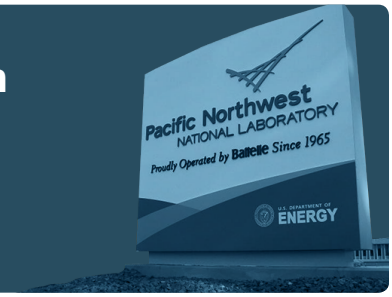
yubico

PNNL Deploys YubiKey Smart Card Authentication Organization-Wide



Case Study

Pacific Northwest
NATIONAL LABORATORY

Industry
Science and Engineering

Protocols
PIV smart card

Products
Various form factors, including YubiKey FIPS Series

Deployment
Employees

About Pacific Northwest National Laboratory

The Pacific Northwest National Laboratory (PNNL) focuses on the advancement of science and engineering. PNNL applies their scientific expertise to tackle some of the most challenging problems in energy, the environment, and national security. Given the sensitive nature of PNNL's work, it is essential to protect the systems and information accessed by PNNL staff.

Modernizing Authentication for All Staff

Historically, the lab used smart cards for strong authentication. However, they were not a requirement for all employees. Only a few privileged users were required to use smart cards, and only for access to specific systems like firewalls, Microsoft Active Directory, databases, or servers. In an effort to improve the security posture of the entire organization, the lab decided to deploy smart cards for all standard user accounts.

In addition to increasing security, it was essential that the authentication process be streamlined and simplified. PNNL needed a solution that would provide high levels of security, yet be intuitive enough for a large number of users to use on a daily basis. This led the team to select the YubiKey.

Crafting the Right Message to Increase Adoption

Far too often, changes to policies, processes, and protocols are communicated to employees as hard requirements, and forced upon the organization by the IT department. This often makes it difficult for companies to deploy new security technologies and receive positive user buy-in. Knowing this, and with a large deployment in mind, PNNL took a radically different approach, taking extra steps to properly communicate with their employees about the changes that were coming and the expected impact.

The PNNL deployment team carefully crafted messaging, and even provided messaging templates that managers could use when communicating with staff. The messaging focused on the usability, simplicity, and the improved user experience of the YubiKey. While the YubiKey is also more secure than the previous authentication process, strong security was a secondary message.

The PNNL IT team also conducted user testing before seeking voluntary early-adopters across the entire organization. This was supplemented by encouraging employees to ask questions in person and in real time rather than reading an FAQ or an email.

Case Study

Pacific Northwest
NATIONAL LABORATORY

Industry
Science and Engineering

Protocols
PIV smart card

Products
Various form factors, including YubiKey FIPS Series

Deployment
Employees

In an effort to humanize the changes, a widely-known and well-liked member of the IT team became the "face of the project". All communications included the IT staff member's photo, as well as images of the YubiKey, so employees became increasingly familiar with the new login and authentication process.

The deployment team also developed and used an online scheduling tool to streamline the YubiKey registration process for employees. The system sent out confirmation emails detailing appointment information for each employee including the items to bring for registration and identity proofing. These same emails were used to reinforce YubiKey messaging and benefits.

Creating and Executing Efficient Deployment Strategies

The key to this customer's successful deployment started with a dedicated, cross-functional team with a strong background in change management. Having a strong team behind the deployment enabled the customer to roll out YubiKeys to over 4,500 staff within six months.

It's important to note that each employee was issued two YubiKeys—one YubiKey 4 Nano and one YubiKey 4—with one serving as the primary YubiKey, and the other as a backup. The YubiKey Nano form factor is intended to stay in the employee's computer as a semi-permanent installation for added convenience during frequent authentication. The YubiKey 4 keychain form factor was provided as a backup device, meant to be kept on the employee's keychain or with their badge.

The deployment team also planned how to handle identity proofing regardless of whether an employee was on or off site. On-site employees were required to bring their badge and a second form of government-issued ID at the time of their in-person registration. At the time of their registration, a high definition (HD) photo was taken in real time and kept as record in compliance with NIST requirements, as part of the identity proofing process.

Off-site employees communicated with a registration agent over video chat and in front of a registration authority member. The registration agent shared a virtual console with the employee, who was then able to create their unique PIN that would be used to operate their YubiKey. The registration agent then inserted the employee's YubiKey into their machine to ensure that the proper certificates were downloaded to the device. This process was repeated to register the second YubiKey. Once the registration process was complete, the employee's YubiKeys were shipped via a third party mailing service, which required a signature to validate chain of custody.

Benefits of YubiKey

- Flexible, strong authentication for all staff
- Quick and easy to deploy across an entire organization
- Intuitive and user-friendly to encourage employee adoption

Yubico AB
Olof Palmes gata 11
6th floor
SE-111 37 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088