keeper

Customer Case Study

Enterprise-Grade Cybersecurity for a US District Court

Comprehensive password management solution strengthens defense against growing cyber threat.

With 96 US District Courts in the United States responsible for their own cybersecurity and a big push for security audits by the US Courts Administrative Office, District Courts are stepping up to defend against evolving security threats.

The single greatest cause of data breach today is weak or stolen employee passwords. The Administrative Office has not yet established password management best practices, which means the Courts must quickly find a password management solution on their own.

Douglas Palmer is the Clerk of Court at Eastern District of New York (EDNY), a US District Court with 29 Article III Judges and 16 Magistrate Judges where he oversees information security and information technology. Doug stays one step ahead by studying industry best practices, trends and emerging threats. He explains how using Keeper's password manager and digital vault helps protect his confidential information from being stolen.

> "Not only do courts store valuable Personally Identifiable Information (PII) but hackers could go after sealed case files."
>
> **Douglas C. Palmer**
> Clerk of Court, US District Court, Eastern District of New York

When did you start using Keeper?

I started using the personal version of Keeper in 2014 and deployed the business solution to our District Court employees in 2016.

Why did your company deploy a password manager?

The data breach epidemic, particularly the OPM hack, woke us up to the threat. There's been a major shift to the cloud which has caused an increasing number of online accounts employees need to manage. I have more than 300 logins that require passwords and the typical court employee has more than 20.

Our users have an average of four devices, which further complicates managing online accounts. Before we deployed a password manager, judges were using the same passwords at home that they used in the office, which means a hacker only needs to compromise one of those accounts to gain access to all of them. It has become necessary to close that vulnerability gap.

Secure password management plays an integral role in our strong security posture by making it easier to protect and manage all of the sensitive accounts we use on a regular basis. The data breach epidemic, particularly the OPM hack, woke us up to the threat. There's been a major shift to the cloud which has caused an increasing number of online accounts employees need to manage. I have more than 300 logins that require passwords and the typical court employee has more than 20.

Keeper Security, Inc. ©2016

What are key benefits you get from utilizing Keeper?

Benefits include greater visibility into our organizational password security, more control over password policy enforcement, quick deployment with Active Directory integration, account revocation and nearly universal client and browser support.

What is the biggest security risk your industry faces?

Malware and information security. Not only do courts store valuable Personally Identifiable Information (PII) but hackers could go after sealed case files. These files have critical information that must be protected. For instance, high profile criminal cases are continually going on trial and the identity of witnesses could be in jeopardy.

Sealed court records may contain a great deal of personal and operational information that must be guarded very closely and a proper password management solution is integral to an effective security posture.

What advice do you have for other government agencies seeking cybersecurity solutions?

Get a zero-knowledge solution that works for your people everywhere, not just where they work. Also, incorporate and enforce a two-factor authentication tool with your password manager. We incorporated Duo Security for VPN, WiFi and Keeper access.

Keeper Security, Inc. ©2016