**Microsoft Security**

Protect EHR data and mitigate compliance risk

Native security and compliance capabilities in the Microsoft cloud are suited for the future of EHR and evolution of cybersecurity threats. With the Microsoft integrated suite of products, you can strengthen cloud security, identity and access management, and mitigate insider risk through a single platform approach, so you're more informed of the greater threat landscape.

66% of healthcare organizations were hit by ransomware in 2021[1]

Ransomware continues to rise in healthcare, yet threats to health records extend beyond injected malware. HIPAA violations and data exfiltration can occur through identity or credential theft and insider risk cases. Microsoft Security's holistic solution provides the ability to protect, detect and respond to the array of threats facing these sensitive data estates.
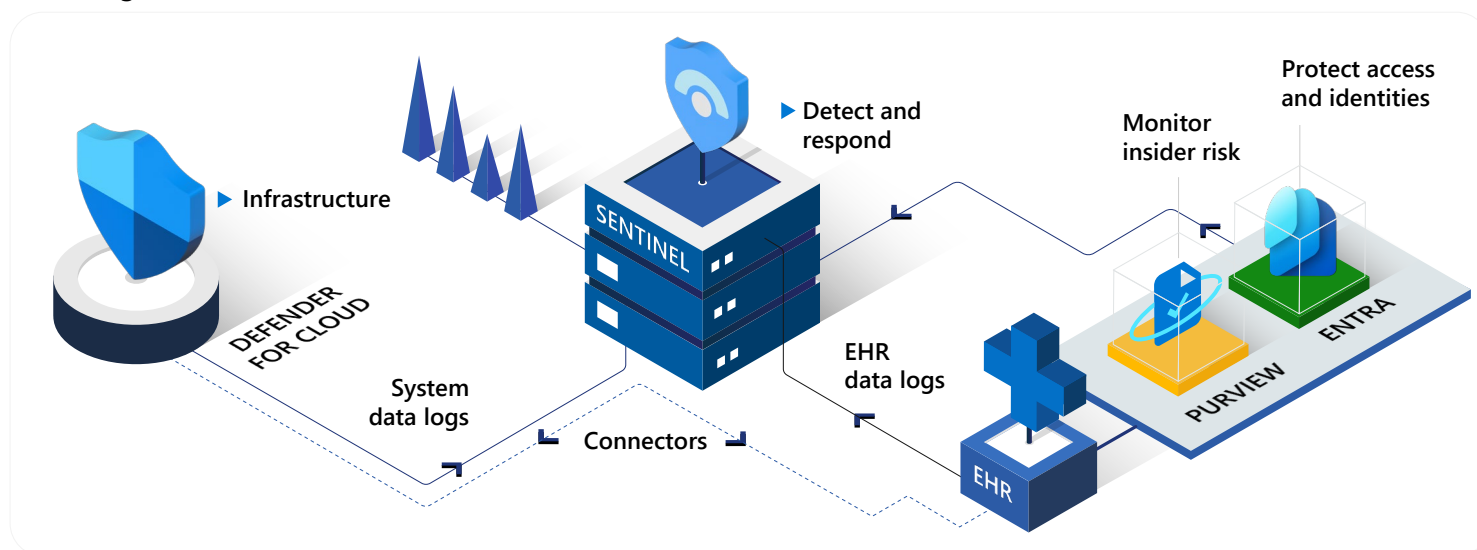
Microsoft Sentinel helps to streamline the ability to detect anomalous activity and take action against real-time threats to patient data.

Azure AD, part of Microsoft Entra

Safeguard credentials
- Limit access for privileged roles to critical operations for reduced attack surface

Conditional access to records
- Define when, where, and how Medical Financial Assistance (MFA) patient records are accessed

Microsoft Purview Insider Risk Management

Authorized patient data handling
- Simplified data governance: Preserve, collect, analyze, and export data for investigations
- Investigate suspicious activities such as record downloads or higher volume of records accessed

Defender for Cloud

Securing core EHR infrastructure
- Protect the SQL and Windows Server backend of the EHR from brute force SQL credential attacks, access from unusual locations or a dormant account, and unusual exports from an authorized user or DNS tunneling.
- Supports a multi-cloud application

Schedule a session with your representative to learn more

[1]Becker's; [2]Sophos