Reach

Case Study | NUTANIX

Measuring & Improving Security Effectiveness at Nutanix with Automated Security Control Hardening

As a global leader in cloud software with more than 22,000 customers, Nutanix offers a unified platform that seamlessly integrates infrastructure and management to enable smooth operations of data and apps across clouds. Their software-defined architecture adapts to various hardware and cloud options to provide consistent operations and data services across cloud, edge, and core environments.

The information security team at Nutanix took on the challenge of automating security control decisions to address the onslaught of new phishing, malware, and account take over attacks focused on the Nutanix global enterprise. Early efforts at adoption of security automation and orchestration helped the team respond to events, but it didn't address prevention. Proactively automating security control hardening of the security tools Nutanix had in place was always a priority, but execution was difficult with employees prioritized on other tasks. Nutanix sought a vendor that could partner to extend automation beyond response and include proactive prevention.

sales@reach.security | reach.security

Using Data to Automate Control Hardening & Attack Prevention

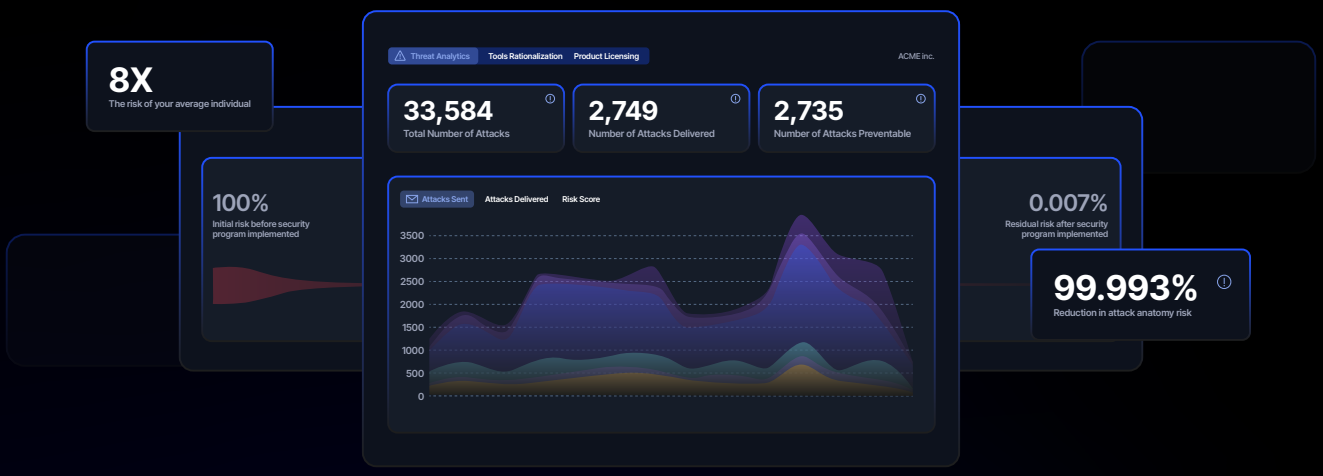
Most organizations lack visibility into the data required to measure and manage the capabilities of their growing security stack. Early in the organization's evolution, the Nutanix information security team continued to find themselves in this predicament and knew there had to be a better way to keep up with the latest threats and automate this process.

In contrast to best practice assessments or quarterly vendor briefings, Reach takes a nuanced approach by translating Nutanix specific threats into preventative controls across the stack. Reach's modeling of threat events, sandbox forensics, user privileges, and product configurations paints a real-time picture of what is breaking through existing defenses and being delivered to end users. The information security team at Nutanix has gained insight into what was getting through, which users were targets, and what was preventable using the products in place currently.

> "They were very early adopters of security orchestration and response automation. They built a lot of automation around taking an event from the SIEM, enriching it, and taking action. As they've continued to mature, they've leveraged Reach to automate the knowledge and tuning of their whole security stack using their data."
>
> **Zach Marks**
> Solution Architect

Hiring for Security Expertise Instead of Security Product Expertise

Demand for security talent has never been greater as the threat landscape continues to evolve.



Reach makes hardening decisions simple by delivering uniform configurations as code that are translated from live attack data in Nutanix's environment. With detailed deployment guides and change control tickets pre-packaged for IT, Nutanix's security teams can now focus on security outcomes without the need to know, monitor, and manually measure product performance.

At the same time, this helps the team to focus on hiring pure security talent instead of hiring siloed security product experts.

> "Hiring specialists was common in the past. Today, more companies are not hiring a specific specialist in a tool because there are so many tools with so many features out there. They'd rather have someone who really understands security and how all the systems work fundamentally."

Measuring, Improving & Reporting on Product Effectiveness

After countless meetings, health checks, and quarterly check-ins from disparate vendors, the team at Nutanix knew there had to be a better way to maximize value out of their security investments.

> They were aware of a lot of blindspots. Some tools have so many features that you have to know they exist and then ask the vendor to turn them on. Looking at all the bells and whistles was not enough. The reality is, vendors release a lot more than can fit in one slide, and security teams often don't have anyone dedicated to reading the release notes for every new version or monitoring every release of every product that they use which leads to blindspots. Reach has really shined a light on those blindspots for client and told them things they didn't know the products could do. Some have even said that Reach is like a cheat code for security products.

Reach's approach to measuring product effectiveness consists of the following:

1
Pull product configurations using cloud APIs at initial setup

2
Model threat data to controls

3
Provide new configuration recommendations

4
Automatically track configuration changes and improvements over time

With Reach, the Nutanix security team can quantify cross-stack metrics over time, such as attacks delivered and attacks preventable using existing tools. The result is increased collaboration with peers in IT Operations and a clearer demonstration to leadership that they are capable of maximizing dollars spent.

sales@reach.security | **reach.security**

Nutanix & Reach: The Story Continues

> In a perfect world, security teams maximize every dollar spent. It doesn't make sense to buy an email security tool, get 70% of the features, and buy a second layer because the first is missing things. There's a certain amount of defense in depth and layering that makes sense, and a certain amount that happens because of suboptimal configurations. To the extent teams can minimize that, they can really optimize the security spend.

In the first month with Reach, Nutanix had measured and deployed new capabilities in a way that fit their organization best. The team will continue to automate security control hardening decisions with Reach to maximize the output of Nutanix's security investments.

> Reach has given Nutanix prescriptive guidance on where they can improve in their existing toolsets. It's 100% tailored to them, and the things that are recommended are done based on the current state of their environment. It's not theoretical, it's practical.

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.