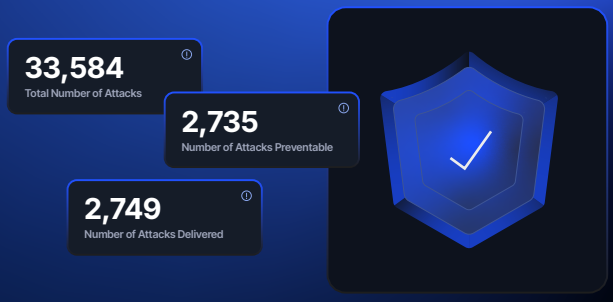
Reach



Case Study | AUTODESK

Maximizing Security Control Utilization at Autodesk

Autodesk is changing how the world is designed and made. Their technology spans architecture, engineering, construction, product design, manufacturing, media and entertainment, empowering innovators everywhere to solve challenges big and small. From greener buildings to smarter products to mesmerizing blockbusters, Autodesk software helps their customers to design and make a better world for all. This spirit of innovation extends to their Trust Organization, who embrace emerging technology to protect both their design platforms and corporate environments against emerging threats.

The Security Control Challenge

Autodesk faced challenges managing their extensive array of security tools, which led to underutilization and inefficiencies. The Trust Organization at Autodesk faced gaps in how users accessed their environments, presenting risks that were difficult to quantify. The Chief Trust Officer flagged these issues, prompting the team to seek a solution that could enable Autodesk to get more from the security tools they already owned.

Solving the Challenge is within Reach

Reach was introduced into Autodesk's environment to address these comprehensive security needs. Unlike other niche solutions that focused on isolated aspects of security, Reach offered a unified platform that covered identity, device, network, and endpoint security holistically. This broad coverage was crucial for Autodesk, which required a product that could integrate seamlessly across various security domains.

The deployment of Reach at Autodesk was notable for its simplicity and speed. Reach required minimal time to integrate into the Autodesk environment. The platform provided actionable insights soon after deployment, facilitating rapid adoption and immediate benefits. Detailed documentation and support from Reach made the process straightforward, allowing Autodesk's InfoSec team to implement comprehensive security changes quickly and effectively.

> "We found value almost immediately once we deployed Reach. It only took a few minutes to integrate the product in the Autodesk environment."
>
> **Ray Winder**
> Director of Information Security at Autodesk

One of the most significant improvements was around customizing security based on workforce risk distribution. The team at Autodesk highlighted a particular instance where Reach identified a subset of users disproportionately attacked relative to the rest of the population. Reach not only flagged these users, but also automated the implementation of tailored conditional access policies to address these risk hotspots. This capability drastically reduced the response time from detection to resolution, enhancing Autodesk's security posture.

Integrating Reach with Autodesk's existing IT systems allowed the security team to automate the creation of detailed tickets and apply security patches or updates directly through the platform, further streamlining their operations. Reach automated many processes that were previously manual, saving significant time and reducing the workload on Autodesk's engineers.

> "We could set up an automation with Reach to populate a ticket with all the relevant details as a way to streamline our workflow."
>
> **Ray Winder**
> Director of Information Security at Autodesk

The Road Ahead

Autodesk has been working with Reach for over a year now, and they are planning to deepen this partnership by exploring further integrations and expanding its capability to cover more areas of their security architecture. The team has even discussed the potential of using Reach for advanced threat hunting activities, leveraging its alignment with the MITRE ATT&CK framework to enhance their proactive security measures.

This ongoing partnership with Reach signifies Autodesk's commitment to maintaining cutting-edge security practices and improving their operational efficiency, ensuring that they remain leaders in both their industry sectors and in cybersecurity.

Get Started with Reach

To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit:

reach.security/try-reach

Reach was founded to help organizations proactively find and fix hidden security blind spots. Traditional approaches surface issues, but stop short of fixing them. This leaves teams exposed, overwhelmed, and under-resourced. We built Reach to close that gap, delivering a platform powered by cybersecurity domain-specific AI models that reveal misconfigurations and underutilized capabilities across your existing security toolset; proactively remediate them; continuously validate that security controls are working as intended; and ensure your defenses stay aligned with your evolving environment and threat landscape.