

Restoring Cyber Resilience for a Manufacturing Supply Chain Business

Without Adding
Operational Burden

Restoring Cyber Resilience for a Manufacturing Supply Chain Business



Without Adding Operational Burden

A manufacturing supply chain organization needed to strengthen cybersecurity after experiencing security incidents, without diverting technical leadership away from core business operations. By implementing a unified, fully managed cybersecurity platform and coordinating resources across the organization's IT service provider ecosystem, Simple Security restored resilience, reduced operational burden, and allowed leadership to restore focus on manufacturing delivery.

At-a-Glance Summary (Executive Snapshot)

Industry

Manufacturing / Supply Chain

Operation Type

Founder-led manufacturing business

Technology Environment

Hybrid infrastructure (on-premise and cloud)

Primary Challenge:

The organization experienced security events while managing digital transformation and cloud migration, resulting in a complex hybrid infrastructure. The need to implement an effective cybersecurity program was distracting leadership from core business priorities.

Solution Delivered:

Simple Security implemented a fully managed cybersecurity platform designed to integrate with existing MSP and infrastructure providers, while assuming ownership of the transition and consolidation from legacy tooling, security operations processes, and cross-functional vendor coordination.

Key Outcomes:

- ✓ Security responsibility shifted away from operational leadership
- ✓ Reduced friction between cybersecurity and IT service providers
- ✓ Improved resilience following security incidents
- ✓ Reduced licensing and infrastructure costs through stack consolidation
- ✓ Technical leadership freed to focus on supporting business



Customer Context (The Before State)

The organization is a manufacturing supply chain company led by highly technical founders who built much of the company's infrastructure internally.

As the business grew, leadership found themselves balancing multiple priorities including maintaining infrastructure, delivering products, supporting operations, and responding to security incidents.

The company had also undertaken a digital transformation initiative, moving many workloads from on-premise infrastructure to cloud environments while still maintaining several critical systems locally, resulting in a hybrid environment.

The Challenge (The Real Problem)

Following security incidents, the organization faced several challenges:

- Hybrid infrastructure spanning cloud and on-premise systems
- Fragmented security controls across multiple technology providers
- Limited internal cybersecurity resources
- Leadership pulled into incident response outside their core expertise

The company needed a cybersecurity partner that could integrate into their ecosystem while removing operational burden.

Why Change (The Trigger)

The organization engaged a legal and incident response advisory partner following security incidents.

After the immediate incident response phase was addressed, the focus shifted to building long-term cybersecurity resilience and hardening the environment to prevent future incidents.



The Simple Security® Approach

Simple Security implemented a lean cybersecurity platform designed to integrate with the organization's existing MSP and infrastructure providers.

Instead of replacing those relationships, Simple Security collaborated with existing partners to ingest telemetry and monitor the environment holistically.

A key differentiator was Simple Security assuming ownership of cybersecurity operations, shifting internal stakeholders from being responsible for security to being informed participants.



Implementation

Implementation focused on integrating cybersecurity controls across the hybrid environment while maintaining alignment with existing IT service providers.

Simple Security worked directly with infrastructure vendors, IT MSPs, and advisory partners to coordinate protection across both cloud and on-premise infrastructure without disrupting operational workflows.

Results

The engagement delivered improvements across both cybersecurity resilience and operational efficiency.

Key Outcomes:

- ✓ Fully managed security program by Simple Security
- ✓ Reduced operational burden on internal technical leadership
- ✓ Improved collaboration across MSP and infrastructure partners
- ✓ Reduced licensing and tooling costs through consolidation
- ✓ Greater resilience against future security incidents

Why It Matters

For fast-moving technical organizations, cybersecurity can become a major operational distraction.

By transferring ownership of security program delivery to Simple Security, the organization maintained resilience while allowing leadership to focus on manufacturing and business growth.

Who This Is For

- Manufacturing and supply chain companies
- Founder-led or engineer-led technical organizations
- Businesses operating hybrid cloud and on-premise environments
- Organizations managing multiple MSP or IT providers
- Companies seeking to reduce operational cybersecurity burden

“Our team needed to focus on building and delivering products for our clients, not managing cybersecurity operations. Simple Security stepped in and took ownership so we could focus on the business.”



Transforming Security, Simplified



If your organization is dealing with security issues, infrastructure complexity, and limited internal security resources, Simple Security can help minimize business impact from organizational change. We deliver a fully managed cybersecurity platform that integrates with, and consolidates your existing IT ecosystem, all while reducing operational burden and improving resilience.

Book a conversation to learn how we simplify cybersecurity.





Protecting what matters
shouldn't be complicated.