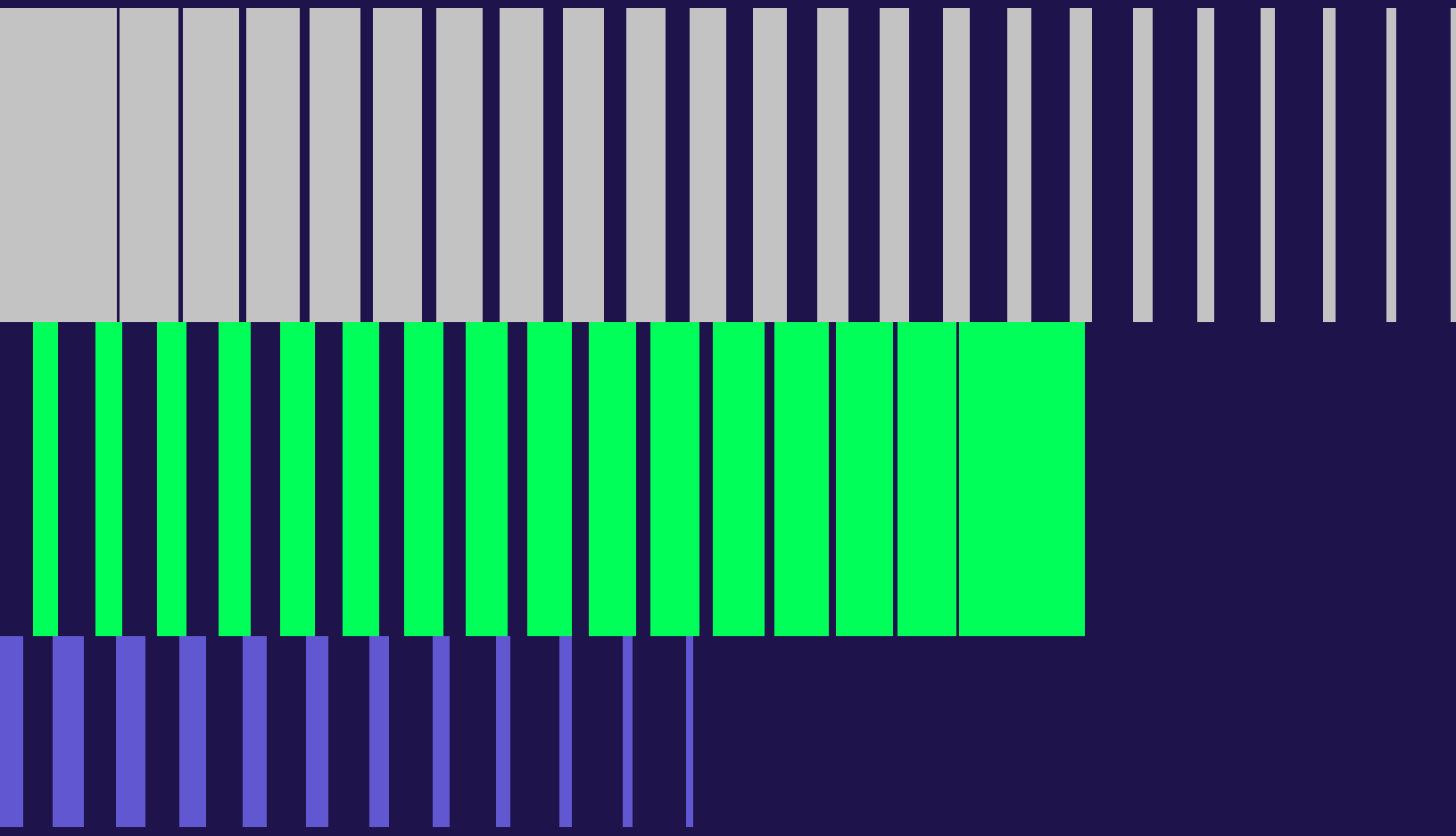
Table of Contents

Infrastructure Access for Data-Driven Platforms

Organizations operating large data platforms must manage access across complex infrastructure environments that include databases, analytics systems, and cloud infrastructure.

As systems scale, maintaining secure access while enabling engineering productivity becomes increasingly difficult.

The companies featured in this guide show how modern teams simplified infrastructure access while improving security visibility and operational control.



01

Benevity Elevates Data Privacy Control and Accelerates DevOps Workflows

Benevity provides corporations with a way to cultivate a culture of purpose, meaning and impact through software that connects their people with the causes they care about—whether it's to donate their time, their money, or just do a simple act of goodness or kindness. To date, Benevity has processed nearly $8 billion in donations and 43 million hours of volunteering time to support 326,000 nonprofits worldwide. The company's solutions also facilitated 530,000 positive actions and awarded 1.2 million grants worth $12 billion. As such, Benevity takes security and compliance seriously to assure its clients'—many of which have large, sophisticated privacy and security protocols of their own—data is safeguarded.

For secure database access for developers, Benevity's site reliability engineering (SRE) team uses StrongDM for enhanced role-based permissions and audit logs on backend systems, providing visibility and due diligence that brings the company and its clients peace of mind.

StrongDM Provides Scalable Role-based Access

The company's technology stack includes Microsoft SQL Server and EC2 in Amazon Web Services (AWS). Before deploying StrongDM, access approval requests for individual user server accounts were provisioned through a custom Ansible script. This would have been fine for just one or two users, but as the company scaled its business they needed to scale their ability to maintain secure workflows and processes at the same time. Additionally, shell access to EC2 required SSH keys, so they needed a solution that would also help streamline and create efficiency in this area.

During the process of migrating to AWS, Benevity wanted to figure out a more scalable approach to managing infrastructure access. The SRE team had three core requirements that any solution must meet:

1. Users must gain faster access
2. Access must be automated and not include a manual access management process
3. The system must uphold industry-leading security standards

"We had some really great demos with StrongDM," says Nina d'Abadie, Director of DevOps at Benevity. "We brought in a few developers to test it out, and it was a really positive experience for them. Our VP was a strong advocate for it and was sold the first time he saw it. Security was appreciative of the auditable access to databases, and we could retire previous ways of access like shared SSH keys."

StrongDM was able to meet Benevity's needs for simplicity and security, and helped streamline how it granted access to users. Furthermore, once Benevity began using StrongDM, the biggest use case quickly became database access.

Devs Gain Self-service Access to Scrubbed, Production-like Data

"We have a really neat use case for StrongDM: Getting developers access to the databases, but in particular, access to scrubbed datasets. We had a team collaboration where they built some cool scrubbing scripts via Lambda that would do a database pullback and scrub it, and this was all tied into StrongDM via Terraform," d'Abadie says. "That meant all of these new databases would be registered into StrongDM as they're pulled back. Now we could easily provide access when spinning up ephemeral databases."

Now, developers can spin up an on-demand database with scrubbed data, but with a production schema. "Developers now have an on-demand, generic dataset that is fully representative of prod—a huge improvement, given that dev environments aren't always representative of production. So now they can do different use cases, test complex scenarios and datasets, and also do performance testing. They spin it up on-demand and have the access they need automatically provisioned without going through additional teams. It's completely self-service," d'Abadie adds.

> "We brought in a few developers to test it out, and it was a really positive experience for them. Our VP was a strong advocate for it and was sold the first time he saw it. Security was appreciative of the auditable access to databases, and we could retire previous ways of access like shared SSH keys."
>
> benevity | Nina d'Abadie
> Director of DevOps

Benevity Saves Time While Boosting Security

With StrongDM, Benevity now automates the internal approval process required to provision database access. It also allows Benevity to leverage role-based access in order to standardize permission levels across teams of developers. StrongDM's audit logs have also proven to be extremely useful to the security team.

"By using StrongDM, not only do we have auditable access to DBs and shell access, but we could retire some of our previous ways of accessing, like shared SSH Keys," says d'Abadie. "For the security team, the compliance aspect and being able to see the audit logs of every single query that was run and everyone that accessed it—that's incredibly valuable," added d'Abadie.

Central Control Plane Improves Visibility

"We have a really neat use case for StrongDM: Getting developers access to the databases, but in particular, access to scrubbed datasets. We had a team collaboration where they built some cool scrubbing scripts via Lambda that would do a database pullback and scrub it, and this was all tied into StrongDM via Terraform," d'Abadie says. "That meant all of these new databases would be registered into StrongDM as they're pulled back. Now we could easily provide access when spinning up ephemeral databases."

Now, developers can spin up an on-demand database with scrubbed data, but with a production schema. "Developers now have an on-demand, generic dataset that is fully representative of prod—a huge improvement, given that dev environments aren't always representative of production. So now they can do different use cases, test complex scenarios and datasets, and also do performance testing. They spin it up on-demand and have the access they need automatically provisioned without going through additional teams. It's completely self-service," d'Abadie adds.

02

Yext Goes Public After Achieving SOC 2 Compliance

Central Control Plane Improves Visibility

Yext powers location data for some of the most recognizable brands. After a dozen years of hard work, the company went public in 2017 with revenue of over one hundred and twenty million dollars.

Achieving SOC 2 compliance represented a key step in the IPO process. Facing tight deadlines and hundreds of mission-critical databases, Yext's infrastructure security team could not afford any delays.

Yext Implements Comprehensive Auditing

With 250+ databases that included multiple database types and versions, Yext faced a difficult and potentially costly challenge to implement the comprehensive auditing necessary to pass SOC 2. Yext estimated it could cost over three million dollars without taking into account labor hours to pull off such a large project.

StrongDM enabled Yext to conveniently log every query and permission change without any infrastructure changes. In three weeks, StrongDM was rolled out to hundreds of staff. The ability to produce query and activity logs across Yext's entire infrastructure provided key capabilities that ensured Yext would always be audit-ready.

StrongDM Reduces Provisioning Time from Hours to Minutes

StrongDM offered more than an audit trail. StrongDM's access management streamlined the work to onboard and offboard technical staff, reducing the time to provision access from 48 hours to 30 minutes. This helped transform how the infrastructure team was perceived by peers at Yext. By eliminating frustrating delays, Yext's Infrastructure team was transformed into a business enabler that could empower teams to work more efficiently and securely.

250+
Databases

$3M+
Annual Savings

47 hours
Faster to onboard

"The effort to achieve SOC 2 compliance without StrongDM would have been a monumental effort, not only in terms of resources, but in terms of cost."

Michael DaSilva
Manager,
Information Security

03

Hearst Simplifies the Deprovisioning Process with StrongDM

HEARST

StrongDM Manages Access without Disrupting Productivity

MediaOS acts as the central hub to manage, monitor, and distribute content for Hearst's 21 magazines, including Elle, Cosmopolitan, and Esquire. MediaOS serves content to 150 million readers a month in a latency-sensitive environment. In under two minutes, the MediaOS platform must analyze content to reveal who is seeing what, identify social visitors, and compare that data to that of similar content.

To deliver that performance, the MediaOS engineering team cannot afford any tooling that impacts productivity negatively.

Efficient Access Means Less Work for DevOps

As a critical part of the Hearst infrastructure, MediaOS is constantly hiring engineers. Because there are so many services, databases, and developers, the onboarding and offboarding process was labor intensive before StrongDM.

Since deploying StrongDM, the process has become much simpler. The DevOps team invites a new hire to the StrongDM platform and assigns a role. The hire inherits all appropriate database permissions. No need to maintain multiple scripts or checklists. That means more efficiency and an easy to access audit trail of every permission change.

StrongDM is Convenient and Secure by Default

Because StrongDM integrates seamlessly with every SQL client, BI tool, and the command line, there's no training required. According to Jim Mortko, VP Engineering, "It's something that you don't even know it's there once it's installed. It just works."

1 Hour
To Deploy

8,000+
Employees

60 sec
Time to Offboard

"You don't even know StrongDM is there. Once it's installed, it just works. It's very simple."

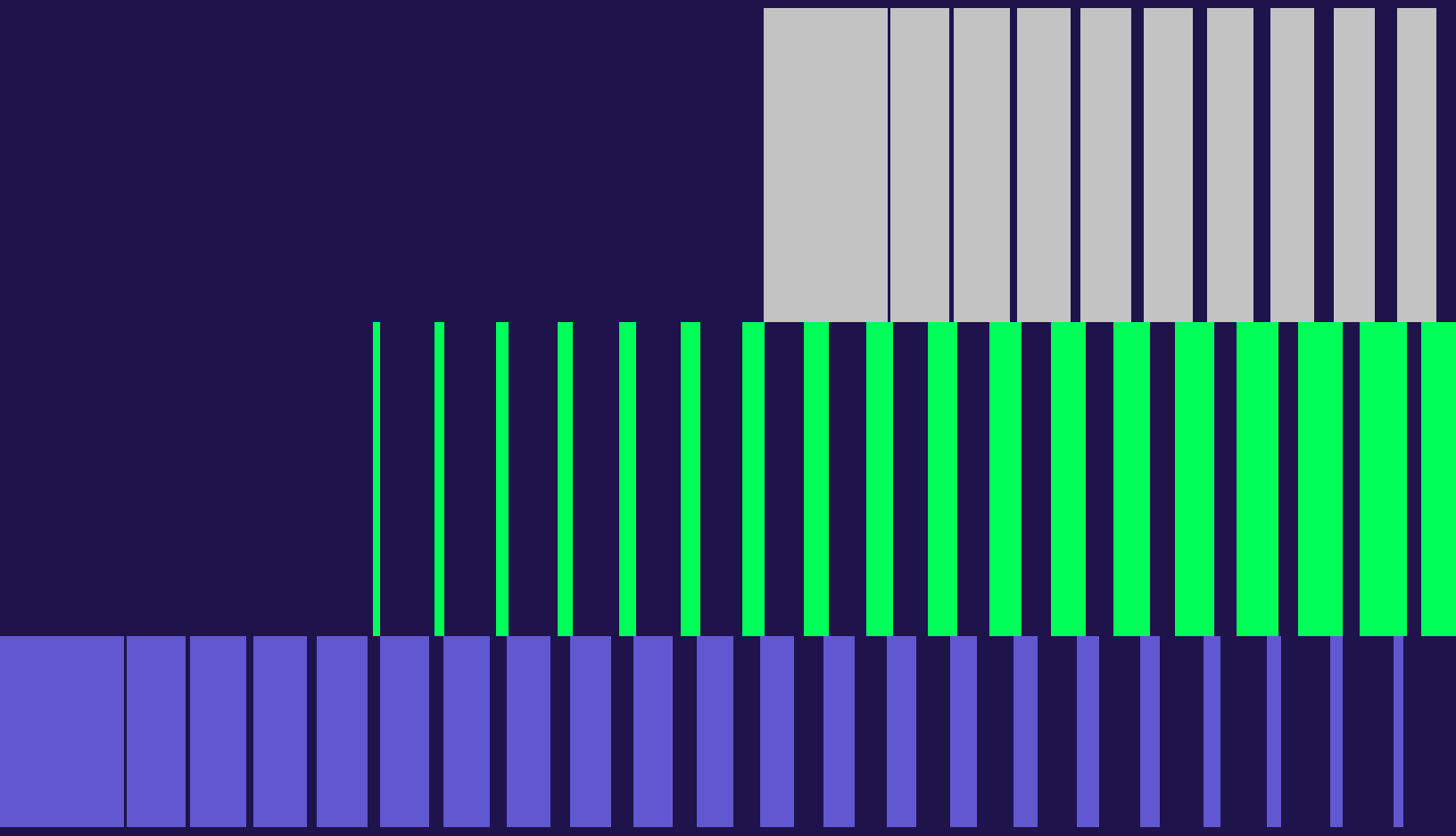
HEARST

Jim Mortko
VP of Engineering

Scaling Infrastructure Access

These organizations demonstrate how modern teams can:

- Scale infrastructure access securely
- Simplify onboarding for engineers
- Improve visibility into infrastructure activity
- Reduce operational complexity across infrastructure systems



strongdm
Now part of Delinea

StrongDM is a Zero Trust access platform that centralizes and simplifies access management for all technical users across every resource in your infrastructure, whether on-premises or in the cloud. By embracing Zero Standing Privileges and implementing Just-in-Time (JIT) access across your full tech stack, StrongDM provides fine-grained, context-based policy enforcement in real time.

Security teams gain complete visibility and control over access and actions with advanced reporting and analytics, helping to identify unused access grants, inactive resources, and over-privileged roles to enhance security and compliance postures. End users enjoy fast, intuitive access to the resources they need when they need them, improving productivity and operational efficiency. Connect with us on LinkedIn, YouTube or head to www.strongdm.com to learn more.