

TrueCode Capital leverages YubiKeys to secure accounts

Phishing-resistant MFA provides high-assurance authentication to protect cryptocurrency exchange accounts



Case Study

TRUECODE CAPITAL

Industry

- Financial Services

Benefits

- Layered security for access control
- Phishing-resistant multi-factor authentication (MFA) to manage risk
- Business continuity and disaster recovery

Protocols

- WebAuthn/FIDO2

Products

- YubiKey 5C Nano
- YubiKey 5Ci
- Yubico Authenticator

Deployment info

- Full organization deployment of 2 YubiKeys per employee
- Included in a welcome package for investors

Cryptocurrency risk management supported by phishing-resistant multi-factor authentication (MFA)

With a strong background in high-performance computing environments and nearly twenty years of developing and capitalizing on emerging technologies through a number of start ups, Joshua M. Peck was seeking a way to maximize the return on his own investments. Further, Peck wanted to be able to make investment decisions based on quantitative advice, not the qualitative advice of financial advisors. Peck wanted to be able to invest in risk-based opportunities, but without the human capital or paperwork associated with traditional opportunities in real estate or angel investment.

Unable to find such a solution, Peck set about building a system that would take advantage of the latest in machine learning, financial engineering and risk management methodologies and apply that to cryptocurrency. After testing the solution he built that achieved an annual internal rate of return (IRR) in excess of 80%, Peck and his partners launched it as part of TrueCode Capital, a cryptocurrency hedge fund investment firm created to help family offices who manage, preserve and grow family wealth.

Unlike the equities market, which has over 100 years of data to support risk profiles and protocols to manage risks, cryptocurrency is new. As a bearer asset that exists on a computer, it comes with new kinds of risks—risk that a hard drive crashes or gets a virus. And risk that a user will be phished. The risk-first philosophy that drove Peck to create TrueCode Capital helped identify the need for a solution to drive down these other forms of risk.

Peck knew that private key storage was a weakness for cryptocurrency, knowing first hand a victim of phone hijacking that resulted in cryptocurrency loss. In fact, legacy forms of MFA that rely on mobile devices such as SMS OTP and push-app may be better than passwords but are also easily breached via phishing attacks, SIM swapping and man-in-the-middle (MiTM) attacks. “Two-factor authentication has been bad for a long time,” notes Peck, referring to SIM jacking and other phone injection attacks that have led to successful crypto attacks. Peck knew that he needed a way to store private keys securely on an offline or “cold” hardware device to help protect credentials from cyberattack.



Steve Walbroehl
CTO and CoFounder

“When you’re thinking about risk management with cryptocurrency, you mostly just think about the price action. But ultimately cryptocurrency projects are software as much as anything, so we need to address cybersecurity risk, counterparty risk and human risk.”

—Joshua M. Peck, Founder and Chief Investment Officer, TrueCode Capital



Yubico adds layers of security for access control

Peck was already aware of the security benefits of the YubiKey, a hardware security key designed by Yubico. Trusted by enterprise and tech leaders across all verticals, Peck knew that the YubiKey offers the strongest protection against advanced phishing and MiTM attacks to defend against cybercriminals with strong two-factor, multi-factor and passwordless authentication.

With the decision to move forward with YubiKeys from day one, Peck only needed to decide which YubiKeys he preferred for himself and the organization. TrueCode Capital selected two kinds of YubiKeys in its deployment to employees and contractors: the YubiKey 5C Nano, a key designed with a low profile that can remain in a USB port, yet remaining entirely separate and secure, and the YubiKey 5Ci, designed with dual support for both the Lightning port and USB-C. Further, TrueCode Capital uses the Yubico Authenticator app to generate 2-step verification codes on the hardware key, adding another layer of protection so that these secrets cannot be compromised.

“ Instead of building an on-prem data-center as many of our peers must do, with Yubico’s support we can secure our cloud vendors appropriately so we can take advantage of the modern cloud stack,” says Peck. The net result has helped reduce both startup and operating costs to the tune of hundreds of thousands of dollars.

Although TrueCode Capital is reliant on third-party custody, trading in exchanges with counterparties who are SOC 2 compliant, securing family wealth includes distributing the YubiKey as part of the welcome package for new family office investors.

“The market risk is easy to manage,” notes Peck. “But managing access control to exchange accounts, managing access control to your computer, managing access to your email—this is the low-hanging fruit of cybersecurity.” The YubiKey is a tool that is deployed right across TrueCode Capital and recommended to all TrueCode Capital investors and any would-be investor in cryptocurrency, as noted in Peck’s upcoming book, *Cryptocurrency Risk Management: A Guide for Family Wealth Managers*.

“There’s a tremendous number of people who have cryptocurrency on the radar,” notes Peck, “But they’re not thinking about how to protect themselves.” While not everyone will be able to invest with TrueCode Capital, based on the Section D exemption from the SEC, Peck wants to be a leader in helping people protect their investments.

Given the relative immaturity of cryptocurrency and blockchain, and the potential for a high payout, cyber attacks continue to evolve. For example, an emerging risk in cryptocurrency is associated with bypassing two-factor authentication through the API, a risk made possible with API keys that are not read-only—exposing these accounts to being drained.



“

People have lost more money out of bad passwords than they have from market draw-downs.”

—Joshua M. Peck, Founder and Chief Investment Officer, TrueCode Capital

YubiKey as enterprise backbone for SSO, business continuity and disaster recovery

TrueCode Capital has integrated the YubiKey as the backbone for enterprise support, including as a means for secure single sign-on (SSO) access to its Identity Access Management (IAM) service as well for business continuity and disaster recovery—two more unique ways to use the YubiKey. Although companies set up processes to support lost YubiKeys, TrueCode Capital stores a secondary YubiKey in a locked box, providing an immediate way to support succession plans for key personnel. The YubiKey then becomes a trusted way to preserve access to accounts and to investor capital, all within a relatively short time frame. This is particularly crucial for those immature cryptocurrency exchanges that may only support a single user, making access control a top priority. It's also a crucial part of estate planning for any investor in cryptocurrency.

Unlike a mobile device that goes everywhere, the YubiKey can be locked up securely when entering a higher risk environment—a factor of importance when attending cryptocurrency events where attendees are a top target for physical device theft. Keeping a mobile device and associated YubiKeys separated while at an event or during travel adds another level of security and peace of mind.



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.

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