simple security®

From Fragile to Enabled:

Turning a SaaS Company's Fragmented Security into a Resilient Program

From Fragile to Enabled:

Turning a SaaS Company's Fragmented Security into a Resilient Program

A rapidly growing SaaS application provider operating in highly regulated markets was struggling with infrastructure sprawl, limited visibility, and unresolved vulnerabilities. By implementing a unified security platform and fully managed delivery model, Simple Security solved the organization's pain-points, transforming their security approach from a fragmented operational burden into a measurable and governed cybersecurity program.

At-a-Glance Summary (Executive Snapshot)

Industry

SaaS Application Development

Company Size

~500 employees

Operating Model

Global customer base across multiple regulated industries

Primary Challenge:

Rapid growth created significant infrastructure sprawl, limited asset visibility, fragmented identity management, and unresolved customer-facing vulnerabilities across the organization's environment.

Solution Delivered:

Simple Security implemented a unified, fully managed cybersecurity platform providing asset visibility, identity governance, vulnerability management, and continuous security posture improvements.

Key Outcomes:

- ✓ 91% reduction in false-positive vulnerability alerts
- ✓ Complete observability of assets and identities across environment silos
- ✓ Reduced operational complexity and tooling overhead
- ✓ Security transformed into a trust center for customers and regulators

Customer Context (The Before State)

The organization is a global SaaS application developer delivering highly visible compliance-focused software to customers across regulated industries.

With approximately 500 employees and customers operating in multiple regions, their application suite plays a critical role in ensuring supply-chain resilience for its clients.

Over several years of rapid growth, the company had expanded its infrastructure significantly across cloud environments, development platforms, and third-party integrations.

While application development continued to scale successfully, the supporting infrastructure and security controls had not evolved at the same pace. This created technology silos, increasing complexity and uncertainty across the environment.

The Challenge (The Real Problem)

Rapid growth had resulted in technical debt and infrastructure sprawl, leaving the organization with limited visibility of assets, identities, and vulnerabilities across its environment.

The organization faced several core problems:

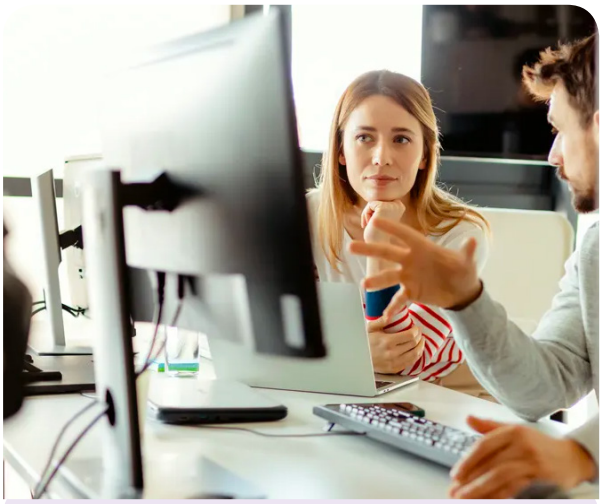
- Lack of reliable asset inventory across cloud, servers, and endpoints
- Fragmented identity management across employees, contractors, and customers
- Vulnerabilities being identified but not always resolved
- Security teams overwhelmed by alert noise
- Limited internal resources to manage multiple security tools and remediate findings

As a result, the company struggled to gain a clear picture of its actual security posture.

Why Change (The Trigger)

External advisory services conducted a review of the organization's security posture and identified gaps in foundational security controls and governance structures.

Combined with previous security events, leadership recognized that the organization had entered a high-risk state driven by complexity and lack of visibility.



The Simple Security® Approach

Simple Security was engaged to deliver a unified cybersecurity program aligned to the organization's business objectives.

Rather than deploying multiple disconnected security tools, Simple Security implemented a fully managed security platform covering endpoint protection, identity governance, vulnerability management, security posture monitoring, and governance reporting.

A key factor in the decision was Simple Security's predictable user-based pricing model, allowing the organization to reduce technology licensing complexity while aligning security costs with employee growth.

Implementation

The implementation followed Simple Security's structured delivery approach, driving measurable progress across a 30-60-90 day project timeline.

Key activities included:

- Mapping all assets across cloud, endpoints, and infrastructure
- Identifying and linking all identities to assets and access points
- Implementing vulnerability and attack surface monitoring across both infrastructure, and codebase
- Hardening endpoints and authentication mechanisms
- Introducing employee security training, testing, and posture scoring

Results

The engagement delivered measurable improvements across security observability, operational efficiency, and risk reduction.

Key Outcomes:

- ✓ 91% reduction in false-positive vulnerability alerts
- ✓ Complete asset observability across infrastructure and endpoints
- ✓ Improved identity governance across employees and connected third-parties
- ✓ Reduced security tooling complexity and operational overhead
- ✓ Improved ability to prioritize and resolve genuine vulnerabilities

Why It Matters

Security moved from being viewed as a burdensome operational risk and cost-center, to becoming a strategic business enabler.

The organization can now demonstrate to customers and regulators that its application suite is protected by a structured and measurable cybersecurity program.

Who This Is For

- SaaS companies with 100–3,000 employees
- Organizations experiencing rapid infrastructure growth
- Businesses operating in regulated industries
- Companies struggling with tool sprawl and alert fatigue
- Teams with limited internal IT and security resources

"What we needed wasn't another tool - it was visibility and turning that into action on the issues in our environment. Simple Security helped us move from uncertainty to observability and control"

Transforming Security, Simplified

If your organization is struggling with infrastructure sprawl, limited security visibility, vulnerability noise, or security tool complexity, Simple Security can help simplify your cybersecurity program.

Book a conversation to see how we move organizations from uncertainty to observability through a measurable, fully-managed cybersecurity program.

simple security®

Protecting what matters shouldn't be complicated.