CYBERARK®
THE IDENTITY SECURITY COMPANY®

eBook

Secure IT Admins in Every Environment: CyberArk Customer Success Stories

Learn how customers leverage CyberArk Identity Security Platform to secure high-risk access across hybrid and multi-cloud infrastructure.

Table of contents

Introduction

With access to the most sensitive systems, tools and credentials, IT administrators are prime targets for cyberattackers seeking to exploit privileged access, infiltrate critical systems, move laterally and exfiltrate valuable data.

Legacy security models—built around perimeter-based defenses and manual access controls—can no longer keep pace with modern identity-based attacks. As organizations embrace hybrid and multi-cloud environments, adopt AI-driven workflows and manage an explosion of machine identities, a new security model is required—one that treats identity as the new perimeter.

A modern, unified identity security approach empowers IT and security teams to mitigate risk, enforce least privilege and enable resilience across hybrid and multi-cloud infrastructures—without slowing down innovation.

Whether securing critical financial systems, driving secure digital transformation in energy and logistics or simplifying compliance in highly regulated sectors, leading organizations are rethinking how they secure the identities at the center of their operations.

These are their stories.

What you'll learn in this eBook:

This eBook showcases five global organizations that have transformed their identity security strategies to meet these evolving challenges. From protecting thousands of privileged IT admin accounts to managing millions of secrets across distributed cloud environments, these companies rely on the CyberArk Identity Security Platform to:

- Centralize privileged access management for human and machine identities.
- Implement intelligent privilege controls™ and enforce least privilege at scale.
- Secure native, federated access across complex cloud infrastructures.
- Enable operational agility without sacrificing security.
- Streamline audit readiness and achieve continuous compliance.

Cisco centralizes human and machine identity security

The leading network provider leveraged CyberArk Identity Security Platform to centrally manage and secure **50,000** privileged human and machine identities and audit **40 million** API secrets calls a month across hybrid and multi-cloud environments.

The challenge

With **100,000** employees, hundreds of partner organizations worldwide and over **1,000** critical applications, Cisco lacked a unified view of privileged access. Gaps in session monitoring and audit reporting left both human and non-human identities operating without centralized governance, control or visibility into who was doing what—and when—across its hybrid and multi-cloud estate.

The solution

Cisco deployed the CyberArk Identity Security Platform—comprising CyberArk Privileged Access Manager and CyberArk Secrets Manager Self-Hosted (formerly Conjur Enterprise)—to consolidate human and non-human privileged access control and identity into a unified platform, so they can centrally audit and secure who has access to what. CyberArk platform's

Key benefits

- Consolidated human and non-human privileged access into one platform.
- Protected **50,000** privileged accounts.
- Handled **40 million** API secrets calls per month via Secrets Manager.
- Isolated and monitored more than **25,000** sessions per month.
- Recorded over **1,000** hours of privileged sessions daily.
- Enabled fast, one-click secure access to business systems.
- Established a security roadmap for future initiatives.

integrations with Cisco's Duo MFA and products from SailPoint and Saviynt, automated identity governance workflows and streamlined onboarding of users and secrets used by applications within the entire DevOps pipeline. Hosted in AWS, CyberArk Secrets Manager is now used across the enterprise-wide hybrid and multi-cloud infrastructure to manage and govern secrets. It gives DevOps engineers a simple process to replace hard-coded credentials with APIs retrieving the secrets applications needed to perform their workloads across their entire CI/CD pipeline.

Hear it from Cisco

We are very proud about what we have achieved with our program. The CyberArk Identity Security Platform helps us secure and manage human and non-human identities in a unified solution. We secure 50,000 human privileged identities, isolate and monitor more than 25,000 sessions per month, and produce more than a thousand hours of recorded sessions per day. From a secrets management perspective, we vault and rotate tens of thousands of credentials used by applications and manage more than 40 million API secrets calls a month.

Santosh Prusty
Senior Leader, Enterprise Security Team, Cisco

Read the Full Story

Coca-Cola Europacific Partners secures digital transformation by centralizing privileged access management

Coca-Cola Europacific Partners' Australian, Pacific and Indonesian operation (CCEP API) deployed CyberArk Privileged Access Manager Self-Hosted to gain a 360-degree view of privileged access activities and create a robust defense against modern identity-based threats.

The challenge

CCEP aspired to be the world's most digitized bottler, but rapid digitization also magnified cyber risk. Its API operation lacked consistent, centralized controls and visibility over elevated credentials. Manual, trust-based provisioning of privileged access and fragmented audit reporting made it impossible to enforce just-in-time access or meet PCI DSS and NIST compliance mandates.

The solution

CCEP API implemented CyberArk Privileged Access Manager Self-Hosted to improve existing privileged access management processes and gain oversight over the use of elevated credentials. Leveraging the CyberArk Blueprint

Key benefits

- Delivered **360°** visibility into all privileged access activities.
- Automated just-in-time provisioning, replacing manual, trust-based processes.
- Integrated seamlessly with SailPoint and Qualys to extend protection across identity and vulnerability lifecycles.
- Accelerated audit readiness for PCI DSS and NIST compliance.
- Reduced time and resources required to manage privileged access.
- Established a group-wide standard for privileged access management.

methodology and auto discovery DNA scans, the company rolled out controls to several hundred IT admin accounts and almost **1,000** local admin accounts even amid COVID-19 lockdowns. Tight integrations with SailPoint for identity governance and Qualys for vulnerability management automated approval workflows, enabling developers to create seamless protection across multiple attack vectors.

Hear it from Coca-Cola Europacific Partners

One measure of the effectiveness of CyberArk is that we now know how every privileged account is being used and there has been a dramatic drop in the opportunity for someone to inflict damage to our environment.

Deploying CyberArk means there are no gaps or inconsistencies in our approval process because we now have a common way of provisioning privileged access. That is a very important step forward because not only is it more secure, but it drives efficiencies.

Mukesh Kapadia
Global Deputy Chief Information Security Officer, CCEP

Read the Full Story

Konoike Transport strengthens identity security posture by 200%

The transport company leveraged CyberArk Privilege Cloud to centralize privileged access management across its hybrid IT environment, enhancing security visibility, reducing operational burdens and improving audit response.

The challenge

Konoike Transport had strengthened its privileged access management in the past through manual operations, but the burden on the field teams and lack of visibility into privileged activities became an issue. The company operates a wide range of systems and servers, and each person in charge had to manage their privileges, which was an old-fashioned practice. Since some systems were operated under shared accounts, failure to change passwords after the person in charge was transferred or left the company could lead to a serious incident. Strengthening both processes and systems became essential to mitigate these vulnerabilities.

Key benefits

- Achieved a **200%** improvement in identity security posture.
- Centralized management of privileged access across hybrid IT environments.
- Enhanced visibility into privileged activities, reducing risks of internal fraud and errors.
- Streamlined audit processes and improved compliance readiness.
- Reduced operational workload on IT teams through automation and ease of use.
- Established a scalable foundation for ongoing digital transformation initiatives.

The solution

After evaluating multiple vendors, Konoike Transport selected CyberArk for its robust capabilities in securing privileged access across complex IT environments. Two key features stood out:

- **Centralized credential management:** CyberArk Privilege Cloud enabled the organization to onboard all privileged accounts into a tamper-proof Digital Vault, apply consistent policy-based controls and automate password rotation, reducing the risk of credential misuse.
- **Comprehensive IT admin security:** As Konoike Transport shifts to a cloud-first strategy, CyberArk's ability to centrally secure privileged access for IT admins and privileged users across on-premises, multi-cloud and hybrid environments was a critical advantage.

Hear it from Konoike Transport

The initial goal was to strengthen security measures by implementing privileged access management. With CyberArk Privilege Cloud, we exceeded our security expectations by approximately 200%.

Since 2018, we have been working on implementing measures against external security threats and fraud first, and then strengthening measures for internal fraud. Privileged access management was one of our key challenges when it comes to internal measures. We believe that measures to secure privileged access management has been taken by implementing CyberArk which has the latest technologies, such as AI. We look forward to a continued long-term partnership with CyberArk.

Masaya Sato
Deputy Executive General Manager, ICT Promotion Division and Digital Transformation Promotion Department, Konoike Transport

Read the Full Story

RBL Finserve leverages identity security to strengthen security posture and simplify audit readiness

The leading financial institution uses intelligent privilege controls to protect customer data and secure the systems and processes that power financial access for millions of households and businesses.

The challenge

RBL Finserve operates a dynamic and expanding IT infrastructure to deliver innovative, personalized financial services to customers. As the business evolved—driven by increased cloud adoption, remote work and third-party outsourcing—new threat vectors emerged that traditional perimeter-based security could no longer defend against. With sensitive financial data at stake and a growing dependence on external partners, the organization needed to modernize its security posture and make identity security the center of its cybersecurity strategy.

The solution

To address these challenges, RBL Finserve partnered with CyberArk to deploy a modern identity security architecture that could scale with its

Key benefits

- Strengthened cybersecurity posture to defend against modern threats.
- Reinforced customer trust by safeguarding sensitive financial data.
- Improved operational efficiency with streamlined access and identity governance.
- Simplified audit readiness with centralized visibility and advanced privileged controls.
- Laid a scalable foundation for future identity-based security initiatives.

evolving infrastructure. Using the CyberArk Identity Security Platform, the company implemented foundational privileged access controls, such as isolating and monitoring privileged sessions and enforcing automated credential rotation, to protect IT administrators and critical systems. To enhance user experience while enforcing strong security practices, RBL Finserve implemented CyberArk Single Sign-On (SSO) and adaptive multi-factor authentication (MFA).

These solutions empowered users with seamless access to target systems while maintaining stringent back-end protection. The result was a secure, unified approach that not only improved internal adoption but also set the stage for broader expansion of intelligent privilege controls across all identities, including workforce users, IT admins, developers and third-party vendors.

Hear it from RBL Finserve

The results speak for themselves – a robust cybersecurity framework centered on identity security has set a new benchmark for digital trust and safety. Our proactive measures protect our business and reinforce the foundation of trust that RBL Finserve is built upon.

S K Mohanty
Chief Information Officer, RBL Finserve

Read the Full Story

Matrix42 boosts cybersecurity productivity by 25% with identity-centric security

German IT services leader improves security management, reduces privileged account complexity and achieves rapid time-to-value with the CyberArk Identity Security Platform.

The challenge

Matrix42 needed a more secure and scalable way to manage privileged access across its cloud-based infrastructure and PaaS environments. Despite a strong foundational cybersecurity posture—backed by Azure's native security tools and 24/7 SOC monitoring—the company identified critical gaps in safeguarding privileged identities. Existing tools, including a basic password manager, lacked the control and visibility to manage privileged access.

A key challenge was managing local admin access for developers and engineers. Permanent privileges increased security risk, but removing them risked slowing down productivity. The company needed a modern, efficient way to secure privileged identities—without disrupting day-to-day operations.

The solution

Matrix42 turned to the CyberArk Identity Security Platform to take control of privileged access across its hybrid infrastructure. The initial rollout focused

Key benefits

- Improved privileged access management across hybrid environments.
- Achieved full time-to-value in six weeks.
- Boosted productivity by 25% in managing privileges.
- Reduced the number of privileged accounts and local admin accounts by 20%.
- Avoided costly investments in data center and infrastructure resources.

on securing high-risk privileged accounts used by developers and IT. Admin support staff and analysts—users with less technical expertise—were also onboarded, benefiting from CyberArk's seamless access experience.

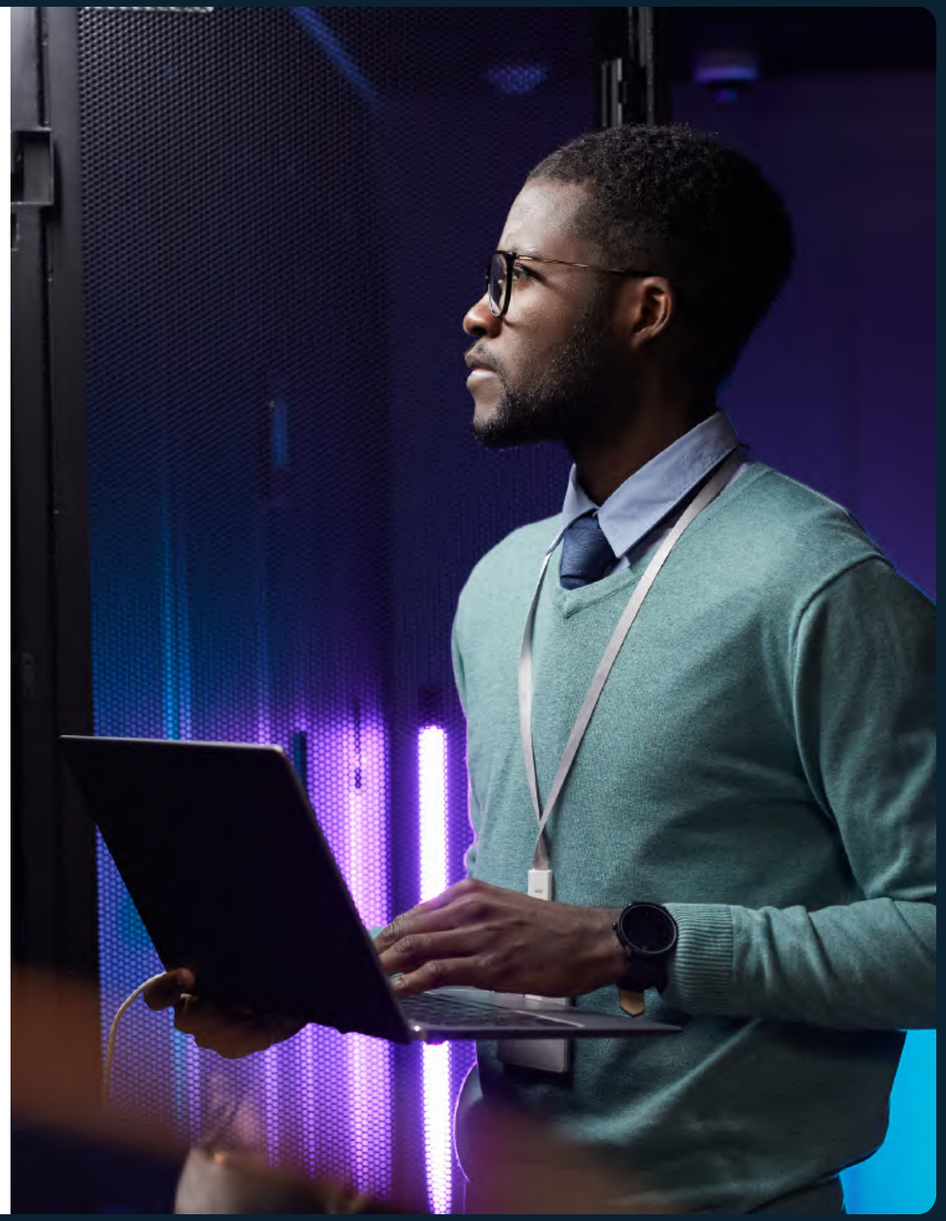
To eliminate excessive endpoint privileges, Matrix42 used CyberArk Endpoint Privilege Manager (EPM) to audit user behavior and identify actual application usage. The audit insights enabled the company to establish precise privilege elevation policies that maintained user productivity while significantly reducing risk. Matrix42 now protects privileged accounts across both Azure and on-prem environments.

Hear it from Matrix42

At Matrix42, CyberArk improves privileged access management (PAM) and is an important part of the company's journey towards an identity-centric security posture. Matrix42 needs to fulfill its business operations securely and CyberArk helps do that efficiently. Our customers expect professional, high-quality privileged access management. Before, we spent ages explaining the actions and processes used, now we just say we use CyberArk, and it is a two-minute discussion.

Thomas Langholz
Director, Information Security, Matrix42

Read the Full Story



Conclusion

As the identity threat landscape continues to explode, one thing is clear: securing privileged access is foundational to protecting modern enterprises. IT administrators, with their elevated access and critical responsibilities, remain a primary focus for attackers—and an essential priority for defenders.

CyberArk Identity Security Platform empowers organizations to protect every identity —human and machine—across on-premises, hybrid and multi-cloud environments with the right level of privilege controls. The result: reduced attack surface, complicated lateral movement and improved operational efficiency.

Ready to modernize your privileged access management program?

Request a Demo

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in identity security, trusted by organizations around the world to secure human and machine identities in the modern enterprise. CyberArk's AI-powered Identity Security Platform applies intelligent privilege controls™ to every identity with continuous threat prevention, detection and response across the identity lifecycle. With CyberArk, organizations can reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities, including workforce, IT, developers and machines, to securely access any resource, located anywhere, from everywhere. Learn more at cyberark.com.