Western Union Rolls Out Skycure to Help Protect Mobile Devices

From small businesses and global corporations, to families near and far away, to NGOs in the most remote communities on Earth, Western Union helps people and businesses move money to help grow economies and realize a better world. A Fortune 500 company and a leader in global payment services, in 2016. With a focus on innovation, Western Union is always looking for new ways to send money through digital, mobile, and retail channels, with an array of convenient pay-out options to meet business and consumer needs.

268 Million
consumer-to-consumer transactions

$80 Billion
principal transferred between consumers

523 Million
business payments

Challenges

- Needed robust tools for helping to protect mobile devices across multiple threat vectors

- Integration between MDM and Mobile Threat Defense (MTD)

- Could not have significant adverse impact on end users' mobile devices

- Intelligent alerting and automated incident mitigation

- Keep mobile device software up-to-date

The Challenges of an Evolving Mobile Landscape

Western Union is a huge proponent of empowering end users via mobile devices. As an organization, Western Union believes in the power of mobility and the agility it brings to employees, which results in a more satisfied customer base. In line with its information security practices, Western Union periodically evaluates its information security program. Ultimately, Western Union determined that it would be beneficial to supplement its then-current solutions, which focused primarily on traditional security: helping to secure end points (like laptops) and the network perimeter.

Western Union decided that it wanted a solution that was built to help protect mobile devices across multiple mobile threat vectors, including the device itself, malware, malicious networks, and OS/app vulnerabilities. The goal was to implement a solution that was agile and able to grow alongside the mobile market.

Solution Deployment

In the first phase of deployment, Western Union rolled out Skycure to employer-owned mobile devices. Since Skycure is a cloud-service, there was no on-premises infrastructure that needed to be deployed or managed, and end users followed short instructions to install the apps themselves out of the Google Play or Apple App Stores.
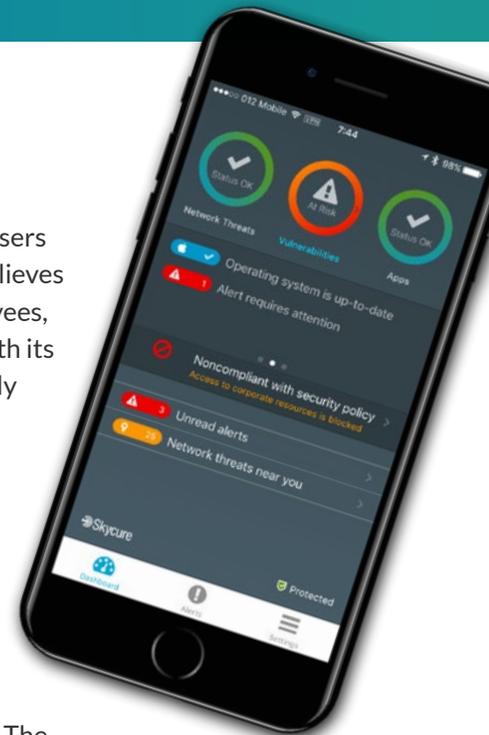
Solution

- Rollout Skycure's Mobile Threat Defense solution to mobile devices

- Use the Skycure console to help monitor and reduce organizational risk

- Pair with MobileIron MDM for policy-based device management

Results

- Mobile security tool that complements mobile management

- Access to key information and alerts for IT via the Skycure dashboard

- First line of support provided by Skycure, minimizing impact on Western Union

- Positive responses, appreciation, from end users

Once deployed, Western Union was able to focus its efforts across threat vectors such as:

- compromised Wi-Fi networks
- malicious applications
- out-of-date mobile device operating systems

"The breadth of Skycure's solution is very impressive."

—Tim Smith
Sr. IT Manager of End User Computing (EUC) and
Corporate Information Security (CIS)

Tim also found that end users had positive things to say about their experiences with Skycure. As Tim explains, "When we initially rolled out and Skycure identified potential malware that our other solutions had missed, we were pleasantly surprised when those users thanked us for alerting them. It is unusual to be thanked for security."

Next Steps

The next two phases for Western Union will involve leveraging Skycure for compliance auditing, and rolling out Skycure to additional mobile devices that are owned by employees themselves.

As a trusted financial institution, Western Union understands that it must take steps to help protect its network, and the Skycure solution is just one part of Western Union's multi-faceted approach to network security.

Skycure
Layered
Security

Cloud-level
Crowd-sourced
Device-level

Malware
Network
Vulnerabilities
Physical
Attack Vectors

About Skycure

Skycure's layered approach to mobile threat defense relies on the device itself to provide the first line of defense, cloud based servers to perform secondary, deep analysis and integrate with critical enterprise infrastructure, and crowd-sourced threat intelligence collected from every Skycure mobile app across the globe to enable predictive determination of both good and bad developers, apps and networks. Additionally, Skycure Research Labs continues their innovative approach to staying ahead of malicious hackers by diligently developing new methods of predicting and detecting unknown threats and identifying some of the most-discussed mobile device vulnerabilities of the past few years, including at least one for every major iOS release.

hello@skycure.com | 1-800-650-4821 | @SkycureSecurity

Skycure®
Mobile Threat Defense