THOMSON REUTERS

Thomson Reuters Finds Security with Password Management
A leading information resource needed a secure way to manage and share passwords across a globally dispersed team.

**CHALLENGE**

- Employees managing passwords with spreadsheets and sticky notes
- Unable to securely share passwords and non-password credentials across geographically dispersed teams
- Inability to track record changes and access

**SOLUTION**

- Cloud-based password manager
- Password and non-password credentials and file storage
- Team sharing and access
- Audit trail of record activity

**RESULTS**

- Stronger data security
- Higher employee productivity
- Comprehensive reporting and analytics
The Challenge

Every day, governments, corporations, legal firms, news organizations and other fact-driven entities rely on Thomson Reuters for reliable, up-to-the-minute information. Factual integrity and data security are nonnegotiable cornerstones of Thomson Reuters’ business, especially amid ongoing cyberthreats. The company devotes entire teams to protecting their assets, one of which is the DevOps team for Tax & Accounting.

Factual integrity and data security are nonnegotiable cornerstones of Thomson Reuters’ business.

Like many information technology (IT) groups, DevOps manages a huge number of passwords, digital certificates and keys to access critical internal systems. With 20 team members spread across the United States, India, Canada and Argentina, however, they struggled to find an efficient way to securely store and share these passwords and credentials. They tried spreadsheets and other password management solutions, but found them lacking the level of security and functionality the team needed.

“At a minimum,” said Preston Scheuneman, DevOps Engineer in Thomson Reuters’ Tax & Accounting division, “we wanted a cloud-based password management solution that first, gave employees a secure alternative to spreadsheets and sticky notes, secondly, allowed us to share passwords and non-password credentials across teams in a secure way and lastly, gave us an audit trail of record changes and access. As a manager, I was also concerned about productivity. Our password management solution had to be easy, intuitive and cost-effective.”

As a manager, I was also concerned about productivity. Our password management solution had to be easy, intuitive and cost-effective.

The Keeper Solution

Preston and his team evaluated several top password management solutions against their objectives. After a live demonstration and a free trial of Keeper, Preston was convinced it was the best fit.

A key differentiator was that Keeper allows users to import passwords from .CSV, web browsers and other password management applications, enabling quick and easy deployment. “We needed to import more than 800 passwords to start,” said Preston. “Keeper’s onboarding process is very intuitive, and I imported all our passwords in bulk right away. The other solutions we tested wouldn’t allow it.”

Preston was also pleased with how easy it is with Keeper to share records and give the team immediate access, compared to other solutions that take up to eight hours to sync. Keeper uses Amazon AWS to host and operate encrypted digital vaults in the cloud, so managers can securely create, share and manage individual records and encrypted folders across teams.

About Thomson Reuters

Thomson Reuters is the world’s leading source of trusted answers and data to help legal, tax, accounting, news and media professionals run their businesses and make sound decisions. Headquartered in Toronto, Canada, the company has nearly 50,000 employees in 100 countries around the world.
Keeper uses Amazon AWS to host and operate encrypted digital vaults in the cloud, so managers can securely create, share and manage individual records and encrypted folders across teams.

Keeper also edged out solutions designed only for web password credentials. Thomson Reuters’ DevOps team manages a complex IT infrastructure that uses private keys, digital certificates, access keys, application programming interface (API) keys and other secret data. Keeper’s digital vault with 256-bit Advanced Encryption Standard (AES) encryption provides the security and privacy each user requires. Customizable fields allow the team to save information in the Keeper vault the way they want rather than being forced to use a predefined template.

The Results

Since deploying Keeper, the DevOps team has significantly increased productivity and visibility across teams and tightened security of Thomson Reuters data. “It’s super easy to generate and use complex passwords with Keeper,” said Preston. “It’s easier and quicker to access our individual passwords as well as shared team passwords on all our devices from one place. It’s a vast improvement over the past.”

The Impact

Weak password security leads to more than 80 percent of data breaches.1 Furthermore, most businesses have limited visibility into employees’ password practices, which greatly increases cyber risk.

Weak password security leads to more than 80 percent of data breaches.

Keeper helped Thomson Reuters solve these problems and protect valuable information assets through robust security features, comprehensive password reporting, auditing, analytics and notifications.

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

<table>
<thead>
<tr>
<th>Americas &amp; APAC</th>
<th>Germany &amp; DACH</th>
<th>EMEA</th>
<th>Iberia &amp; Italy</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1312 829 2680</td>
<td>+49 89 14377293</td>
<td>+353 21 229 6011</td>
<td>+34 919 0165 13</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Ireland</td>
<td>Netherlands</td>
<td>Sweden &amp; Nordics</td>
</tr>
<tr>
<td>+44 20 3405 8853</td>
<td>+353 21 229 6020</td>
<td>+3120 262 0932</td>
<td>+46 8 405 049 28</td>
</tr>
</tbody>
</table>

1 Verizon Data Breach Investigations Report, 2017