ERICOM
BE CONNECTED, BE SECURE

Healthcare Use Case

Deliver secure access for medical professionals, while preventing lateral movement on network

Security Challenge

Despite the efforts of talented, hard-working IT teams, hospital networks frequently have security gaps, due to perennially inadequate resources and the large number of people - internal and 3rd parties - who require access, as well as the challenges involved in patching multiple essential systems.

Consequences

In recent years, hospitals and healthcare organizations have been repeatedly – and often successfully targeted by ransomware attacks. Cybercriminals view vulnerable healthcare systems as attractive targets. They believe that, with patient lives in the balance, hospitals are likely to quickly pay ransom.

Risks

Phishing and attacks on vulnerable tools like VPNs are often used to breach hospital networks. Once malware enters the network, lateral spread enables theft and/or encryption of vital patient information, accounting, operations, scheduling and network-connected life-support systems.

Solution

Ericom Application Isolator provides policy-based, microsegmented access for users based on their authenticated identity, to prevent lateral network movement and vastly reduce exposed application and data surfaces in the event of attack.

Ericom Application Isolator: Policy-based Zero Trust Network Access Controls that Prevent Lateral Spread of Ransomware and Other Malware

Ericom Application Isolator is a cost-effective solution that enforces least-privilege, identity-based microsegmented access controls on existing VPNs and network infrastructure. Applications are fully cloaked from unauthorized users, who cannot attack applications and data that they do not see on the network. For healthcare organizations, this means that medical records are visible only to approved patient-facing staff, for instance, while only individuals who are authorized to see payment information can access relevant applications. As a result, even if a hacker gains access to a network, most applications will be invisible – and therefore inaccessible – to them. The same holds true for a malicious insider – their access would be restricted to a subset of systems, versus the entire network, thereby mitigating the damage that any individual can do.

Sales Contact

Softprom Distribution GmbH
Graben 19, 1010 Vienna, Austria

www.softprom.com
info@softprom.com

SOFTPROM