Safeguarding Data with Privileged User Access Controls

The Flaw in the System

Since the introduction of multi-user computer systems over 40 years ago, there has been a fundamental flaw in their security architecture. The flaw? - The concept of a Root User, Domain Administrator, System Administrator or other high level computer operator – and their data access rights. These users have always had access to every aspect of a system – software installation, system configuration, user creation, networking, resource allocation and more, as well as access to all the data associated with the system.

These accounts exist because of the need for system maintenance and management. But, as systems have become more closely interlinked and with increasing amounts of private and confidential data accessible to them, there is increased risk from privileged user accounts.

Compounding this are the ways that many enterprise IT departments have traditionally done business, and the advent of new technologies and threats:

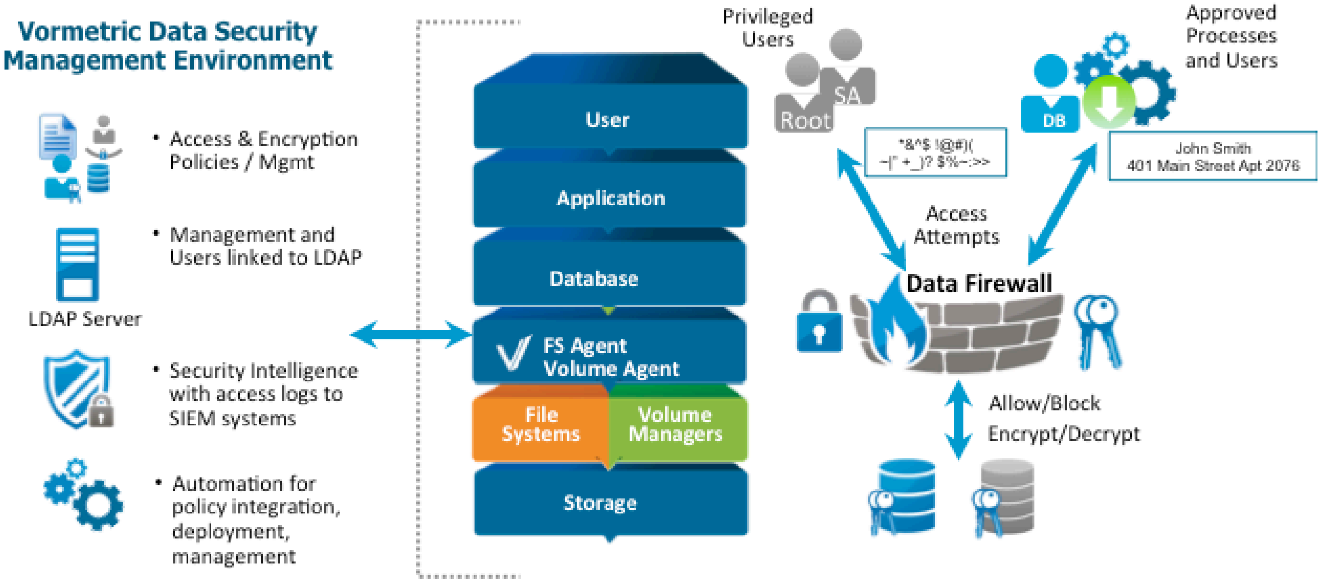
- **Rights too broadly assigned –** Superuser privileges are often assigned to DBAs, application developers, SysAdmins and others that don't have a real "need" for this level of access to private and confidential data.
- **Sharing of privileged accounts –** Traditionally, many IT departments allowed unrestricted sharing of privileged user accounts (logins and pass words), leading to a loss of personal accountability.
- **Cloud, virtualization and big data expand the threat -** With each new technology layer used as part of system deployment and management new privileged user roles are created.
- **Advanced Persistent Threat (APT) attacks target privileged accounts** –Attackers have now found that if you want access to everything, you want to compromise privileged user accounts and their system and data access rights. Though they may initially enter through less sensitive accounts – privileged user credentials are a primary target.

> "With commercial tools, such as Vormetric, 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 at the CIA-GovInfoSecurity – June 21, 2013

> "I've been a systems engineer, systems administrator … When you're in positions of privileged access like a systems administrator for the intelligence community, you're exposed to a lot more information on a broader scale than the average employee."

Edward Snowden – Former infrastructure analyst at the NSA – June 2013


Vormetric Data Security Management Environment
• Access & Encryption Policies / Mgmt
• Management and Users linked to LDAP
LDAP Server
• Security Intelligence with access logs to SIEM systems
• Automation for policy integration, deployment, management
User
Application
Database
FS Agent
Volume Agent
File Systems
Volume Managers
Storage
Privileged Users
Root
SA
*&^$!@#)(
~|" +_)? $%~:>>
Approved Processes and Users
DB
John Smith
401 Main Street Apt 2076
Access Attempts
Data Firewall
Allow/Block
Encrypt/Decrypt

The Vormetric Data Firewall enables privileged users to do their jobs, and never see protected data.

Organizations that need to protect data from the inherent risks of privileged users typically need to do so in order to:

- **Meet Compliance Requirements –** Segregation of roles by user type to protect specific data types such as credit card information for PCI-DSS and Personally Identifiable Information (PII) under the US HIPAA/HITECH acts.
- **Prevent Data Breaches –** Data breach laws such as US Federal and State data protection laws, the EU Data Protection Directive, South Korea's Personal Information Protection Act (PIPA) and the UK Data Protection Act pose fines and costly notification requirements on loss of protected data.
- **Safeguarding Intellectual Property –** With government sponsored attacks a reality for manufacturers and infrastructure providers, and their primary target intellectual property (IP), organizations now need to secure data from both malicious insiders as well as from partners and contractors.

The Solution – The Vormetric Data Firewall

The tasks performed by privileged users to maintain, repair and initiate systems are not optional – these roles were created in order to meet real enterprise requirements that are not going away. What's needed is to enable these users to perform their tasks, while removing their ability to view private and confidential data. And when a category of account has a legitimate need for access to this sensitive data, to have the information available that allows identification of anomalous usage patterns that may indicate that the account has been compromised.

Transparent - Vormetric Data Firewall meets these needs with a transparent solution - enabling critical system processes to continue, without exposing data. Using protections at the file system and volume level, the solution allows the meta-data and file system structure to be seen by administrators, but reveals only encrypted data to these accounts. At the same time, processes and users that legitimately require access (such as a database process to a database table file) have access to unencrypted data (cleartext).

Strong – The Vormetric solution firewalls your data – using a policy driven approach, linked to LDAP and system accounts, that provides granular access to protected structured information (in databases) or unstructured data (in file systems) by process, user, time and other parameters. Vormetric even monitors and prevents access by tracking how users become their role. If a Root user creates a new account with data access rights, then escalates to become that account, Vormetric will still identify that account with the Root user and prevent access to cleartext data. The result of this approach – Privileged users can manage systems without risk of exposure to protected information

Efficient – Vormetric Encryption is a high performance, low overhead solution, leveraging the AES NI hardware encryption built into Intel x86 processors. The result: Minimal changes to response times for operational processes.

Easy – Deployments in days to weeks, not weeks to months, across physical systems, cloud, big data, and virtualized environments that are easy to manage, easy to understand.

About Vormetric

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps enterprise customers and government agencies protect what matters — their sensitive data — from both internal and external threats. In a world of Advanced Persistent Threats (APTs), Vormetric's market-leading privileged user access controls and security intelligence are invaluable. The company's scalable solution suite protects any file, any database and any application — anywhere it resides — while maintaining application performance and avoid-ing key management complexity. Many of the world's largest and most security-conscious organizations and government agencies, including 17 of the Fortune 25, have standardized on Vormetric to protect their sensitive data and provide them with advanced data security and data security intelligence.

Copyright © 2013 Vormetric, Inc. All rights reserved. Vormetric is a registered trademark of Vormetric, Inc. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Vormetric.

Critical Vormetric Data Security Elements

Data Firewall – Using high performance encryption along with access controls to provide multi-layer data protection, Vormetric creates a Data Firewall that protects against both internal and external threats to data.

Fine-grained Access Controls – Vormetric provides fine-grained, policy-based access controls that restrict access to encrypted data –ensuring that data is decrypted only for authorized users and processes.

Encryption and Key Management – Vormetric provides the strong, centrally managed, encryption and key management that enables compliance and is transparent to processes, applications and users.

Security Intelligence – Vormetric logs capture all access attempts to protected data, providing high value security intelligence information that can be used with a Security Information and Event Management (SIEM) solution to identify compromised accounts and malicious insiders.

Automation – For fast rollouts and integration with existing infrastructure, both web and command line level APIs provide access to the Vormetric Data Security environment for policy management, deployment and monitoring.

> "100% of breaches involved stolen credentials."
>
> **Mandiant – April 2013**

Vormetric, Inc.
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
South Korea: +82.2.2190.3830
info@vormetric.com
www.vormetric.com