yubico

Boliden advances its reputation for innovation with YubiKeys

Phishing-resistant MFA enables digital transformation

Case Study

NEW BOLIDEN

Industry

- Natural Resources

Benefits

- Increased security
- Faster login
- Improved user experience
- Multiple protocols on one device

Protocols

- FIDO2
- PIV

Products

- YubiKey 5C NFC

Deployment info

- Privileged users

Mathias Ignberg
Service Manager: Identity & Access Management and Cloud at Boliden

A strong heritage of innovation and commitment to sustainability

Boliden is one of Europe's leading metal mining companies. Based in Sweden, with presence around the Nordic region and beyond, Boliden produces a vast array of the metals required for modern life: zinc, copper, lead, nickel, gold, palladium, platinum and silver. Known for their commitment to sustainability, with a vision to be the most climate-friendly metal provider in the world, Boliden operates at the forefront of innovation, utilizing cutting-edge technology to optimize and improve their operations.

Mathias Ignberg is Service Manager for Identity & Access Management and Cloud at Boliden. In more than a decade in his role, the company has grown and so has its reliance on cloud systems like Microsoft Azure and Amazon Web Services. "We are really forward leaning regarding technology and try to optimize everything," says Ignberg. Boliden's employees are spread out across offices, mines and smelters, which are often in remote locations. Employees need to be able to securely access their company accounts from wherever they are.

Evolving cyber threat landscape called for better risk mitigation

As the importance of online identities and cloud access has grown, the global cybersecurity landscape has also evolved. Cybercriminals are getting smarter, explains Ignberg: "It's interesting but also very scary how attackers now have an ecosystem—it's even possible to buy cybercrime as a service. We have a SOC (Security Operations Centre) team that is monitoring our environments 24/7 and, of course, we see lots of attacks coming in." Like many businesses, Boliden worries about ransomware encryptions.

> "The nightmare from the company's perspective," says Ignberg, "is being forced to stop production. Smelters can't just be turned off and on. They are complex and even a temporary pause can lead to serious long-term consequences. We know exactly how much it would cost for us to stop production even for several hours."

The mining process can be dangerous, as explosions release toxic gases into the air. That's why Boliden hopes to push the boundaries of automation so that workers no longer need to be physically present in the mines. Fully remote operations, aided by autonomous self-driving vehicles, would improve employee safety and allow for continuous production. Making this change requires implementing reliable, powerful internet connections for all mines, even deep underground. However, being connected to the outside world also brings cybersecurity risks.

Boliden urgently needed **better protection** for privileged accounts

Zero Trust and passwordless: an ambitious new approach to identity protection

As Boliden moved towards increased digitization, previous cybersecurity protections were deemed insufficient. "We just had username and password," says Ignberg. "Honestly, it was terrible. With the modern threat landscape, we urgently needed better protection for highly privileged accounts like global admins and domain admins." It was time for a new approach. "The two big drivers," says Ignberg, "are a Zero Trust philosophy and being on the journey to passwordless login. Since people are roaming around more and using more cloud services, it makes the protection of identities more important. From a security standpoint, passwords by their nature are bad. Going passwordless is a win-win. It's better for the user: they don't need to remember a password so it's easier for them to sign in to everything. On the other hand, it's also much more secure. Of course, there are challenges to making it work— it requires changing how people work and think. It's not something you do overnight."

> "From a security standpoint, passwords by their nature are bad. Going passwordless is a win-win. It's better for the user: they don't need to remember a password so it's easier for them to sign in to everything. On the other hand, it's also much more secure."
>
> Mathias Ignberg, Service Manager: Identity & Access Management and Cloud at Boliden

Boliden decided to implement FIDO2/WebAuthn authentication to simplify online account login, increase security and, most importantly, reduce their reliance on passwords. "We are aiming for a passwordless world," says Ignberg, "and a big part of that is the YubiKey." While FIDO2 authentication was possible using other methods, like Smart Cards, Ignberg decided to purchase YubiKeys for highly-privileged accounts: "I was actually given a sample key from another brand a few years previously, but it didn't work as well. It's much easier to use YubiKeys, which is why we went with them. We liked that YubiKeys are a FIDO device and that they can also be used as a Smart Card.

YubiKeys deliver stronger security assurance than mobile MFA

Boliden is still using Windows Hello for Business and Microsoft Authenticator applications in certain parts of their operations. "I like anything that helps get rid of passwords," says Ignberg, "but the use case needs to determine which solution we choose. The YubiKey is safer than mobile authentication so for highly privileged accounts we only use YubiKeys, not the authenticator. The advantage of YubiKeys is that they are physical devices that need to be touched in order to work — this adds an extra layer of security. We use YubiKey 5C NFCs, but we don't restrict how employees use the device. If they want to use the NFC capability, great. If they just put the YubiKeys in the USB port, that's also okay. We use the YubiKeys for FIDO2 authentication to Azure, Micorosoft Office 365 and AWS, but also as Smart Cards, using certificates, to protect privileged accounts and server access on-prem. The same YubiKey can be used for everything. We wanted one device to cover all aspects, both in the office and when traveling."

Overall, deployment has been a success. "Implementation was very simple," says Ignberg, "and so far everything is working well. We have not tried to put numbers on it, but YubiKeys have increased our feeling of security and saved us time. For example, I don't need to know passwords for a lot of services anymore, and I feel safer. It's definitely improved the experience. People are very happy when they don't have to use passwords anymore. Then they say, 'Hey, YubiKeys are really good!'" Boliden also allows employees to use the YubiKeys for their private accounts. "We are not restricting them," says Ignberg, "because protecting private accounts also helps the company. I use the YubiKeys for my own private accounts."

The YubiKeys are a good fit for Boliden's ethos of innovation. "YubiKeys are a big enabler for digitization," says Ignberg. "They protect the identity of the end user and make their life easier. If a company moves towards digitization, you have to do it securely. It was different 15 years ago, but since more and more tools and functions are cloud-based, it's essential to protect identities."

> "
>
> YubiKeys are a big enabler for digitization. They protect the identity of the end user and make their life easier. If a company moves towards digitization, you have to do it securely. It was different 15 years ago, but since more and more tools and functions are cloud based, it's essential to protect identities."
>
> Mathias Ignberg
> Service Manager: Identity & Access Management and Cloud at Boliden

Expanding YubiKey deployment to a broader set of use cases

While the initial deployment was relatively small, Boliden plans to roll out FIDO2 authentication across the entire organization in phases. "First, we want to roll out to all IT employees company wide," says Ignberg, "then we want to offer YubiKeys to end users more widely. It all depends on the use case. We see big potential for using YubiKeys in our open-pit mines, where a big chunk of the workforce only has a mobile device. We need to let the local IT staff make their own decisions, but there are different mines where the teams are always keen to try new things. I hope the project will really pick up speed during the next year."

Ignberg is delighted with the results so far and has advice for anyone else considering starting on a similar journey. "Start! Just start," says Ignberg. "Start small, with your most important admin accounts. It's better to start even if you don't have the full picture or know exactly how you're going to do it. It's better to protect a few users rather than none. The more accounts and identities you protect, the better."

Contact us
yubi.co/contact

Learn more
yubi.co/energy

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.