SOLUTION IN ACTION

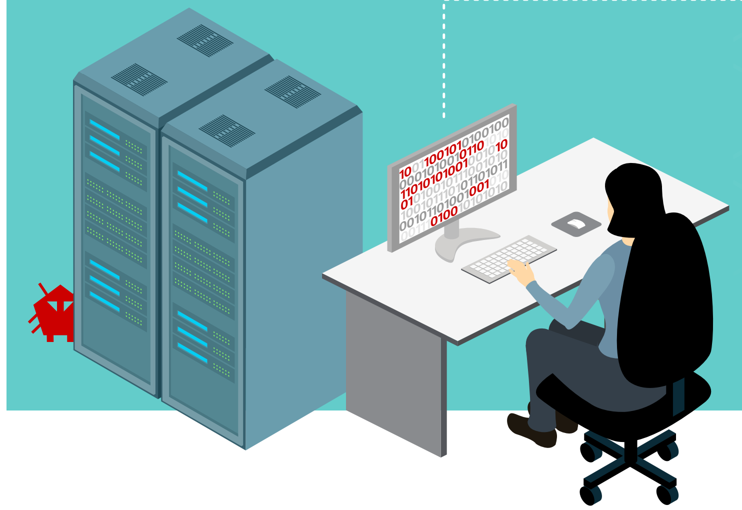
Securing Patient Data: Services Designed to Manage Risk

▸ **Hospitals can leverage services for a risk-based approach to security** that ensures regulatory compliance and patient data protection. Here's how one hospital implemented a multipronged approach to its security review:

BASIC SECURITY PARAMETERS

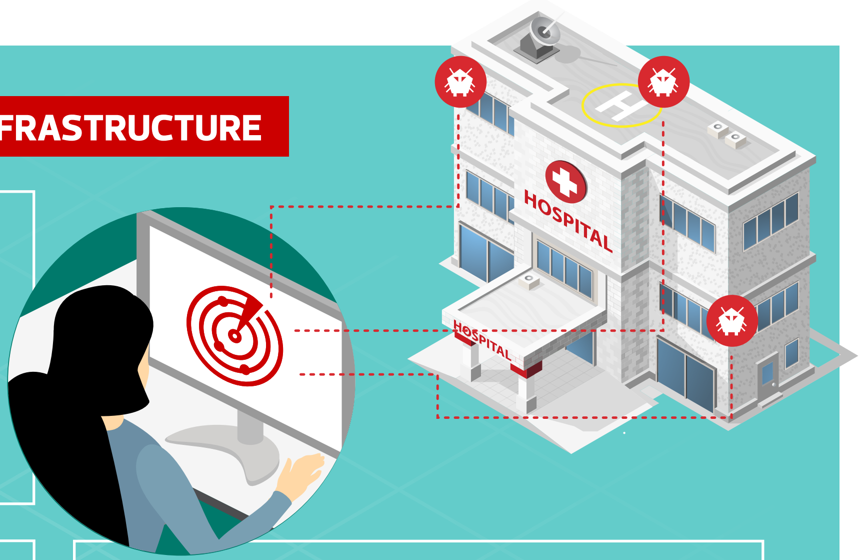
With ransomware, phishing, malicious emails, hackers and other security threats on the rise, a hospital realizes it is facing an expanded threat landscape and must defend its data, devices and networks.

To improve its **security posture**, the hospital ensures it has the **basic protections** in place – **firewalls, secure endpoints, encryption and two-factor authentication**. It then reaches out to a trusted technology partner to take advantage of **comprehensive assessments** and **services** that can build on this secure foundation.



ADVANCED SECURITY INFRASTRUCTURE

Their trusted partner begins by focusing on information security and conducts a **vulnerability assessment** of existing IT systems to **identify where existing security weaknesses lie**, followed by a report with specific recommendations for addressing and prioritizing each gap.



Next, **penetration testing** is conducted to identify **hard-to-detect vulnerabilities** that can't be discovered without painstaking manual analysis, including **poor passwords, default passwords, internet weaknesses, wireless encryption and filtering, and chain-of-trust issues** that let hackers breach the network and attack other systems.

To further test the hospital's security, **social engineering** is used to create custom phishing scams, telephone-based attacks and even physical intrusion scenarios like a dropped thumb drive in a parking lot, all to **determine the viability of existing security protocols**. Finally, **a data loss prevention (DLP) assessment** is used to evaluate how prone the hospital is to having patient data stolen, or suffering from data loss of any kind.

PROTECTION AND COMPLIANCE

Because of this multifaceted security review, the hospital can determine where its **protections are strong**, where there's **room for improvement** and where **fixes** must be immediately implemented. This ultimately helps ensure **compliance with HIPAA and HITECH regulations**, while providing **multilayered security across gateways, networks, servers, clients and applications** – all to better protect patient data.

BEHIND THE SCENES

A risk-based security approach involves a comprehensive assessment that evaluates all possible risks and assigns each a "risk score" based on the chances it will happen, along with its potential impact on the healthcare organization. This allows providers to prioritize and focus on the most immediate and/or damaging threats first.

Learn more about comprehensive security services that can safeguard networks, data and devices across your healthcare enterprise. Request a free security scan at **CDW.com/threatcheck** or contact your CDW Healthcare account manager at **800.500.4239**.

COFENSE

SOPHOS

tigerconnect

TREND MICRO

CDW PEOPLE WHO GET IT
HEALTHCARE