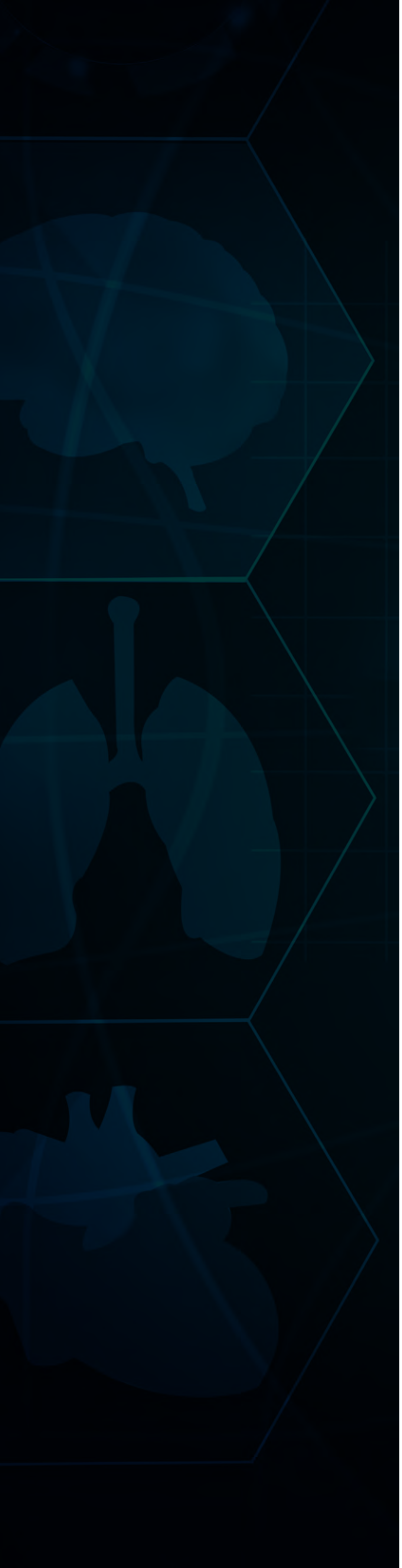
KEEPER
Cybersecurity Starts Here®

CASE STUDY

Keeper Gives Teleradiology Practice Total Visibility into Employee Password Habits

REV 7.17.22



OVERVIEW

Keeper's customer is a concierge-level teleradiology practice that performs preliminary and final emergent radiologic interpretations for radiology practices and medical institutions. In an emergency setting, communication is critical for effective real-time treatment decisions.

“We're dealing with people's lives and health, so we can't afford to make mistakes,” says the client's chief technologist and co-founder.

The company also cannot make mistakes when it comes to data security. “We deal with protected health information (PHI),” the client notes. “We have to keep both patient data and our internal communications secure with multi-factor authentication (2FA) and a comprehensive password manager.”

> **We have to keep both patient data and our internal communications secure with multi-factor authentication (2FA) and a comprehensive password manager.**

PROBLEM: LACK OF PASSWORD HYGIENE

The client company had instructed its staff to exercise good password hygiene, including 2FA and strong, unique passwords for every account. However, password manager usage was on an individual basis, with some employees using Keeper, some using other password managers, and some not using a password manager at all. The lack of consistency and centralized administration meant that the client had no visibility into employee password practices and no way to enforce its password policies.

Eventually, they experienced a limited email breach. “Someone used a weak password, and their email was compromised through a brute-force attack,” the client recalls. “Although no PHI was compromised and the scale of the breach was limited, we saw this incident as our opportunity to improve our cybersecurity by enforcing our password policies.”

> “
>
> **Although no PHI was compromised and the scale of the breach was limited, we saw this incident as our opportunity to improve our cybersecurity by enforcing our password policies.**

SOLUTION: ENFORCE PASSWORD SECURITY WITH KEEPER

After evaluating several password managers, the client chose Keeper due to its ease of use, excellent admin console, password autofill feature, zero-knowledge security architecture, and affordability. “I have been using another password manager for 10+ years and was happy with it. As part of my due diligence I began using Keeper and other password managers. I can say that Keeper was the easiest, most consistent and best manager I’ve used, bar none. Keeper had a low learning curve, and it was easy to implement. The autofill feature is highly accurate. When I need to autofill my login credentials, it detects the field correctly, without me having to customize anything. The other password managers I evaluated were not as accurate. I had to keep tweaking them.”

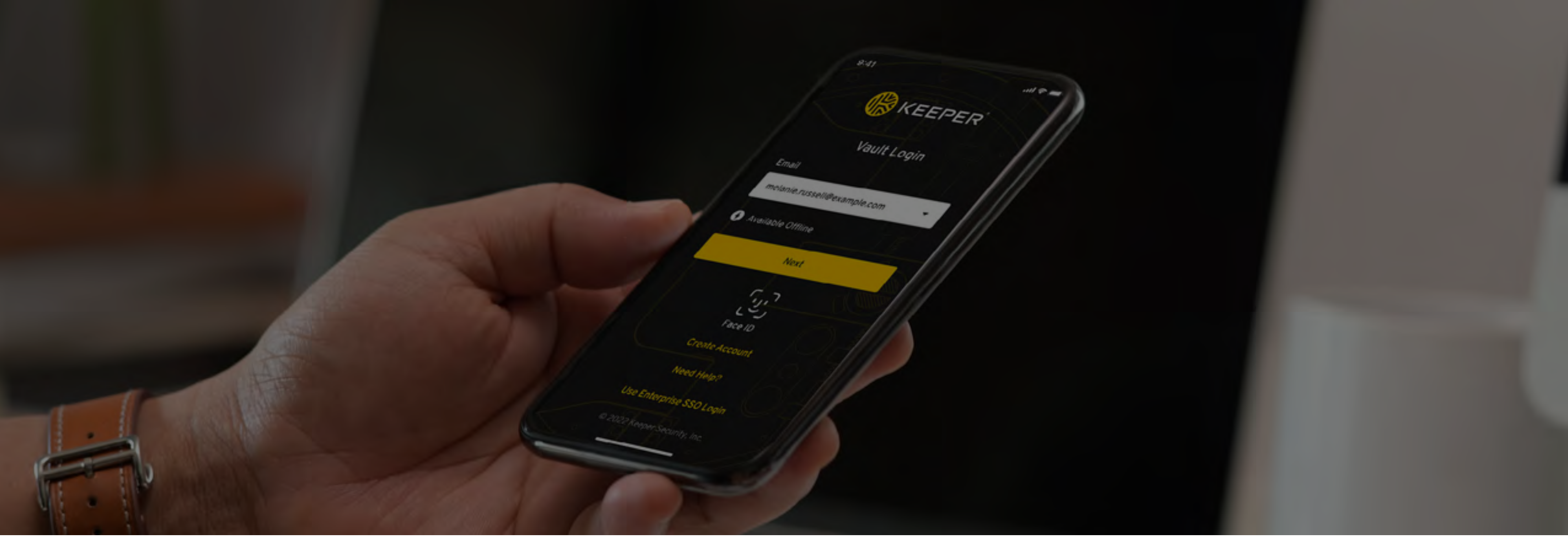
The client reports that the migration to Keeper went off without a hitch. “I’d been storing some of my passwords in my browser, and I also had some stored in one of the other password managers I evaluated. Transferring all of those passwords into Keeper was trivially easy, and I haven’t looked back. The migration didn’t cause any problems. I was able to delete all the passwords from my browser, and uninstall the other password manager, without skipping a beat.”

RESULTS & BENEFITS

“Everything that Keeper is supposed to do, it does really, really well,” says the client. “The administrative functions are great, and there are lots of visual dashboards, which make it easy for me to monitor my staff’s password practices. Sometimes, my staff members will try to use weak passwords, but now, I can see what they’re doing, and I can fix it.” He reports that the company is also benefiting from some of Keeper’s role-based access control (RBAC) controls, along with the ability to share passwords safely and securely.

Keeper has also bolstered the client’s confidence regarding the company being protected against further password-related data breaches. “Before we deployed Keeper, I couldn’t be sure that all of my people were following our password policies because I couldn’t check. Now, I know for certain that they’re using strong, unique passwords because Keeper shows me what they’re doing.”

> “
>
> **Before we deployed Keeper, I couldn’t be sure that all of my people were following our password policies because I couldn’t check. Now, I know for certain that they’re using strong, unique passwords because Keeper shows me what they’re doing.**



ABOUT KEEPER

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **https://keepersecurity.com**.

Keeper Third-Party Attestations and Certifications

Keeper Awards and Recognition

2021 Enterprise Leader
4.7 out of 5 stars

Editors' Choice
4.5 out of 5 stars

Gartner Peer Insights
4.6 out of 5 stars

Spiceworks
4.9 out of 5 stars