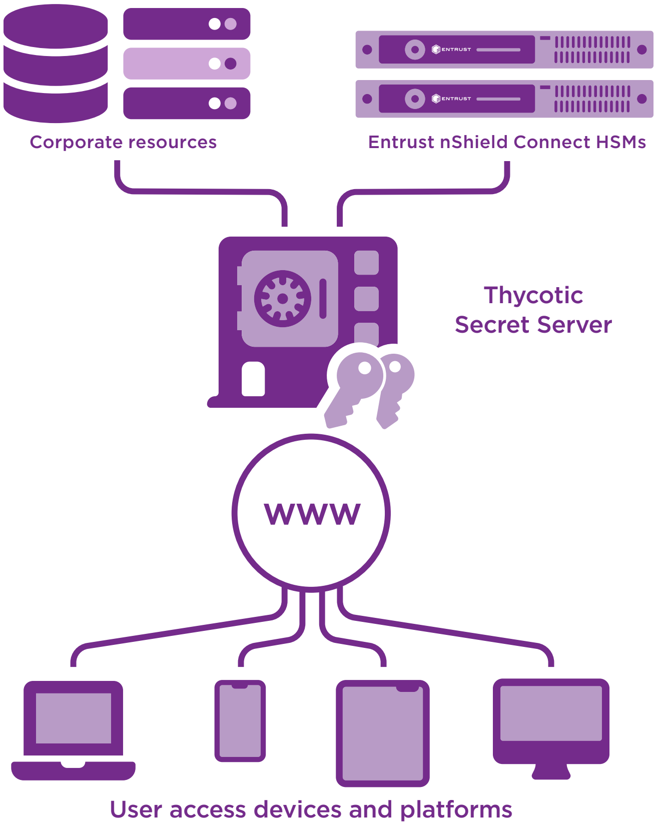
Entrust and Thycotic Bolster Security of Privileged Access Management

Integrated solution provides added layer of protection

HIGHLIGHTS

- Secure privileges for service, application, root, and administrator accounts across your organization on premises or in the cloud
- Run solutions for privileged account discovery, turnkey installation, and out-of-the-box auditing and reporting tools
- Manage multiple databases, software applications, hypervisors, network devices, and security tools, even in large-scale, distributed environments
- Protect cryptographic keys used to access privileged access credentials within a tamper-resistant FIPS and Common Criteria certified Entrust nShield® hardware security module (HSM)
- Facilitate auditing and compliance with data security regulations


Corporate resources
Entrust nShield Connect HSMs
Thycotic Secret Server
WWW
User access devices and platforms

Entrust nShield Connect HSMs provide an additional layer of protection by controlling the encryption key used by the Thycotic Secret Server to secure access credentials.

LEARN MORE AT ENTRUST.COM

Entrust and Thycotic Integrated Solution

The Problem

Privileged user accounts are a top target of cybercriminals seeking access to enterprise IT systems and sensitive data.

Attacks on IT infrastructures target privileged user account credentials. These credentials are highly attractive to attackers because a compromise can open an easy path to an organization's most sensitive information. Privileges can also be abused to gain access to more accounts, and compromised credentials can go undetected for an extended period because the attacker appears to be a trusted user.

The Challenge

Privileged account credentials need to be encrypted and further secured by high assurance protection.

Organizations establish privileged accounts for highly trusted individuals. These accounts provide unique access and privileges based on the roles and responsibilities of the trusted individuals. For example, a privileged user might be able to upgrade an operating system, add or remove software, or access files and directories that are inaccessible to typical users.

Because cyberattacks frequently target privileged accounts, organizations require full control over privileged account credentials, including the ability to audit their use, impose automatic time restrictions, and instantly revoke access as needed. Such capabilities are not available when managing privileged credentials via spreadsheet or other manual processes. Encrypting privileged account credentials protects them from unauthorized access. Securing the underpinning cryptographic keys used to encrypt these credentials is critical to protect from attacks.

The Solution

Thycotic's Secret Server privileged access management solution fortifies security by integrating Entrust nShield HSMs to secure underpinning encryption keys.

Thycotic's Secret Server simplifies detecting, controlling, changing, and auditing privileged accounts across the organization. The solution gives security and IT teams the agility to secure and manage all types of privileges, protecting administrator, service, application, and root accounts from cyber-attack. Secret Server enables rapid deployment and gives enterprises direct control to customize as they grow. Organizations can strengthen their IT security, protect their data within global governance requirements, and scale across on-premises and cloud systems as their requirements change.

To achieve the highest assurance protection, Thycotic's Secret Server integrates Entrust nShield Connect HSMs to protect the root encryption keys. nShield HSMs offer FIPS 140-2 Level 3 and Common Criteria EAL 4+ protection for the keys that protect privileged account credentials. The combined solution provides an added layer of security that protects privileged credentials and the access they unlock for authorized privileged users.

Entrust and Thycotic Integrated Solution

A Closer Look

Why use nShield HSMs with Thycotic's Secret Server?

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. They are specifically designed to safeguard and manage cryptographic keys and processes within a certified hardware environment to establish a root of trust.

Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can compromise confidential information. Entrust nShield HSMs, offered as an appliance deployed at an on-premises data center or leased through an as-a-service subscription, provide enhanced key generation, signing, and encryption to protect sensitive data and transactions. Using HSMs as part of an encryption and/or key management strategy is considered a best practice among cybersecurity professionals.

Integration of Entrust nShield HSMs with Thycotic's Secret Server:

- Secures keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensures availability by using sophisticated key management, storage, and redundancy features to guarantee keys are always accessible when needed
- Delivers high performance to support increasingly demanding transaction rates
- Complies with regulatory requirements for public sector, financial services, and enterprises

Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys. For more information visit entrust.com/HSM.

Thycotic

Thycotic is a global leader in privileged access management, a critical layer of IT security that protects an organization's data, devices, and code across cloud, on-premises, and hybrid environments. The company's modern cloud-ready solutions dramatically reduce the complexity and cost of securing privileged access, providing more value and higher adoption than any alternative. Thycotic is trusted by over 12,500 leading organizations around the globe, including 25% of the Fortune 100. For more information visit thycotic.com.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com **entrust.com/contact**