



Customer Case Study

Telenor secures and empowers a global workforce



Industry

Telecommunications

Objectives

Protect the supply chain through NIS2 compliance, lock down BIOS settings, and simplify global reimaging challenges.

Business outcomes

- Saved 1 full-time employee by implementing Sure Admin.
- Simplified and secured passwordless BIOS setting management across a global PC fleet.
- Achieved 10% - 15% reduction in OS recovery help desk tickets.
- Increased employee productivity with user self-serve OS recovery.

Country

Norway

Approach

Implement **HP Sure Admin**¹ and **HP Sure Recover**² for enhanced supply chain security, secure device lifecycle management, and improved employee productivity.

Strict security for a global, hybrid workforce

Telenor, a major Telecom company in Norway, offers a full suite of mobile and fixed services in the Nordic region and parts of Asia, including Bangladesh, Pakistan, Malaysia, Thailand, and Singapore. Its End User Computing (EUC) team of 25 support approximately 11,000 employees globally. While most staff work in a hybrid model, those located far from a Telenor office work fully remote. Despite this global spread, Telenor maintains a unified security posture across countries, applying the same stringent rules to all employee PCs, whether they are in the office, hybrid, or remote.



“[HP provides] secure components such as the Endpoint Security Controller. It’s even quantum-safe”

“HP is one of the few vendors out there that does something about [the quantum threat] instead of talking about it.”

Thomas Gudmundsen
Head of Information Security,
Telenor Shared Services.

AI and the move to firmware attacks

As the threat landscape evolves, AI is enabling hackers to launch faster, more persistent attacks.

“AI can be used for so many things: crafting malware, attacking our software, but it can also be used to lower the bar on how to attack firmware,” says Thomas Gudmundsen, Head of Information Security at Telenor Shared Services. “Attackers are going down the security stack to the hardware level to steal customer data.”

This shift, combined with the emerging threat of quantum computing, requires a more resilient approach to device security.

Quantum-resistant firmware protection

HP Wolf Security capabilities provide a dedicated layer of firmware protection built directly into business-class PCs.

This is powered by the **Endpoint Security Controller (ESC)**, a physically isolated security microprocessor that runs before the CPU starts. At device startup, the ESC validates that the BIOS and other critical firmware have not been tampered with. It has self-healing properties, ensuring the integrity and authenticity of the platform.

The ESC acts as the root of trust for the PC and cryptographically protects the layers below the operating system such as the BIOS. Many HP Wolf Security features are BIOS-based and cryptographically secured, including **HP Sure Admin** and **HP Sure Recover**.

Passwordless BIOS administration

At Telenor, the need for a new approach became clear after an EUC employee mistakenly shared a BIOS password in an unobfuscated script. This triggered an immediate lockdown, forced the company to change BIOS passwords for all employee PCs, and led to burdensome monthly BIOS password changes.

Paul A. Teigland, Team Lead for Device Management & Core Services, EUC at Telenor Shared Services, approached HP to find a sustainable path forward. The HP team immediately recommended **HP Sure Admin**.



HP Sure Admin

HP Sure Admin replaces passwords with a secure, multi-factor authentication system to access the BIOS settings. Now, instead of managing passwords, the admin sends a QR code to the person who needs access. When the person scans the code, they receive a one time PIN, allowing for secure, temporary access without the risk of a password leak.



Working with HP Norway and HP Security Labs, Telenor moved from a successful Proof of Concept to seamless global deployment. Teigland noted that having a direct line to the HP team ensured any questions were resolved immediately.

Remote OS recovery

Historically, Telenor's remote and hybrid employees facing operating system issues required a new golden image to resolve the problem. This process began with a help desk call, followed by an EUC team member manually shipping a jump drive to the employee and providing remote support. These manual interventions drained EUC resources and caused significant user downtime.



HP Sure Recover

To solve this, Telenor implemented **HP Sure Recover**, a secure method to reimage a machine quickly. This way, employees can restore their own device with the latest golden image, significantly reducing help desk tickets and getting users back to work in a fraction of the time.

"We don't always have access to a local office or a local network where we can retank devices on prem office to do a break fix. [Now, employees] can just restore the device and they're up and running within an hour."

Paul A. Teigland.

Collaborative partnership

By working closely with HP teams, Telenor has successfully implemented HP Wolf Security solutions with a direct feedback loop. As security requirements and threats evolve, this partnership ensures that Telenor's security stack remains resilient and future-ready.

"My relationship with HP Security Labs and HP Norway feels more like a joint engineering effort rather than a customer-vendor relationship," says Teigland. "They are there to help you. They love it when you implement their tools, and they are there to assist you."

Continuous resilience

With **HP Sure Admin** and **HP Sure Recover**, Telenor has enhanced supply chain security, increased the EUC team's operational efficiency, strengthened security across the entire PC lifecycle, and improved employee uptime and availability.

Expanding on the successful implementation of these capabilities and the continued backing of the HP team, Telenor plans to continue fortifying its security stack with HP Wolf Security solutions.

"Implementing HP Sure Admin saved us at least one full-time employee that had to package the updates for the passwords and [make] sure that all the devices and our fleet was updated to the current correct password."

"Other unexpected benefits I got from Sure Admin was the ease of handling the platform. How easy it is after it's set up to make it work, to give access to users, to get into or remove access if they don't need it."

Paul A. Teigland
Team Lead - Device Management &
Core Services, End User Computing
Telenor Shared Services

[Watch video](#)

1. HP Sure Admin requires HP Manageability Integration Kit or HP Wolf Security Controller and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.
2. HP Sure Recover is available on select HP products and requires an open network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.

