

Delivering Healthcare Cyber Resilience

Without Disrupting
Patient Care



Delivering Healthcare Cyber Resiliance

Without Disrupting Patient Care



A multi-facility healthcare provider needed to strengthen cybersecurity and regulatory compliance while ensuring that patient care services remained uninterrupted. By implementing a fully managed, compliance-aligned cybersecurity platform, Simple Security helped the organization improve resilience, meet regulatory expectations, and protect patient data, without disrupting clinical operations and duty of care.

At-a-Glance Summary (Executive Snapshot)

Industry

Healthcare Provider

Organization Size

Multi-facility healthcare provider with hundreds of direct patients under active care and over five thousand across daycare programs

Regulatory Environment

HIPAA compliance and duty of care obligations

Primary Challenge:

The organization needed to improve cybersecurity resilience and regulatory compliance without interfering with the delivery of patient care services or increasing operational complexity.

Solution Delivered:

Simple Security implemented a fully managed cybersecurity platform aligned with the NIST Cybersecurity Framework, enabling HIPAA-aligned technical safeguards while providing predictable per-user pricing and white-glove deployment.

Key Outcomes:

- ✓ Full endpoint and system coverage implemented in one week
- ✓ HIPAA-aligned foundational controls mapped to the NIST framework
- ✓ Improved resilience against cyber attacks targeting healthcare
- ✓ Minimal operational disruption for care providers
- ✓ Scalable security model aligned to workforce growth



Customer Context (The Before State)

The organization is a healthcare provider delivering critical care services across more than 20 facilities and mobile in-home care.

Their primary responsibility is ensuring uninterrupted delivery of care to patients. Any disruption to systems, infrastructure, or operational services could directly impact patient well-being.

Because of this mission, the organization historically focused the majority of its investment and operational attention on patient care delivery rather than technology modernization.

While some internal technical expertise existed, many staff members responsible for technology were also performing other roles within the organization. Cybersecurity governance had not yet been formally established.

The Challenge (The Real Problem)

Healthcare organizations are frequent targets of cyber attacks due to the high value of patient data and the operational impact of service disruption.

The organization faced several structural challenges:

- No dedicated cybersecurity leadership
- Limited internal IT resources and technical depth
- Multiple facilities and mobile care staff
- Devices and systems deployed across multiple locations with limited interconnectivity
- Increasing regulatory compliance and investor expectations

Security controls must safeguard and minimize access to patient data, while avoiding disruption to clinical workflows.

Why Change (The Trigger)

The organization engaged a compliance and governance partner to ensure ongoing alignment with regulatory standards.

During this engagement, the compliance provider identified gaps in foundational cybersecurity controls required to support regulatory obligations such as HIPAA and cyber-hygiene best practice.

Leadership needed a solution that could strengthen cybersecurity resilience without requiring significant internal technical resources or cost implications.



The Simple Security® Approach

Simple Security was selected because its platform aligns with the NIST Cybersecurity Framework, meeting the necessary technical safeguards needed for HIPAA.

The white-glove delivery model ensured that both cybersecurity technology and also foundational IT could be implemented and managed without placing additional demands on internal teams.

Predictable per-user pricing allowed security costs to scale naturally alongside the number of care providers supporting patients.



Implementation

The implementation required rapid deployment to meet board and regulatory reporting expectations.

Simple Security worked closely with the organization and its compliance partner to deliver coverage across all facilities.

Within one week, the organization achieved full endpoint and system security coverage across its environment.

Results

The engagement delivered measurable improvements in cybersecurity resilience and operational confidence.

Key Outcomes:

- ✓ Full endpoint and system coverage implemented in one week
- ✓ Alignment with HIPAA technical safeguards through NIST framework mapping
- ✓ Improved protection of patient data and clinical systems
- ✓ Reduced operational risk from cyber attacks
- ✓ Security implemented without disrupting patient care workflows
- ✓ Predictable security costs aligned to workforce growth
- ✓ Regular board-level reporting and metrics that demonstrate posture improvement and ROI

Why It Matters

For healthcare providers, cybersecurity is not just about protecting data - it is about protecting the continuity of care.

The organization ensured patient services remain protected from cyber disruption while maintaining compliance with regulatory expectations.

Who This Is For

- Healthcare providers and care networks
- Organizations operating under HIPAA or healthcare compliance requirements
- Multi-facility service providers with mobile workforces
- Teams with limited internal IT or cybersecurity resources
- Organizations needing security that does not disrupt operational delivery

“Patient care always comes first. What we needed was security that protects our systems without interfering with how we deliver care. Simple Security made that possible.”



Transforming Security, Simplified



If your organization must balance cybersecurity, compliance, and uninterrupted service delivery, Simple Security can help. We provide a fully managed cybersecurity platform aligned to regulatory frameworks, delivered in a way that reduces complexity and supports operational resilience.

Book a conversation to learn how we simplify cybersecurity for mission-critical organizations.





Protecting what matters
shouldn't be complicated.