yubico

Blockchain security firm Halborn protects remote team with YubiKeys

Phishing-resistant MFA provides seamless employee onboarding

Case Study

// HALBORN

Industry
- Security

Benefits
- Identity-based access control to secure systems and data
- Scalable to support seamless onboarding for global, remote team
- Seamless login to SSO through G Suite

Protocols
- FIDO2

Products
- YubiKey 5 Nano
- YubiKey 5C Nano

Deployment info
- Full global team
- 2 YubiKeys per employee

Blockchain security firm Halborn drives exponential growth, built on a solid security foundation with YubiKeys

Halborn is an award-winning blockchain cybersecurity firm providing end-to-end security from smart contract audits and penetration testing to cloud automation. With the growth of crypto-currency usage and crypto crime, costing up to $3.2 billion globally in 2021, Halborn's services are increasingly in demand to help clients, including Layer 1 blockchains, infrastructure providers, financial institutions and app and game developers, stay safe in the new Web3 ecosystem.[1]

Halborn was founded in 2019 by serial entrepreneur Rob Behnke and Steven Walbroehl, a renowned ethical hacker with 25 years of cybersecurity security experience. Since its launch,it has self-funded its growth to over 100 employees, including 80 best-in-class security engineers from across the world. Halborn recently raised a $90 million Series A funding round to help accelerate the growth of its security team and the development of blockchain security SaaS products.

Remote work drives need to prioritize modern phishing-resistant multi-factor authentication (MFA)

As a remote-only organization and one of the most trusted and fastest-growing Web3 security firms, Halborn has consistently prioritized its own security architecture. While traditional factors such as passwords or SMS are widely known and used, Halborn needed an extra layer to secure its whole team. When founding Halborn as a fully-remote organization, Behnke and Walbroehl relied on the YubiKey, Yubico's phishing-resistant multi-factor authentication (MFA) security key.

"As we started hiring individuals, remote work was a concern," noted Walbroehl. "Information must be protected." The award-winning YubiKey is built for security and trusted by the world's largest organizations to help put a stop to phishing attacks and account takeovers. In fact, it was already a trusted solution used by Halborn CEO and CoFounder Rob Behnke.

Behnke and Walbroehl made the YubiKey a standard part of every employee's onboarding process, even as that team has grown to spread across more than 50 different countries. "It's been really easy for us to set up YubiKeys as a standard security measure for everyone," notes Walbroehl.

Steve Walbroehl
CTO and CoFounder

> "As a blockchain security firm, securing information with strong MFA is non-negotiable. YubiKeys provide a really safe way to do this for every team member's account."
>
> Steve Walbroehl, CTO and CoFounder, Halborn

[1] Chainanalysis, 2022 Crypto Crime Report

Empowering employees with a highly secure, yet low-friction and productive environment

To support the 100% remote, diverse, and bright team of engineers and ethical hackers, Halborn leverages a unique gamification system designed to reward and incentivize its employees based on proof of work and continuous learning. For this highly-competitive and self-reliant culture, traditional security tools and processes could be a source of potential friction in the employee experience.

Traditional security tools such as anti-virus often cause significant problems for security testing tools, leading to errors or requiring whitelisting. Instead, Halborn opts to focus on supporting the productivity of its employees and employee use of its open-source tool Ziion by focusing on preventative security. Preventative security includes restrictions on downloading data, endpoint control, role-based access controls, and a VPN that is secured by G Suite's single sign-on (SSO) and MFA with the YubiKey. All of this information is logged and monitored to ensure endpoints remain properly configured and policies remain enforced. With the YubiKey securing endpoint access to its systems and data, Halborn has created a more efficient security posture, a key factor to supporting its growth.

"The YubiKey provides that control and protection on the access layer," notes Walbroehl. "If there were a SIM swap or two-factor breach, the hardware piece—something you need—is now there so you can't use those credentials."

In the early days of the organization, Halborn reimbursed its employees for their choice of laptop and two YubiKeys, with the second spare key to be stored securely to protect against loss. Today, Halborn is shifting to a company-owned model to provide additional endpoint control, leveraging dropshipping to supply pre-imaged laptops and YubiKeys directly to employees. Employees follow Yubico's guided tutorials to set up their YubiKeys, often the "easiest component in onboarding," shares Walbroehl.

The imperative to secure client information with layered protection

Having been mindful of its own user base, its employees, Halborn is also very mindful of the fact that it is in a position to help protect the future of blockchain-powered projects around the world. But this trusted position comes with an obligation to protect the information it gathers about its clients.

Halborn does not take custody of customer data, but it does provide security assurance through advanced penetration testing and smart contract audits, the results of which need to be kept secure. In addition, as part of helping to secure the frontier of emerging technology, Halborn employees find zero-day exploits nearly every week, information which could put many organizations and the public at risk if used inappropriately.

"We make sure that when contracts and tokens come out they are done properly so that people do not lose money," notes Walbroehl. "Our reputation is on the line to make them secure—and to stay secure ourselves." To date, Halborn has a perfect record of protecting its own system—thanks, in part, to the YubiKey.

As a part of its adherence to NIST and ISO 27002 standards, Halborn leverages the YubiKey as a second factor for single sign-on (SSO) access to G Suite, which the company uses for everything, and as part of a four-factor authentication for privileged access to its most sensitive assets. The YubiKey acts as proof of identity, something a user has, used in combination with other factors to add additional layers of protection for Halborn's data. Halborn's example, as one of the top Web3 security firms, sends a clear message in today's world: passwords are just not enough.

Best practices to ensure a secure future for all Halborn stakeholders

Halborn continues to focus on ensuring that its remote workforce of bright, innovative and highly motivated team members continues to experience a secure posture, as it interacts with clients. And, as part of its Advisory Services, Halborn recommends its own clients adopt best practices in identity and access control, including secure MFA and hardware devices such as the YubiKey. Further, as a course author for the SANS Institute, Walbroehl advocates for stronger education on how blockchain works and how to defend against threats—including how to protect against identity-based attacks with a modern smart card and FIDO-based hardware security key such as the YubiKey.

> “Access and identity are the true perimeter of a remote organization. There’s nothing better than a hardware device for protecting this.”
>
> Steve Walbroehl, CTO and CoFounder, Halborn

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088