

«Thales eSecurity»

SAFEGUARDING DATA WITH PRIVILEGED USER ACCESS CONTROLS





The Challenge

Over the course of the past few decades, computing architectures, security approaches, and security threats have all changed radically. However, over that time, a common security gap has persisted: the risks posed by administrative access privileges.

In order to carry out their responsibilities, administrators need the permissions required to execute such tasks as software installation, system configuration, user permission management, resource allocation and more. Through this access, administrators virtually always also have access to the data and services that run on the systems they manage. Further, teams of administrators have often shared their administrative credentials. While this facilitated easier distribution of workloads, it also made it difficult to assign specific activities to a specific individual—and so to hold anyone accountable for a policy violation or breach.

While this security gap is nothing new, it is one that has grown increasingly critical to address. In recent years, virtually all servers and equipment an organization relies on have grown increasingly

interconnected, both with other internally managed systems as well as external networks and equipment. With the increasing adoption of virtualization, cloud services and big data implementations, new layers of administration—and of administrative privileges—also are added that potentially expand the risk.

Administrative privileges have left many organizations exposed to these threats:

- **Insider abuse.** It is often easy for malicious insiders to abuse their privileges, whether to make money or sabotage the business. These risks are exacerbated in the cloud, where organizations may be exposed to the threat of their own administrators, as well as those of the cloud provider.
- **External attacks.** Administrative privileges represent a vital asset, and one that is increasingly targeted by external attackers. For example, an advanced persistent threat (APT) attack may use social engineering tactics to gain one administrator's credentials, and use that as a launching point to access and exploit other systems and services.

> Vormetric Transparent Encryption

GUARDING AGAINST ABUSE OF PRIVILEGED USER CREDENTIALS

With Vormetric Transparent Encryption, you can effectively guard against the abuse of privileged user access. Vormetric Transparent Encryption provides comprehensive, robust and granular controls, operating at the file system and volume level. The solution features capabilities for data-at-rest encryption, key management and privileged user access control.

Vormetric Transparent Encryption also provides detailed data access audit logs and capabilities for seamlessly integrating this intelligence with security information and event management (SIEM) systems. Through the solution's centralized policy and key management, customers can address security policies and compliance mandates across databases, files and big data nodes—whether they're located in the cloud or in virtual or traditional infrastructures.

Vormetric Transparent Encryption delivers critical capabilities that protect against the abuse of privileged user permissions.

STRONG PROTECTION FOR DATA

The combination of Vormetric's encryption + policy-based access controls allows privileged users to perform their work without exposure to data. Logs capture details of access for intelligent pattern analysis and alerting.

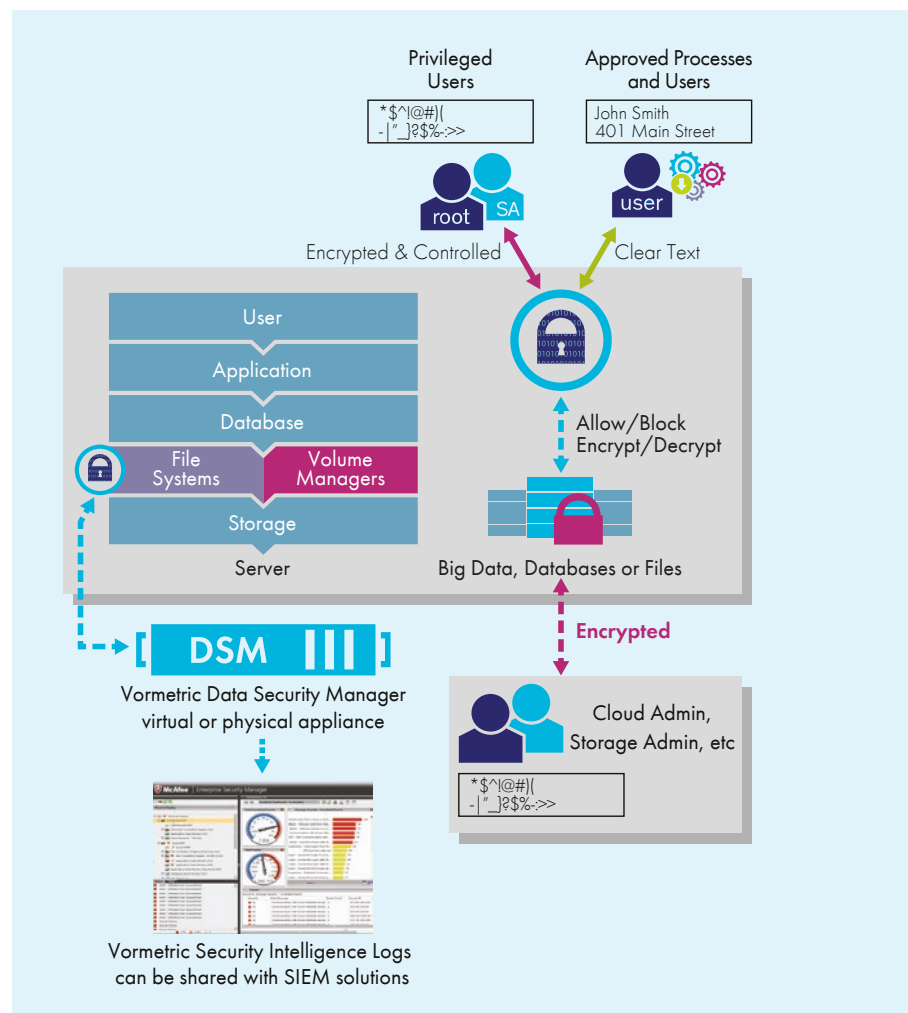


Figure 1: The Vormetric Transparent Encryption enables privileged users to do their jobs, and never see protected data.

SEPARATION OF PRIVILEGED USERS AND SENSITIVE USER DATA

Security administrators can create a strong separation of duties between privileged administrators and data owners. Files can be encrypted, while leaving their metadata in the clear. This enables IT, hypervisor, cloud, storage and system administrators to perform their responsibilities, without being able to gain access to the sensitive data residing on the systems they manage.

SEPARATION OF SECURITY ADMINISTRATION DUTIES

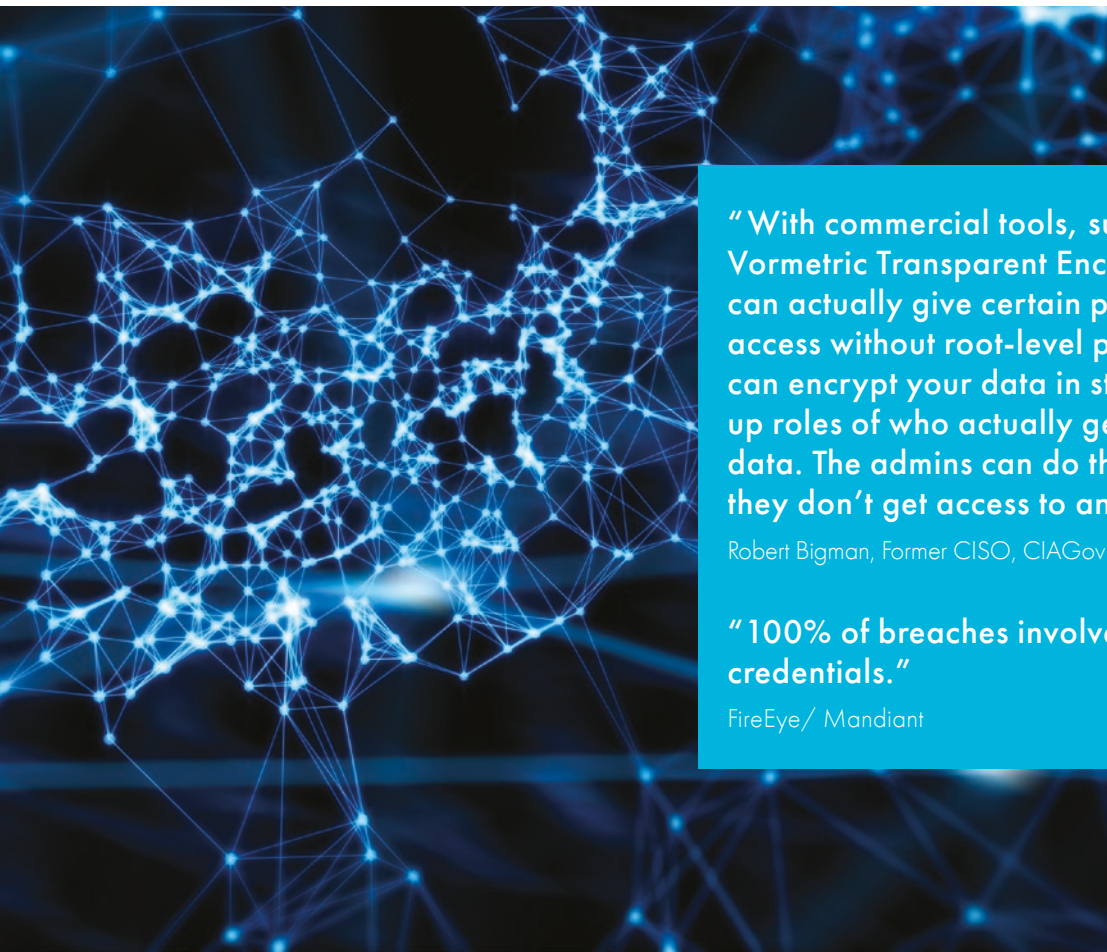
Strong separation-of-duties policies can be enforced to ensure that security administrators do not have complete control over data security activities, encryption keys or administration. In addition, the Vormetric Data Security Manager (DSM), which controls policy and key management for Vormetric Transparent Encryption, supports two-factor authentication for administrative access.

GRANULAR ACCESS CONTROLS

In addition to encryption and key management, the solution can enforce very granular, least-privileged user access policies, enabling protection of data from multi-phase attacks and misuse by privileged users. Specific policies can be applied by user, process, file type, time of day and other parameters. Enforcement options are very granular; they can be used to control not only permission to access clear-text data, but what file-system commands are available to a user.

SECURE, RELIABLE AND AUDITABLE KEY MANAGEMENT

The solution provides extensive audit capabilities that can be used to report on all activities relating to key usage, including key generation, rotation, destruction, import, expiration and export.



“With commercial tools, such as Vormetric Transparent Encryption, you can actually give certain people certain access without root-level privileges. You can encrypt your data in storage to set up roles of who actually gets to see the data. The admins can do their jobs, and they don’t get access to any data files.”

Robert Bigman, Former CISO, CIAGovInfoSecurity

“100% of breaches involved stolen credentials.”

FireEye/ Mandiant

DETAILED DATA ACCESS AUDIT LOGS

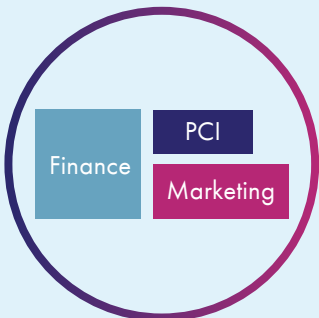
Vormetric Transparent Encryption provides detailed logs that report on process and user access to protected data. The logs specify when users and processes accessed data, under which policies and if access requests were allowed or denied. Through these logs, administrators can identify when a privileged user submits a command like “switch user” in order to attempt to imitate, and potentially exploit, the credentials of another user. Logs also track security administrators’ actions performed on the DSM.

ENHANCED INTELLIGENCE THROUGH SIEM INTEGRATION

Sharing the solution’s granular logs with a SIEM platform helps uncover anomalous access patterns that may indicate an attack is in process. For example, a process may suddenly access much larger volumes of data than normal, or an administrator may attempt an unauthorized download of files. These events could point to an external attack that has not yet been detected or malicious insider activities. The solution features pre-packaged dashboards in leading SIEM systems that provide intuitive, immediate insights into security status and trends. Should unauthorized access attempts be detected, the solution can provide automated alerts.

PRIVILEGED USER ACCESS CONTROL IN HADOOP

Vormetric Transparent Encryption’s file- and folder-level access controls can be applied to data and name nodes within Hadoop clusters. These controls enable Hadoop administrators and Hadoop Distributed File System (HDFS) users to establish encryption zones and multi-tenancy within the data lake environment, and each zone can have its own unique access policies and encryption keys.



The diagram shows a large purple circle containing three colored boxes: a blue box labeled 'Finance', a dark blue box labeled 'PCI', and a pink box labeled 'Marketing'. To the right of the circle, there are two lists of text.

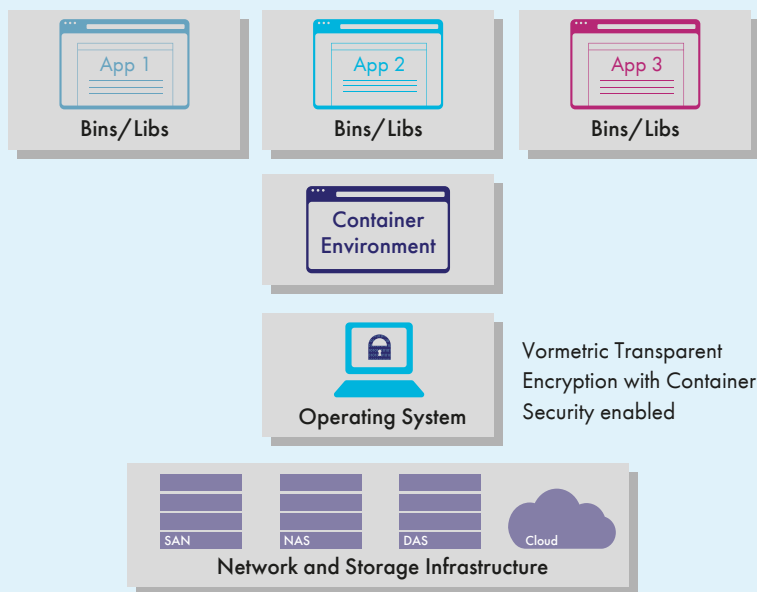
Zone Advantages:

- > Isolate groups
- > Improve security
- > Support compliance
- > Surgical encryption

Zone by:

- > Users
- > Groups
- > Folders

Vormetric Transparent Encryption enables the creation of encryption zones and multi-tenancy support for a hadoop data lake.



PREVENTING ABUSE BY PRIVILEGED USERS WITHIN CONTAINER ENVIRONMENTS

Container technologies are powering business-critical applications for established enterprises and industry disruptors alike, but like other innovations also come with unique risks to data. The potential for violation of compliance requirements, privileged user abuse and cross container data access are critical problems for sensitive data when using containers. Supporting both Docker and OpenShift container environments, Vormetric Container Security adds encryption, data access controls and data access audit logging for information stored within containers, or accessed from containers, that can mitigate these risks with appropriate security controls.

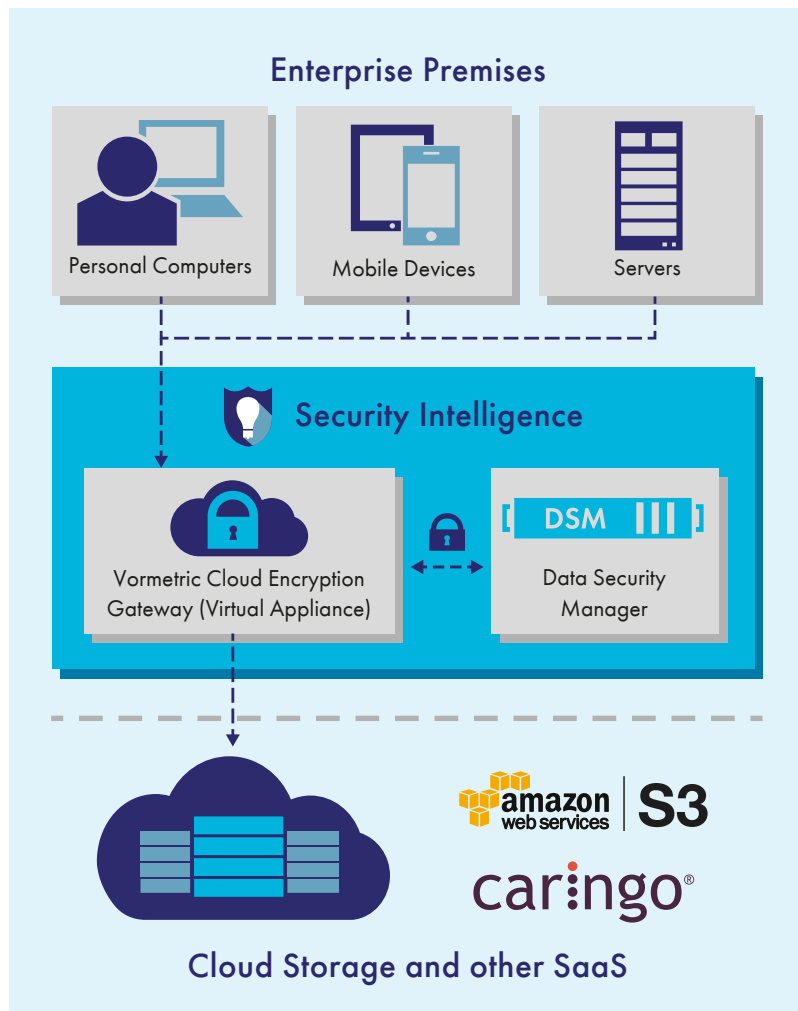


Vormetric Cloud Encryption Gateway

EXTENDING PRIVILEGED USER ACCESS CONTROLS TO AMAZON S3-COMPATIBLE CLOUD STORAGE ENVIRONMENTS

The Vormetric Cloud Encryption Gateway offers encryption and access controls for data stored within Amazon Simple Storage Service (S3)-compatible cloud storage environments. The solution provides LDAP-based group access controls that effectively limit access by

privileged users within the organization. In addition, by enabling enterprise security teams to control encryption keys, the solution can exclude access from outside the enterprise, including from cloud storage provider's privileged users.



“Separation of duties through Vormetric’s policy-based encryption features have allowed us to guarantee the autonomy of encrypted data, even if support staff have system administrator or privileged user capabilities. This in turn has contributed to our efforts in attaining compliance with several of the ISO 27000 series of standards.”

Justin Knowles, director of information technology and security, Bridgeway Software, Inc.



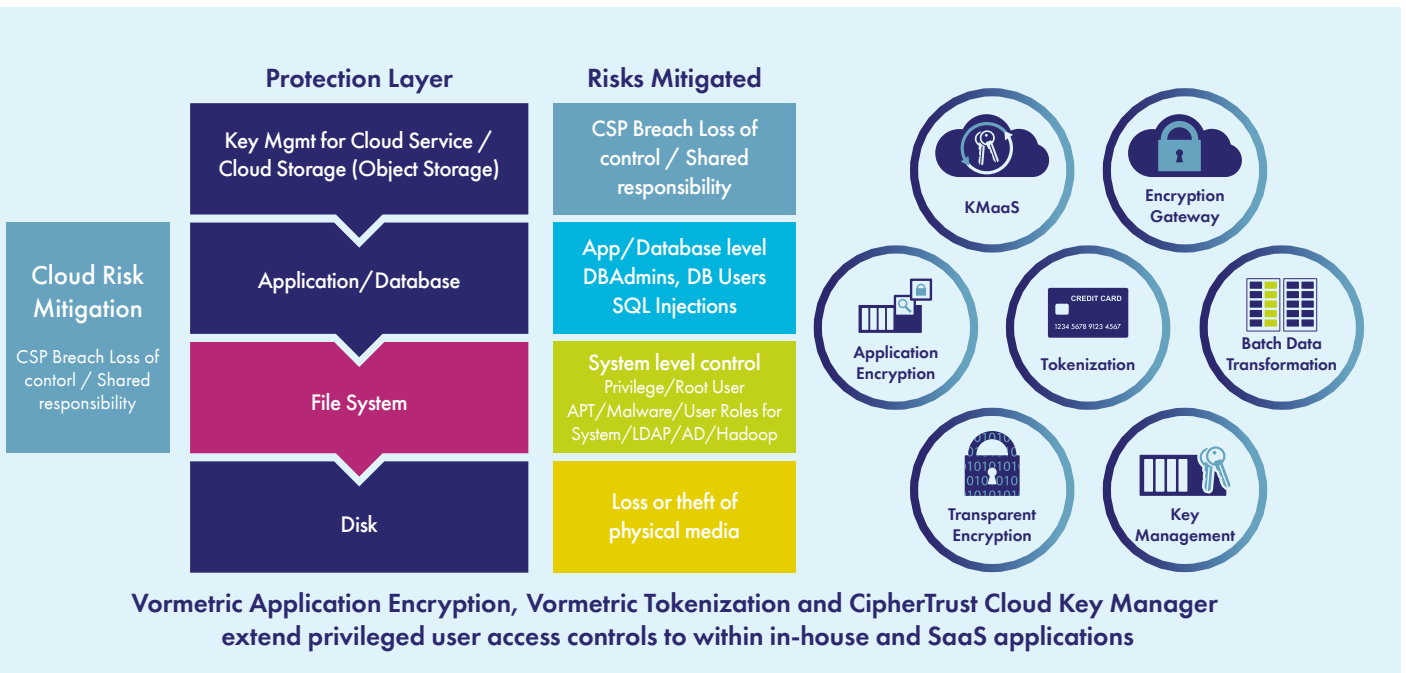
Additional platform capabilities

VORMETRIC APPLICATION ENCRYPTION, TOKENIZATION AND KEY MANAGEMENT AS A SERVICE (KMAAS) PROVIDE ADDITIONAL CAPABILITIES FOR PROTECTION AGAINST PRIVILEGED USERS

Vormetric Application Encryption and Vormetric Tokenization add capabilities to control access based on user roles, but with a difference: Developers are in control of what data is encrypted or anonymized using tokenization and who will have access to the information. Once implemented, this provides not only all the protection found at the file system level by Vormetric Transparent Encryption and the Vormetric Cloud Encryption Gateway, but also protects within the application.

Access can be controlled based on roles and users defined within the application environment - including database or application administrations and other privileged users within the application environment.

Finally, CipherTrust Cloud Key Manager extends these controls into SaaS, PaaS and IaaS environments, managing encryption keys for Salesforce, Azure and other online environments that exclude access by cloud environment privileged users to enterprise data.



About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

