# Using Delinea to Enhance Cybersecurity, Streamline Compliance, and Reduce Costs

## ✓ Challenges

Boyner's IT environment is wide and varied, supporting customer information, employee information, 3rd party provider and supplier information, e-commerce, and mobile applications. The organization wanted to make sure they were in the best position to protect sensitive and regulated data and secure privileged accounts — including those that rely on remote access. Some of the challenges the organization faced included:

- Reducing risk from unauthorized account access
- Establishing and maintaining password security
- Supporting identity security for 3rd parties
- The need to automatically discover legitimate accounts

### Identity Security Challenges

From the Boyner perspective, Privileged Access Management (PAM) represents one of the most substantial areas of cybersecurity risk, given the large potential attack surface area it presents: Without a secure and comprehensive approach to PAM, unsecured user accounts may be relatively easily exploited by malicious actors. Not only does this attack vector raise serious concerns regarding compliance with various industry standards and regulations, but Boyner has found statistical security data that also highlights its prevalence as a primary factor for breaches. As a result, a key part of Boyner's cybersecurity mission is to recognize the importance of securing account management processes and to proactively and effectively mitigate these risks.

## Background

Boyner is a leader in Turkey's retail and fashion industry and is comprised of 6 distinct brands. It includes more than 250 department stores, with e-commerce websites, mobile applications, and a workforce of over 8,000 employees. Their focus is on working for the unconditional happiness of millions. Boyner brings innovative brands and vision together with dynamic and vibrant department stores to provide customers with a unique shopping experience. Boyner works continuously to create a positive impact on society and the environment. Boyner has a complex IT environment, and the organization wanted to take steps to support compliance requirements, the full lifecycle of password security, and the protection of privileged accounts, to help protect its customers and its brand.

**BOYNER**

As a starting point, the Boyner CISO particularly wanted to focus on establishing and maintaining password security in a secure vault (the classic Privileged Access Management — or PAM — use case), combined with the ability to provide secure and controlled third-party remote access to monitor, record, and analyze those activities to protect the business.

### Compliance Challenges

The Boyner believes supporting compliance requirements is key to enhancing  operational effectiveness. To that end, the organization needed to align with ISO 27000 standards, as well as with the local compliance procedures established by Boyner. The ability to create this alignment will help ensure that the company not only meets international quality benchmarks, but also enables it to support local regulations, such as ISO 27K KVKK, which is the Turkish version of the European Union's General Data Protection Regulation (GDPR).

Additionally, there is a need to establish clear industry standards that can serve as a reference point for best practices within the sector. By achieving this alignment and developing comprehensive industry standards, Boyner will be able to improve its overall compliance framework, better protect sensitive and regulated data, and better position itself in the marketplace.

# Boyner saw a 40% reduction in time and cost associated with managing privileged accounts, and they also experienced a 60% reduction in the effort so support compliance efforts.

## ✅ Solution

After a thorough investigation, to help address these identity security and compliance challenges, the Boyner CISO decided have his team deploy Delinea Secret Server, together with Delinea Privileged Remote Access.
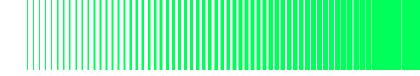
### Secure vaulting

Boyner uses Delinea Secret Server to help improve visibility into and control over how privileged admins are accessing accounts and information. Secret Sever is used to understand and efficiently track changes in the environment, improve visibility and oversight, and improve response times when issues or inconsistencies arise.

### Secure privileged remote access

To complement the secure vaulting capabilities provided by Secret Server, Boyner also deployed Delinea Privileged Remote Access to address vulnerabilities and risks associated when third parties (such as vendors, suppliers, consultants) access the Boyner environment. The solution is used to monitor, record, and analyze activities related to third party access, to better secure the business.

### Differentiating architecture

Boyner is using Delinea Secret Server and Delinea Privileged Remote Access on the Delinea Platform, which supports a Software-as-a-Service (SaaS) deployment model with shared services. Managing their identity security technology through a cloud platform offers several advantages — primarily by improving output while reducing hardware costs and eliminating the management and security expenses associated with the systems. Since the solution runs on cloud, the Boyner team no longer needs to worry about various hardware requirements and scalability, and also no longer needs to deal with patching. With these obstacles removed, the security team can focus more on identity security and protecting the business.

## ✅ Results

Boyner found that Delinea provided uniquely strong discovery features and a simpler, easy-to-use user interface than other solutions in the market. By using Delinea Secret Server and Privileged Remote Access on the Delinea Platform, Boyner has been able to improve security controls, empowering their security team to take clearer action more quickly than before. Ultimately, this helps Boyner manage and **resolve vulnerabilities in less time and reduce the cost of managing infrastructure, as well as reducing the cost of security operations.** Some of the resulting benefits of using Delinea include:

- **›40% reduction in the time and cost** associated with managing privileged accounts

- **Significant decrease in incidents** related to the misuse of privileges

- **30-50% reduction in time spent controlling user activity across systems**, enabling improved efficiency of investigations and incident response

- **60% reduction in the effort needed to support compliance efforts** and enhanced audit readiness

The immediate impact of deploying the Delinea solutions has been that the Boyner security team feels confident in their approach to identity security and can measure their progress. The organization has significantly enhanced its security visibility, which has led to a noticeable improvement in the overall quality of its PAM-related security operations. This increase in visibility allows for better monitoring and detection of potential threats, ensuring a more proactive approach to risk management and response. As a result, security operations at Boyner are now more efficient and effective, contributing to a safer environment for everyone.

Based on their success with Delinea thus far, Boyner plans to expand their Identity Security efforts in the future to enhance endpoint security and manage authorized accounts effectively.

# Delinea