



Building Resilience and Zero Trust at Monolithic Power Systems

About Monolithic Power Systems

Monolithic Power Systems (MPS) is a leading provider of high-performance, semiconductor-based power solutions. With a reputation for innovation in data center communications and video acceleration, MPS supports thousands of global employees across 15 offices. Headquartered in Kirkland, WA, the company has seen rapid business expansion and increasing operational complexity.

The Security Challenge

When Huy Ly joined MPS, the company had just experienced a cyberattack. What started as an effort to stabilize a compromised environment quickly turned into a broader initiative to build a modern, resilient security program from the ground up.

With a background in infrastructure and development at companies like Oracle, Intuit, and Ancestry, Huy brought a unique perspective: one shaped by high-availability environments and service-oriented IT. But securing a global, fast-moving company with limited resources required more than vision, it required efficiency.

From onboarding and offboarding to safeguarding intellectual property and preventing ransomware, the security team needed a way to operate at scale without increasing headcount.

“

We're a 4,000-person company with less than 10 security engineers. Almost everything is automated from onboarding to laptop provisioning.

Huy Ly
Head of Global IT Security/Infrastructure



”

Solving the Challenge with Reach

MPS partnered with Reach to enhance the security team's visibility, efficiency, and control. Initially drawn to Reach's Zero Trust and remediation-focused approach, Huy quickly realized the platform could help monitor and optimize tool configurations across email, EDR, and network security without adding more manual work.

“

Reach became like a virtual assistant. It tells me what's going on in the environment, what needs to change, and what's getting missed.

”

Legacy methods of analyzing configurations like hiring consultants or relying on periodic audits simply couldn't keep up with the dynamic pace of change. With Reach, MPS could continuously baseline, detect misconfigurations, and validate changes without disrupting operations.



Email Security Hygiene:

Reach helped identify shadow rules and dangerous patterns in email usage, such as compressed file transfers used for phishing. Within 3 months, MPS significantly reduced risk and improved detection.

EDR Noise Reduction:

Reach helped the team clean up noisy configurations, making alerting and monitoring more actionable.

Zero Trust Acceleration:

By showing how tools were configured, what features were enabled, and what usage patterns looked like across users, Reach enabled the team to make faster, more confident policy decisions.

“

We validated everything in small groups, tested for breakage, then rolled it out globally. We found a lot of ‘aha’ moments that we wouldn’t have seen otherwise.

”

Why Reach

For Huy, Reach wasn’t just about risk detection, it was about building a security operating model that could scale globally without compromising on vision.

“

Security talent is limited. That’s why I partner with innovators; people willing to build with me. Reach fit that mindset perfectly.

”

By combining infrastructure-first thinking with Reach’s automated platform, MPS transformed how security got done by focusing on resiliency, Zero Trust principles, and sustainable operations.

Looking Ahead

Huy sees Reach as a strategic partner in evolving areas like AI, ransomware defense, and identity protection. With a strong foundation in place, the focus now turns to expanding coverage, closing gaps, and staying ahead of fast-moving threats.

“

What keeps me up at night? The sophistication of attackers and how fast they move. With Reach, we’re not just keeping up, we’re getting ahead.

”

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