CASE STUDY (Core Security)

Global Manufacturing Client

Background

This Core Security customer is a leading global manufacturer and exporter of hightech equipment, employing more than 150,000 staff across the world.

The company has always embraced information technology for competitive advantage, and the company has built a world-class IT organization that prides itself on delivering superior quality of service and application availability to its employees, business partners, and customers, even while enforcing stringent security policies that protect its network resources.

Prior to implementing a solution, the company's corporate help desk responded to, on average, 15,000-20,000 support calls each month from employees and contractors requesting forgotten or expired passwords to be reset on its numerous enterprise systems, applications, and intranet Web portals.

At times, this volume reached 40,000 calls per month and averaged $21 per call. Resolving these requests manually was both costly and time-consuming, given the strict requirements that every caller must be properly authenticated, and that detailed support tickets must be created within the Remedy Help Desk system to ensure complete, accurate audit trails for all password reset activities. Call resolution, which often took up to 10 minutes depending on which system passwords needed to be reset, could be further delayed by the fact that help desk staff did not always have the authority to reset passwords on all systems. As a result, more time was needed to manually notify and gather the people who were needed to reset different system passwords.

Relaxing password strength or the frequency of password expiration was not an option given the company's strict security policies. Enterprise-wide single sign-On was not an option due to its complexity, the wide variety of systems implemented, and the security requirement that different

OVERVIEW

With the help of Core Security's Password Management, the IT staff at this global manufacturing customer has achieved its goals of reducing the costs of managing access and authentication for its large community of end users, improving productivity through self-service and user support responsiveness, enhancing overall password security and adhering to audit compliance requirements. Key results include:

+ Reduced monthly help desk calls, delivering cost savings of more than $70k per month
+ Cut password reset resolution times for internal systems from 10 minutes to less than 60 seconds
+ Cut password reset resolution times for Partner Network from 2 days to less than 60 seconds
+ Enforced stronger passwords in conjunction with security policy, without relaxation of reset frequency

> *"Core Security's Password Management has all of the selfservice password reset, support staff reset, and password synchronization capabilities we were looking for, so the decision to implement it enterprise-wide was an easy one."*
>
> **—VP and Support Systems Manager**

passwords be used on some systems to protect particularly sensitive data. In addition, the company had introduced its Partner Network to provide online services and information to its remote employees and customers. The Partner Network, which also includes the customer portal, is also protected by usernames and passwords, and the IT staff realized that password-related lockouts would be even harder to resolve, and could negatively impact customer service.

The Approach

The IT staff set out to find a solution that could securely automate the entire password reset process, consistently enforce password policies, reliably authenticate users, satisfy extensive auditing requirements, and provide out-of-the-box connectors that could accommodate the wide variety of legacy and Web-based systems and applications.

The Result

Reducing User Support Costs and Improving Service Quality

More than 375,000 employees, contractors, business partners, and customers now have access to Core Security's Password Management for self-service password automation. On average, the solution automates between 40,000 and 50,000 password resets month. In October 2006, Core Security's Password Management reached a new high point by resetting more than 100,000 passwords. Approximately two-thirds of the monthly support calls are completely eliminated as a result of end users utilizing its self-service Web and Telephone (IVR) password reset interfaces. The remaining third are automated through the solution's Support Staff interface, which enables help desk administrators to automate the authentication, password reset, and auditing steps for increased efficiency and security. The company is realizing significant cost reduction as a result of this call avoidance and call automation.

In addition to the hard dollar cost savings, end users are more productive, because they can now use Core Security's Password Management to reset their own passwords 24x7x365, usually in less than 60 seconds. Users of the Partner Network, who sometimes experienced 2-day waits for password reset while resources across multiple time zones were coordinated and identities were validated, also notice the dramatic improvement in service quality.

Enforcing Security Policies and Synchronizing Passwords

Critical to the success of Core Security's solution at the company has been its ability to manage passwords and enforce strict security policies across a wide range of IT systems, even when policies differ per system. Core Security's password policy engine enables IT staff to construct different password policies for individual systems, or group systems together to share a common policy using Core Security's Selective Synchronization features. During the password reset process, end users can select a group of systems for reset, and Password Management automatically synchronizes the passwords on each of the grouped systems in real time.

Ensuring Audit Trails with Remedy Integration

The Remedy Help Desk system, which tracks all password change requests, is highly complex – the schema changes frequently, and over 100 fields are required for each ticket that is opened. The company relies on to Core Security's Service Link technology, which provides bi-directional API-level integration with Remedy, to automate the opening, updating, and closing of Remedy trouble tickets for all password activities.

Core Security's Password Management enforces the data types of the Remedy schema, and ensures that all fields are accurately filled out through its custom macro facility, which captures user, managed system, network, and other environment data as part of each Remedy ticket.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.