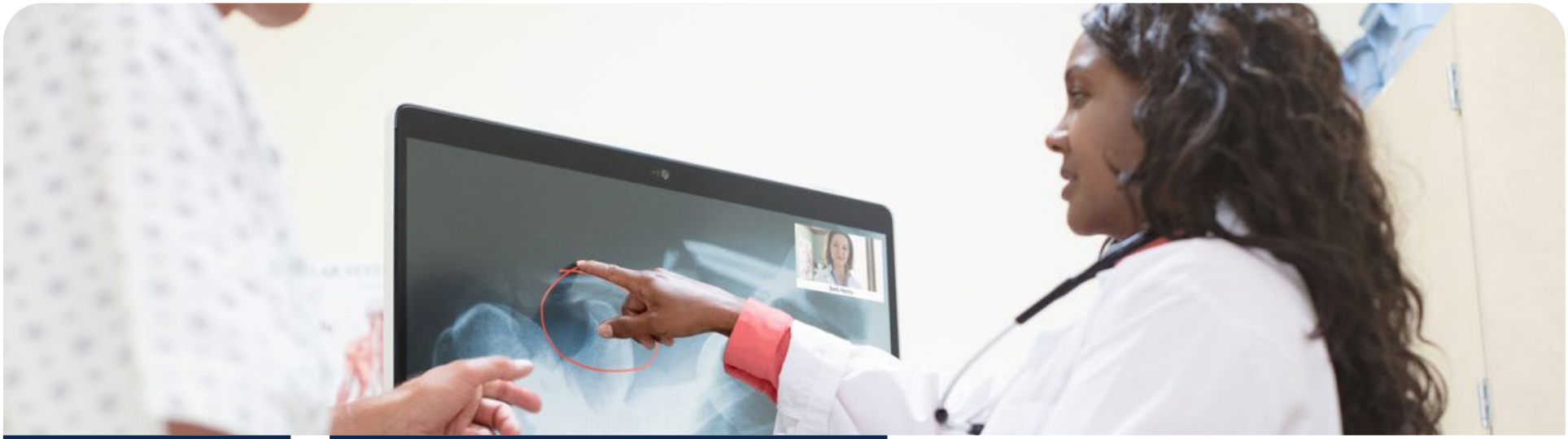
MarinHealth Keeps Employee and Patient Information Safe from Cybercriminals



Customer summary

Customer name
MarinHealth Medical Center

Industry
Healthcare

Results

MarinHealth keeps its employees and patient information safe by:

- Implementing multi-factor authentication (MFA) for external, internet-facing user portals such as Office365, Citrix Gateway login interfaces, and other important web applications
- Giving employees a reliable, easy-to-use way to provide login credentials

For MarinHealth, a midsized hospital based in Marin County, California, giving its employees external access to internal applications such Office365 and electronic medical records (EMRs) is standard practice. Therefore, it was of critical importance to put safeguards in place to protect employee and patient information from cyber criminals. Securing this information was a high priority because employee login to cloud-based Office365 and internal applications made available through an on-premises Citrix gateway required only a single authentication factor (1FA username and password). To strengthen security, MarinHealth turned to Cisco Duo in partnership with Citrix to provide multi-factor authentication-based access that would create a zero-trust framework.

Business challenge and results summary

Credential stuffing is a common malicious practice in which cybercriminals buy credentials from the dark web and attempt to use them to enter an external-facing system. Unfortunately, protecting against credential stuffing is beyond a security team's direct control; the team can tell users not to share passwords across accounts but cannot control this behavior. Therefore, teams must turn to MFA technology as their primary line of defense.

A security breach—at MarinHealth or any other hospital—has several consequences. First, a breach is a HIPAA violation that must be reported to the U.S Department of Health & Human Services and to patients. Second, if security is compromised, an estimated 40 hours of effort, on average, is required to investigate the breach. Finally, a breach can give cybercriminals access to protected health information that can be used as the basis for extortion.

To mitigate these potential risks, MarinHealth chose Cisco Duo, an easy-to-use, best-in-class security solution. Ease of use was particularly important to the hospital, because a difficult-to-use login interface can result in an influx of support requests from employees simply attempting to read email while not at the hospital. In addition to enterprise-class quality and ease of use, MarinHealth was pleased to discover that its Cisco Duo Care team was a true partner, always available to provide top-notch support.

> "The Duo experience is just very straightforward for our end users, with an experience that is very simple and consistent. It's pretty extraordinary how few tickets and issues we get with Duo given how especially pervasive it is within the hospital"

Scott Christensen
Security and Systems Engineer, MarinHealth Medical Center