KEEPER
Cybersecurity Starts Here®

Case Study

Password Manager Helps Defend U.S. District Court Against Cyberattacks

A court storing critical trial and personal data needed a secure way to manage passwords for employees who all have multiple online accounts and devices.

Challenge

- U.S. District Court employees with 20+ accounts requiring passwords
- Courts responsible for their own cybersecurity, including password management

Solution

- Password manager and digital vault
- Zero-knowledge architecture
- 2FA protection against unauthorized access
- Password vault access via mobile devices

Results

- Password security visibility
- Password policy enforcement
- Seamless integration with existing systems

About The U.S. District Court for the Eastern District of New York

There are 94 district courts and two special trial courts in the U.S. federal court system. The U.S. District Court for the Eastern District of New York has 26 Article III Judges and 16 Magistrate Judges. They serve eight million residents in the counties of Kings, Nassau, Queens, Richmond and Suffolk, and concurrently with the Southern District, the waters in Bronx and New York counties.

The Challenge

District courts in the U.S. are responsible for their own cybersecurity. Amid increasing cyberattack risks, the Administrative Office of the U.S. Courts (AO) encourages district courts to identify and address their information technology (IT) security vulnerabilities. Among these vulnerabilities are weak or stolen employee passwords.

In the U.S. District Court for the Eastern District of New York (EDNY), the typical court employee has more than 20 accounts requiring login passwords. They also have an average of four devices, which further complicates online account management. Many times, EDNY judges and other employees were using the same passwords at home that they used in the office, which meant a cybercriminal who compromised one account could gain access to all of them.

> **The typical court employee has more than 20 accounts requiring login passwords.**

"The data breach epidemic, particularly the 2015 attack on the U.S. Office of Personnel Management, woke us up to the threat," said Doug Palmer, EDNY Clerk of Court, who oversees information security and IT. "Since the AO had not yet established password management best practices, the courts were left to find a solution on our own."

The Keeper Solution

As someone with 300+ accounts that require passwords, Doug was well aware of the potential risks he and his staff faced. He stays one step ahead by studying industry best practices, trends and emerging threats, which led him to use the personal version of Keeper's password manager to protect his own information. Seeing how well it worked, he deployed the business version for his EDNY employees.

"Not only do courts store valuable personally identifiable information, we store sealed case files that must be protected," said Doug. "These files have critical information, such as the identities of trial witnesses, plus a great deal of personal and operational information we must guard very closely. I truly believe a proper password management solution is integral to an effective security posture. The Keeper solution met all our criteria."

> **I truly believe a proper password management solution is integral to an effective security posture.**

The Results

Keeper brought immediate benefits to EDNY, including greater visibility into organizational password security, more control over password policy enforcement, account revocation capabilities and nearly universal client and browser support. Keeper's zero-knowledge architecture ensures no one but the user can access their data, not just at the office, but wherever they work. EDNY also implemented Keeper's two-factor authentication (2FA) from DUO Security as an extra layer of protection. Keeper integration with Microsoft Active Directory, which Doug's team uses to manage devices on the network, was seamless.

The Impact

U.S. District Courts are part of the federal judiciary system that resolves disputes by determining facts and applying legal principles to decide who is right. Information flowing in and out of the court system is vital to this process and must be protected from data breaches. Keeper helped EDNY close a vulnerability gap created by weak passwords, which leads to more than 80% of data breaches. [1]

> **Keeper helped EDNY close a vulnerability gap created by weak passwords, which lead to more than 80% of data breaches.**

About Keeper

Keeper Security develops leading password manager and security software for protecting businesses and client information. Keeper works with companies of all sizes across every industry to mitigate the risk of data breaches, bolster data security and privacy, increase employee productivity and strengthen cybersecurity reporting and compliance.

To learn more about Keeper Security's leading password manager and security software, visit **keepersecurity.com.**

Business Sales

Americas & APAC
+1 312 829 2680

Germany & DACH
+49 89 143772993

EMEA
+353 21 229 6011

Iberia & Italy
+34 919 01 65 13

United Kingdom
+44 20 3405 8853

Ireland
+353 21 229 6020

Netherlands
+31 20 262 0932

Sweden & Nordics
+46 8 403 049 28

[1] Verizon Data Breach Investigations Report, 2017

