ARMOR PROTECTS YOUR HEALTHCARE DATA IN THE CLOUD

Securing healthcare networks is becoming more difficult. The number of applications and devices that connect to healthcare IT systems increases daily. Artificial intelligence (AI), the internet of health things (IoHT), and real-time health system (RTHS) solutions open new avenues for threat actors. This leaves healthcare IT departments to close the gap, while also managing a list of responsibilities:

- Protecting client data
- Ensuring IT infrastructure is stabilized
- Guiding internal data security policies
- Educating personnel on how to prevent breaches, etc.

In addition, they must remain compliant with the regulations mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

SIMPLIFY CLOUD SECURITY AND COMPLIANCE

Armor delivers managed security services to protect your cloud—private, public, or hybrid—and on-premise IT environments. Respond to cyberthreats in real-time at a fraction of the cost of traditional solutions. Our security controls are mapped to compliance mandates such as PCI DSS, HIPAA/HITRUST, and GDPR, providing security and compliance benefits to reduce regulatory scope, simplifying the auditing process, and lowering management costs.

Securing your company and getting complete visibility across your IT environment shouldn't be so hard. Armor provides protection and audit-ready compliance in minutes, unifying visibility into and control over your entire IT environment.

For a decade, we have provided 24/7/365 security and on-demand support to our clients.

Armor Anywhere—Protect your data across cloud—private, public, and hybrid—and on-premise IT environments with our security-as-a-service (SECaaS) solution.

Armor Complete—Simplify your cybersecurity with our secure hosting service.

ARMOR

BUILT FOR SECURITY, ARMOR SOLUTIONS GO BEYOND COMPLIANCE

Armor clients inherit HITRUST CSF controls by securing their data and applications with our certified solutions. We make HIPAA compliance simple:

- **HITRUST CSF-certified solutions:** Armor is certified against CSF from the Health Information Trust Alliance (HITRUST).
- **Inherited compliance controls:** Our managed solutions were built to address the risk-based nature of HIPAA compliance and pass their compliant status to customer data.
- **HIPAA compliance support:** Our SOC teams provide 24/7/365 support to help you overcome any compliance challenge.
- **Security-driven compliance:** We built our systems to maximize security. Compliance was an outcome, not a goal.

TRUSTED BY HITRUST

Many healthcare organizations require business partners to be HITRUST CSF certified. The HITRUST CSF standardizes security guidelines for ePHI data, keeping it compliant and safe.

Not only are we HITRUST certified—HITRUST is our client. Choose the security provider HITRUST trusts to protect its data.

> The company has built its infrastructure specifically for security. It's extremely well suited for our client data. It's HIPAA-compliant and has helped us streamline the scope of our own internal audits.
>
> — HITRUST

Focus on patient outcomes and innovation while Armor focuses on:

- Protecting EMR, ePHI, and other sensitive data where it's stored
- Simplifying compliance for HIPAA/HITRUST
- Enabling security for internet of things (IoT) devices

Security priorities in healthcare:

- Create internal policies to help staff understand the importance of security and the role each employee plays
- Keep up with security updates and patches to remain current with evolving cyberthreats
- Scan your attack surface and identify vulnerabilities
- Prioritize security efforts; implement effective counter-measures to mitigate the risks

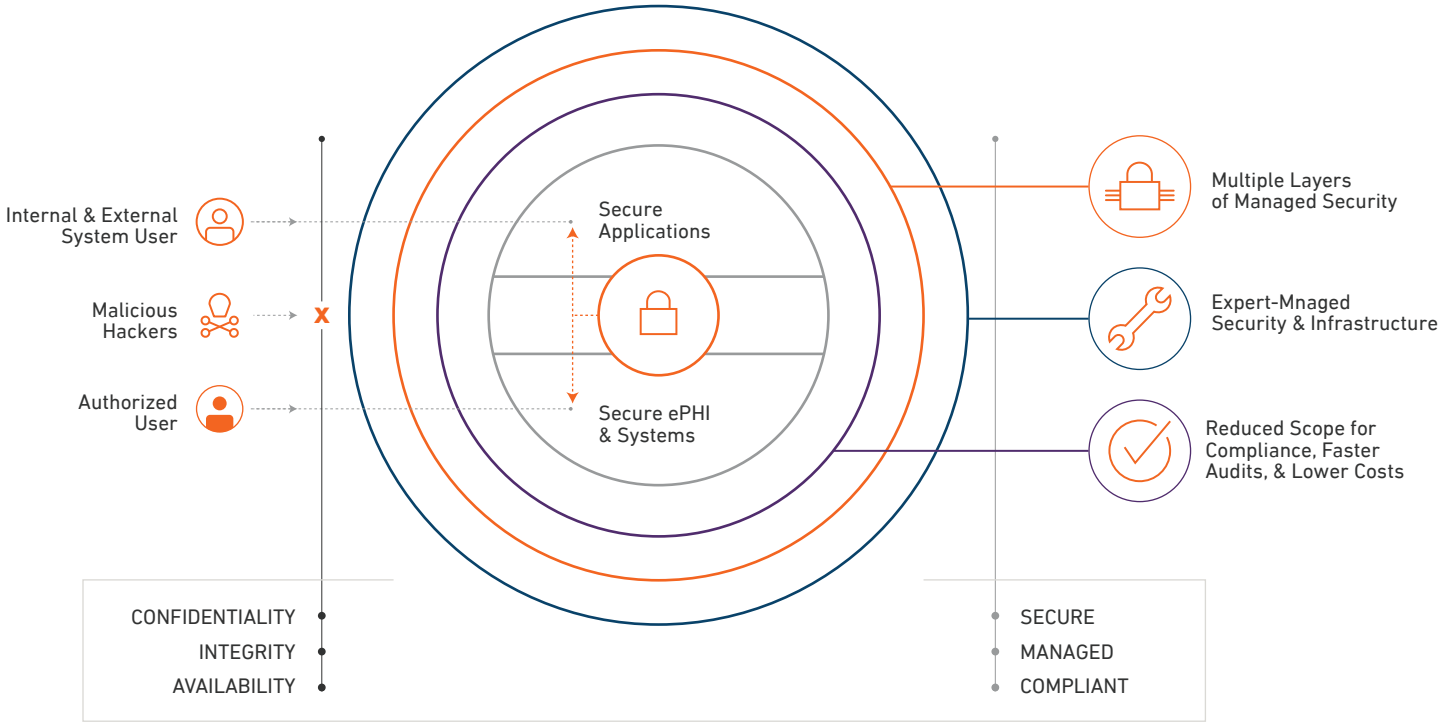
ARMOR

WHAT IS THE HITRUST CSF?

HITRUST established the Common Security Framework (CSF) to help simplify industry guidelines for hospitals, healthcare organizations, insurance firms, patient care, providers, and respective IT companies.

The CSF harmonizes the requirements of existing standards and regulations—including federal (e.g., HIPAA, HITECH), third party (e.g., PCI, COBIT), and government (e.g., NIST, FTC)—to provide organizations with the needed structure, detail, and clarity for information protection and risk management.

CERTIFICATIONS FOR CORPORATE RESPONSIBILITY



SECURITY CONTROLS

- Malware Protection
- Data Encryption
- Patch & File Integrity Monitoring
- Intrusion Detection

COMPLIANCE BENEFITS

- Armor CISO Consultation
- On-Staff HIPAA Analysts
- Audit Preparation
- HITRUST Partnership

