CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

Since the introduction of multi-user computer systems over 40 years ago, there has been a fundamental flaw in the security architecture. The flaw? - The concept of a Root User, Domain Administrator, System Administrator or other high level computer operator – and their user 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 user access to all the data associated with the system.

Credit Unions should be fortifying their defenses by encrypting their data and setting policies on who can access their sensitive data. They should be encrypting their data where it resides on their databases and on servers with sensitive data. They should also enable privileged users to perform their tasks, while removing their ability to access private and confidential data.

Encrypting sensitive data in databases has clearly gone beyond optional, and is now a firm requirement. Whether an organization is looking to secure intellectual property, comply with privacy or regulatory mandates, or simply guard the organization's brand against the damage associated with data breaches, database encryption represents a vital imperative.
By providing database encryption for sensitive data in databases, organizations can establish a strong line of defense that can help secure sensitive assets against a range of threats. However, while the reasons to adopt database encryption are clear, that doesn't mean the effort is simple. In fact, for many organizations, database encryption has presented a range of obstacles, including degraded database performance, laborious revisions to application code, and complex and time consuming key management efforts.

With Vormetric solutions, you can gain the capabilities you need to encrypt and secure sensitive assets in databases, while avoiding the challenges traditionally associated with database encryption. Today, Vormetric offers a range of offerings that help safeguard assets in databases.

The tasks performed by privileged users to maintain, repair and initiate systems are not optional – these roles exist in order to meet essential requirements for all enterprise environments. What's needed is to enable these privileged users to perform their tasks, while removing their ability to access private and confidential data. And when a category of privileged user 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 privileged user account has been compromised.

continued on Page 2

Sol Cates
Chief Security Officer

Vormetric Data Security™

Contact Info
www.vormetric.com
Phone: 888.267.3732

Sol Cates is the Chief Security Officer at Vormetric. As CSO, he is tasked for ensuring Vormetric's internal security profile remains robust, while maintaining a strong pulse on the technical and business decision making process in today's IT/IS organizations. Cates partners with teams throughout the company and the industry to engage with both customers and partners. He is sought after to speak publicly to elevate industry understanding of data security best practices in today's complex cyber threat landscape.

CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

Transparent– The Vormetric Data Security Platform meets privileged user management needs with a transparent solution - enabling critical system processes to continue, without exposing data. Using protections at the file system and volume level, the privileged user access management 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 privileged 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 user 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, our privileged user management solution will still identify that user 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

The data security compliance and regulation challenges for credit unions are daunting. Data-at-rest protection requirements are found within PCI DSS requirements for credit card related information, GLBA, SOX/J-SOX, NCUA, data privacy and data residency laws, and even the USA Patriot Act. Each requirement adds to the need to protect sensitive information wherever it resides.

The Vormetric Data Security Platform is the only solution with a common, extensible platform to meet critical compliance, regulatory and sensitive data-at-rest protection needs:

- Single framework for data-at-rest protection

A common, extensible infrastructure that protects data at the file system or volume level, as well as within databases and files, regardless of the environment. Traditional data centers, virtual environments, private-public-hybrid clouds or big-data implementations are all supported with common policy control, agents and management infrastructure sets. The result – Low total cost of ownership, as well as simple, efficient deployment and operation.

- Meet global compliance requirements and regulatory standards

With Vormetric, meet data-at-rest requirements for industry compliance and regulatory standards while protecting information with this single solution to multiple needs, across enterprise, cloud and big data environments.
Vormetric provides a proven data security solution to enable rapid compliance with multiple aspects of PCI DSS. Vormetric Data Security Platform products help credit unions comply with PCI DSS 3.0 requirements 3, 7, 8 and 10 that call for the privacy protection of cardholder information. Vormetric Data Security secures cardholder data in databases as well as voice files, reports, and images.

Sol Cates
Chief Security Officer

Vormetric Data Security™

Contact Info

www.vormetric.com
Phone: 888.267.3732

Sol Cates is the Chief Security Officer at Vormetric. As CSO, he is tasked for ensuring Vormetric's internal security profile remains robust, while maintaining a strong pulse on the technical and business decision making process in today's IT/IS organizations. Cates partners with teams throughout the company and the industry to engage with both customers and partners. He is sought after to speak publicly to elevate industry understanding of data security best practices in today's complex cyber threat landscape.