yubico

BeyondTrust enforces Zero Trust for privileged accounts using YubiKeys

YubiEnterprise Subscription

Learn more about YubiEnterprise Subscription.

YubiEnterprise Delivery

Learn more about YubiEnterprise Delivery.

BeyondTrust enhances security for privileged accounts using hardware-based MFA

BeyondTrust is a global leader in Privileged Access Management (PAM), developing a family of identity intelligence and access solutions that help customers across all verticals. With a vision to address the most urgent cybersecurity challenges of the day, BeyondTrust's mission is strongly aligned with Zero Trust principles that enforce continuous authentication, least privilege and adaptive access control.

Morey J. Haber is a well known voice in security as a long-time blogger, speaker and accomplished author of several books on IT security, including Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations. Haber serves as the Chief Security Officer at BeyondTrust. In the 18 years Haber has worked with BeyondTrust, digital security has shifted significantly, with privileged accounts now consistently the top target by threat actors.

"Attacks are becoming privileged-based, identity based and pretty much every report reinforces that identity is the real number one problem," notes Haber. "As a security company, we have to practice what we preach, use all of our own products, and have very strict controls on any type of privileged access within our environment."

BeyondTrust was purchased in 2018 by Bomgar and, together with two other organizations, evolved to today's leadership position in enterprise security. However, such a merger of organizations meant that the journey to Zero Trust, including getting SOC 2 and ISO 27001 certifications, required significant retooling of internal processes and infrastructure.

BeyondTrust has adopted Zero Trust architecture internally, and in its own products, and even for end users. That means that privileged accounts with elevated access to data or systems on the network, cloud or in application are hardened, removed, and monitored to reduce risk.

As part of its ongoing risk assessments, BeyondTrust identified potential weaknesses in its multi-factor authentication (MFA) strategy which relied on mobile push apps. "We started identifying problems with standard push technology like SIM-jacking and Denial of Service," notes Haber, acknowledging the susceptibility of legacy mobile authentication to phishing and targeted attacks. "We are moving our security posture away from anything that a threat actor could document, steal or guess, whether that's a password or algorithm for a key."

To combat these known weaknesses with push app technology, the Information Technology team began looking for a more secure and reliable MFA solution. BeyondTrust selected the YubiKey 5 and 5C Nano multi-protocol security keys, delivered through YubiEnterprise Delivery, Yubico's turnkey logistics and security key delivery services. The YubiKey is the only authentication technology proven to stop account takeovers at scale.

BeyondTrust

Industry
• Enterprise Security

Benefits
• Enhanced MFA for all privileged users
• Identity authentication confidence for privileged access management
• Reduced support costs
• Reinforced employee education

Protocols
• MFA
• Passwordless

Products
• YubiKey 5 & 5C Nano
• YubiEnterprise Subscription
• YubiEnterprise Delivery

Deployment info
• Enterprise-wide
• 1,500 users

> " The YubiKey complements our Zero Trust architecture and helps get us closer to Zero Trust."

Modern strong authentication secures a hybrid workforce, with a fast and easy user experience

YubiKeys were first rolled out as a pilot to the most sensitive assets in IT and InfoSec, protecting the privileged accounts that are the highest risk for any organization. After Haber's team measured, monitored and tested the effectiveness of the YubiKey to meet its security and reliability standards, the phased rollout started with executive team members and other privileged accounts with access to sensitive data.

"Once the YubiKey started to be adopted, it became a very strong case for the right way to do things to protect the organization."

The final phase of the rollout will extend the YubiKey to the remainder of the 1,500 BeyondTrust employees, the vast majority of which are considered remote, with a large portion operating hybrid between remote and office-based using mobile devices.

To better protect its remote and mobile workforce and reduce the risk of Shadow IT, BeyondTrust is replacing all legacy MFA technology that relies on passwords and push notifications with modern, secure passwordless login flows. Authentication to the device is purposefully kept separate from authentication to applications or resources, a security control used to separate user identity from privileged account identity. Employees authenticate to corporate-issued laptops, through password or integrated biometric scanner, with secondary authentication using YubiKey.

As a portable root of trust, YubiKey offers a physical and cryptographic guarantee of possession that protects the private key material against exfiltration or tampering. Further, the YubiKey reduces the risk of phishing attacks by helping remove uncertainty in the authentication flow. Since push apps send links via SMS or require a "click to allow" workflow, people may click or allow access that opens the door to cyberattack.

> " With the YubiKey, you can enforce training to 100% because you don't open or click, you're touching with your finger to validate with biometrics. We can finally say 'Don't click, don't open' and have no exceptions."
>
> Morey J. Haber Chief Security Officer, BeyondTrust

In addition to implementing the best authentication controls possible today, many organizations are experiencing a wide variety of outages associated with push app technology, leading to "floods of requests" to the support team. Push apps are dependent on cloud services and mobile carriers, leading to many points of failure, as Haber notes, from connectivity issues to carrier outages or even geopolitical disruption.

"The YubiKeys are a simpler architecture with less dependencies on push notification and cell phone vendors in order to provide a higher level of security," notes Haber. The YubiKey acts as a portable root of trust for authentication into websites, services and applications without reliance on cellular connectivity—the user simply inserts a security key into the USB port and taps to authenticate.

Optimizing return on investment with YubiEnterprise Services

Measuring the ROI of the YubiKey deployment, BeyondTrust has taken a comprehensive view that includes security, reliability, and support. In addition to reducing support costs associated with push notification failures and security risks associated with SMS notifications, BeyondTrust has taken advantage of YubiEnterprise Subscription and Delivery services to help get hardware security keys to users with the ability to upgrade form factors based on device type, user preferences or new YubiKey offerings.

" YubiEnterprise Subscription forces you to stay on top of the ball in terms of security."

The YubiEnterprise Subscription "as-a-service" model delivers unsurpassed flexibility for the foreseeable future at an optimized cost. YubiEnterprise Subscription future-proofs BeyondTrust's security investment, providing an extra stock of YubiKeys to support lost or stolen keys or company growth. With YubiEnterprise Delivery, the entire distribution process has been offloaded with turnkey delivery. Haber notes: "It's huge that we do not have to worry about inventory, shipping, tracking or delivery."

Staying ahead of a changing threat landscape with highest integrity authentication

Haber has more than 25 years of IT industry experience and has noted the increased demands being placed on organizations and the C-suite to balance digital transformation and a remote workforce with a growing threat landscape and unstable geopolitical conditions. "It's a lot harder to protect assets," notes Haber, "As a security company, there are no second chances." As Haber notes, this is a situation that could lead to a lot of sleepless nights but some of the risk can be mitigated by embracing better solutions like YubiKeys for a common problem.

" The average tenure of a CSO right now is a year and a half. I am two-and-a-half years plus—and I'm still sleeping."

What is Haber's secret to avoid sleepless nights? Staying on top of gaps and getting back to basics.

"The more things change, the more they stay the same," notes Haber, "So when you think of new technology, whether it's digital transformation, trying to adhere to cyber insurance regulations, or remote workers, it all boils back to the original 101 basics: identity, privilege and vulnerability." As the threat landscape evolves, the tools evolve using the same basic building blocks, so it is essential to get those pieces right.

One of those building blocks is provided by YubiKey: "The YubiKey solves for better identity authentication confidence. As a CSO and cyber security author of the Attack Series of books available on Amazon, this strategy is not unique. I have chosen to protect my organization and publish my strategy so that everyone, and anyone, can benefit on how to successfully secure their organization."