![Lookout logo]

Case Study

Schneider Electric Secures 90,000 Devices with Lookout

The Challenge

Schneider Electric is leading the digital transformation of energy management and automation in homes, buildings, datacenters, and infrastructure across all industries and takes a modern, technology-enabled approach to its mission of developing best-in-class energy management and automation systems to customers. They understand that in order to deliver safe, reliable, efficient, and sustainable energy solutions as they continue to expand, they need to enable a strong mobile workforce all over the world that can rely on its mobile devices and applications to deliver on projects and boost efficiency in the field.

As Schneider has grown to over 170,000 employees in more than 100 countries, security has become top of mind. To manage mobile devices, Schneider uses EMM to control access to corporate resources such as email and internal applications, a SIEM to aggregate any security data, Single Sign-On for simplified access, and other traditional security measures to protect corporate resources. With all of this in place, there was one more piece to cover - securing mobile users and devices.

This project was led by Simon Hardy, who is the Global Head of Office 365 Services and Enterprise Mobility for Schneider. Simon knew that a Mobile Threat Defense (MTD) solution was key to enabling a secure mobile workforce, but he needed to find a solution that could easily be implemented into their existing infrastructure across a massive fleet of mobile devices. It was key for this MTD to be able to easily integrate with Schneider's EMM and SIEM solutions in order to deliver immediate value by identifying threats and helping Schneider align with stringent compliance requirements for users and internal reporting.

Customer Profile

As a leader in energy management and automation with operations in over 100 countries, the vision of Schneider Electric is to help its customers achieve more with less resources in a more connected, distributed, and smart world where the need for energy will continue to increase. Schneider Electric strives to help its customers achieve the most efficient and sustainable use of resources, assets, processes, and infrastructures with innovative technology solutions and services.

Industry: Utility / Managed Service

The Solution

Lookout Mobile Endpoint Security

Results

- Secure over 90,000 managed and unmanaged iOS and Android devices

- Seamlessly integrated with existing SIEM, SSO, and EMM platforms

- Deployed across the entire global fleet through Microsoft Intune

- Executed their BYOD mobility policy with Lookout securing all unmanaged devices

Security Challenges

- Implementing a cybersecurity tool that protects mobile Office 365 users connecting to corporate data.

- Demonstrating to auditors the ability to address cybersecurity threats on mobile devices, as well as detailed visibility into mobile device usage by employees.

- Securing a rapidly-expanding workforce all over the globe while embracing two different mobility policies

Schneider's security strategy was based on access rather than securing the actual devices and apps themselves. They also had measures in place to guarantee a secure gateway and connection to corporate assets. However, Simon acknowledged that reinforcement to all endpoints was a necessity, and they placed mobile devices at the top of the list for strengthening beyond the measures they were already using.

Solution Criteria

- Integrate with existing EMM, Single sign-on, SIEM, and other security tools

- Protect intellectual property and ensure alignment with various compliance standards and regulations.

- Be easy to implement, maintain, and manage while also educating the workforce on mobile threats

- Provide strong threat detection based on a large dataset with minimal false positives

The Solution

By selecting Lookout Mobile Endpoint Security, Schneider gained immediate visibility into the mobile security and risk posture of its mobile users. Knowing his team had a sizable deployment ahead of them, Simon decided to deploy in a series of steps by first securing a small number of key individuals in production to make sure the solution met requirements and expectations. Upon original deployment, Lookout exceeded expectations such that Schneider increased the deployment to cover 50,000 devices. Soon after, they expanded to 90,000

"Lookout is a well-known company in mobile security with more than 210 million devices already observed. We also found it to be the most mature solution throughout our entire evaluation, so we felt confident in our decision to go with the market leader" Lookout not only reinforced existing security tools, but filled a gap in Schneider's security posture. Combining Lookout with EMM means that, as devices access corporate resources, there's a continuous check on the health of the device to make sure only healthy devices are accessing corporate data without putting the entire company at risk. By pushing Lookout to employee devices with EMM and leveraging oneclick activation, Schneider was able to roll out coverage to a large mobile workforce with ease.

The Results

With with 90,000 Android and iOS devices now secured by Lookout, Schneider is aligned with both internal and external security requirements and is gaining unmatched visibility into mobile risk. The straightforward deployment process for back-end administrators and end-users alike made it easy to ensure full coverage in each step of the rollout process.

Being a global organization means that Schneider needs to constantly protect its employees against attacks in the field, which they've been able to do with sharp and accurate detection of Man-in-the-Middle attacks with an extremely low false positive rate, and align with the security and privacy laws of over 100 countries, which they can do for mobile devices by creating policies in the back end of the Lookout platform.

Schneider secures 60,000 devices that are managed with Intune, as well as an additional 30,000 unmanaged devices. Proof of the simple rollout process and immediate value out of the AI-backed threat detection for both device and app-based threats gives Schneider the confidence to make Lookout an integral part of expanding its mobility program all across the globe. With Lookout, Schneider was able to build a complete mobile security strategy as they embraced a more complex mobility program with simple deployment, immediate visibility into app and device-based risks, and alignment with internal and external security compliance policies around the world.

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo