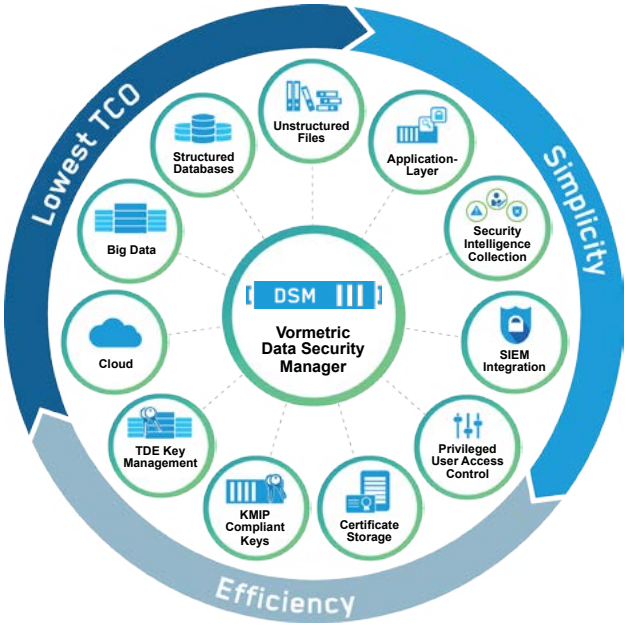
Vormetric Data Security Platform Data Sheet

The Vormetric Data Security Platform makes it efficient to manage data-at-rest security across an entire organization. The Vormetric Data Security Platform is a broad set of products that share a centrally managed and extensible infrastructure for simple one-stop data-at-rest security. The continuously expanding product-line currently includes transparent file-level encryption, application-layer encryption, integrated key management, and security intelligence. Deployed separately or in tandem you can address security policies and compliance mandates across databases, files and big data nodes—located across physical, virtual, cloud and hybrid infrastructures. With this platform's comprehensive, unified capabilities, you can quickly address your security and compliance requirements for multiple enterprise use cases, while significantly reducing total cost of ownership (TCO) for data-at-rest security.



THE VORMETRIC DIFFERENCE

The Vormetric Data Security Platform delivers a comprehensive range of capabilities, including encryption, key management, access policies, privileged user access controls, and audit logging. Through these capabilities, organizations can establish the common controls required to address the demands of a range of security and privacy mandates, including the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, PIPA, Data Residency, FISMA, NIST-800-53 and other global data protection and privacy laws.

SECURITY USE CASES

- Database Encryption
- File-level Encryption
- Application-layer Encryption
- Privileged User Access Control
- Security Intelligence
- Key Management

COMPLIANCE

- PCI DSS 3.0
- HIPAA
- NIST 800-53
- FISMA
- PIPA
- Data Residency

BEST OF vmworld 2014
Exclusive Media Partner
Gold Award
Security/Compliance for Virtualized Environments

SC MAGAZINE AWARDS 2014 Europe WINNER

Best Encryption Solution

Deloitte. Technology Fast500

PLATFORM BUSINESS BENEFITS

Lower Total Cost of Ownership for Data-at-Rest Security

The Vormetric Data Security Platform makes it simpler and less costly to protect data-at-rest. The platform enables your IT and security organizations to quickly safeguard data across your organization in a uniform and repeatable way. The Vormetric Data Security Platform replaces a multitude of point products scattered across your organization enabling a strategy for consistent and centralized data control, compliance and security.

Simple and Efficient

The Vormetric Data Security Platform makes administration simple and efficient, offering an intuitive Web-based interface, as well as an application programming interface (API) and command-line interface (CLI). IT resources are efficiently used because data-at-rest security can be applied quickly and consistently. Furthermore, this high-performance solution enables efficient use of virtual and physical server resources, reducing the load on the service delivery infrastructure.

Beyond Compliance: Better Security

Moving security close to the data is more effective because it minimizes the potential for any surreptitious access. Vormetric offers a unique approach for protecting databases, files, and big data across the entire organization. The platform provides capabilities for encrypting data, controlling access, and creating granular security intelligence logs. These security intelligence logs can accelerate detection of advance persistent threats (APTs) and insider threats because they offer visibility into file access. In addition, these capabilities and logs satisfy many common compliance reporting requirements.

PLATFORM PRODUCTS

Vormetric Data Security Manager

Offers centralized management of keys and policies for the entire suite of products available within the Vormetric Data Security Platform. It is available as a virtual or FIPS 140-2 physical appliance.

Vormetric Transparent Encryption

Is an agent that runs in the file system to provide high-performance encryption and least-privileged access controls for files, directories, and volumes for both structured databases and unstructured files.

Vormetric Application Encryption

Simplifies adding column-level encryption into existing applications by removing the complexity of the developer supporting cryptographic and encryption key management operations.

Vormetric Key Management

Can be used to centrally manage keys for Vormetric products, Oracle Transparent Data Encryption (TDE), and Microsoft SQL TDE. In addition, the product securely stores certificates and offers support for the Key Management Interoperability Protocol (KMIP).

Vormetric Security Intelligence

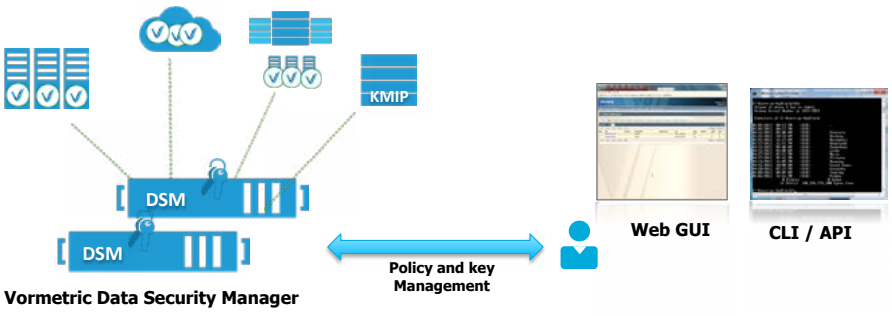
Are granular file access security event logs that are easy to integrate with Security Information and Event Management (SIEM) systems to produce compliance and security reports to produce an audit trail of permitted and denied access attempts from users and processes.

Key Platform Capabilities

- A single console for managing all data-at-rest security policies
- On demand extensibility through licensing and software
- Enterprise-class architecture, scale and performance
- Security and compliance across all server environments: physical, virtual, cloud, big data, and hybrid environments
- Enforcement of least-privileged user access policies
- Pre-defined dashboards and reports with popular SIEMs

Vormetric Data Security Manager Specifications

The Vormetric Data Security Manager (DSM) centralizes control of the Vormetric Data Security Platform. The DSM changes the data security game by enabling an IT organization to have a consistent and repeatable method for managing encryption, access policies, and security intelligence for all structured and unstructured data. Once the DSM is in place, you can quickly address new security mandates, compliance requirements, and emerging threats. You can use the DSM to provision Vormetric Transparent Encryption and Vormetric Application Encryption, and to manage keys and certificates for third-party devices. By delivering centralized control of a breadth of data-at-rest security capabilities, DSM provides low total cost of ownership, efficient deployment of secure services, and improved visibility and control.



RELIABLE, FIPS VALIDATED, SECURE SYSTEM DESIGN

To maximize uptime and security, the DSM features redundant components and the ability to cluster appliances for fault tolerance and high availability. Strong separation-of-duties policy can be enforced to ensure that one administrator does not have complete control over data security activities, encryption keys, and administration. In addition, the DSM supports two-factor authentication for administrative access. The hardware appliance is available with FIPS 140-2 Level 2 and FIPS 140-2 Level 3 validation.

UNIFIED MANAGEMENT AND ADMINISTRATION ACROSS THE ENTERPRISE

DSM enable enterprises to minimize encryption and key management costs by providing an appliance to manage heterogeneous encryption keys, including keys generated by the Vormetric Data Security Platform, IBM InfoSphere, Guardium Data Encryption, Oracle TDE, Microsoft TDE, and KMIP-compliant encryption products. It features an intuitive Web-based console for managing encryption keys, policies, and auditing across an enterprise. The product also centralizes log collection across any number of agents.

Key Benefits

- Single console for all platform policy and key management
- Multitenant
- Proven scale to 10,000+ agents
- Cluster support for high availability
- Toolkit and programmatic interface
- Easy integration with existing authentication infrastructure
- Available as a virtual or physical appliance

VORMETRIC DATA SECURITY MANAGER SPECIFICATION TABLE

Specification	Description
General Specifications	
Administration Interfaces	Secure Web, CLI, SOAP
Number of Management Domains	1,000+
API Support	PKCS#11, Microsoft Extensible Key Management (EKM), SOAP
Security Authentication	Username/Password, RSA two-factor authentication (optional)
Cluster Support	Yes
Backup	Manual and scheduled secure backups. M of N key restoration.
Network Management	SNMP, NTP, Syslog-TCP
Syslog Formats	CEF, LEEF and RFC 5425
Certifications and Validations	FIPS 140-2 Level 2, FIPS 140-2 Level 3, Common Criteria in process, Suite B
Hardware Specifications	
Hard Drive	Mirrored SAS drives
Memory	12 Gigabytes
Safety Agency Approval	FCC and UL certifications
Serial Port	1
Power Supplies	Redundant 800 watts max, field replaceable, AC 100 - 240V auto sense, 47-63 Hz
Chassis Dimensions	2U Rack mountable, 17" x 17" x 3.5" inches (43.18 x 43.18 x 8.89 centimeters)
Weight	30 lbs (13.64 Kgs)
Maximum BTU	410
Operating Temperature	10º to 35º C (50º to 95º F)
Non-operating Temperature	-40º to 70º C (-40º to 158º F)
Operating Relative Humidity	8% to 90% (non-condensing)
Non-operating Relative Humidity	5 to 95% (non-condensing)
Minimum Virtual Machine Specifications	**Recommendation for Vormetric Data Security Manager Virtual Appliance**
Number of CPUs	2
RAM (GB)	4
Hard Disk (GB)	80
Support Thin Provisioning	Yes

VORMETRIC DATA SECURITY MANAGER LICENSING OPTIONS

Name	SKU	Description
DSM Enterprise—Physical	VOR-DSM-AP50-ENT	Physical appliance. No agent management limit. FIPS 140-2 Level 2.
DSM Enterprise—Virtual	VOR-DSM-VM50-ENT	Virtual appliance. No agent management limit.
DSM Enterprise—Physical with FIPS 140-2 Level 3	VOR-AO-HSM00-PL-P	Physical appliance. No agent management limit. FIPS 140-2 Level 3.

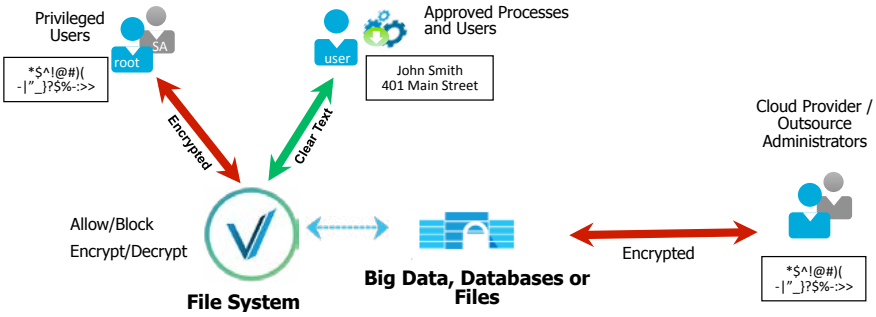
Vormetric Transparent Encryption Specifications

Vormetric Transparent Encryption enables data-at-rest encryption, privileged user access control, and the collection of security intelligence logs for structured databases and unstructured files —including those residing in physical, big data, and cloud environments. By leveraging this transparent approach, your organization can implement encryption, without having to make changes to your applications, infrastructure, or business practices. Unlike other encryption solutions, protection does not end after the encryption key is applied. Vormetric continues to enforce least-privileged user policies to protect against unauthorized access by users and processes, and it continues to log access. With these capabilities, you can ensure continuous protection and control of your data.

VORMETRIC TRANSPARENT ENCRYPTION ARCHITECTURE

Vormetric Transparent Encryption is an agent that runs at the file system level or volume level on a server. The agent is available for a broad selection of Windows, Linux, and Unix platforms, and can be used in physical, virtual, cloud, and big data environments — regardless of the underlying storage technology. All policy and key administration is done through the Vormetric Data Security Manager.

Vormetric Transparent Encryption agents are distributed across the server infrastructure. As a result, the product delivers scalability and eliminates the bottlenecks and latency that plague proxy-based solutions. In addition, you can use hardware-based encryption acceleration products, such as Intel AES-NI and SPARC Niagara Crypto modules, to further enhance encryption performance.



POWERFUL PRIVILEGED USER ACCESS CONTROLS

The agent enforces granular least-privileged user access policies that protect data from misuse by privileged users and advanced persistent threat (APT) attacks.

Granular 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.

Key Benefits

- Broadest platform support in industry: Windows, Linux, and Unix operating systems
- Easy to deploy; no application customization required
- High performance encryption
- Strong encryption and Suite B protocol support
- Privileged user access control
- Log all permitted, denied and restricted access attempts from users, applications and processes

Technical Specifications

Platform Support

- Microsoft: Windows Server 2003, 2008, and 2012
- Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server and Ubuntu
- Unix: IBM AIX, HP-UX, Solaris

Database Support

- Oracle, DB2, SQL Server, MySQL, Sybase, NoSQL environments and others

Application Support

- Transparent to all applications and custom applications including SAP, SharePoint, Documentum, etc.

Big Data

- Cloudera CDH 4/5, MongoDB, other HDFS environments

Encryption Hardware Acceleration

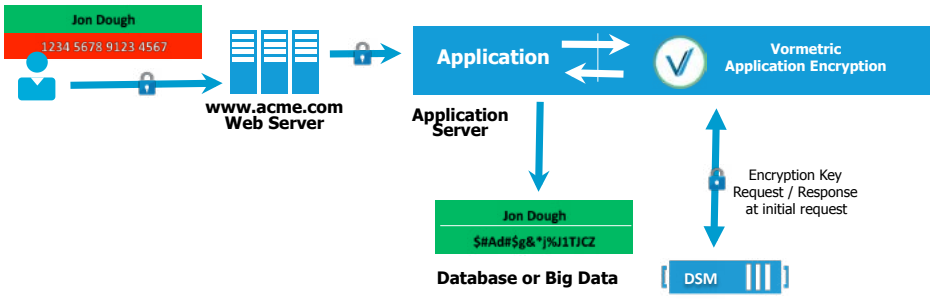
- Intel Data Protection Technology with AES-NI and Secure Key
- SPARC Niagara Crypto modules

Policy and Key Administration

- Vormetric Data Security Manager with AES-NI and Secure Key

Vormetric Application Encryption Specifications

Use Vormetric Application Encryption any time you need to do application-layer encryption of a specific field or column in a database, big data node, or PaaS environment. Vormetric Application Encryption is a library that simplifies the integration of encryption with existing corporate applications. The library provides a set of documented, standards-based APIs that can be used to perform cryptographic and key management operations. Vormetric Application Encryption eliminates the time, complexity, and risk of developing and implementing an in-house encryption and key management solution.



REDUCING APPLICATION-LAYER ENCRYPTION COMPLEXITY AND COSTS

Application-layer encryption is typically employed when compliance or regulatory mandates require encryption of specific fields at the application layer, before data is stored. Vormetric Application Encryption reduces the complexity and costs associated with meeting this requirement, simplifying the process of adding encryption capabilities to existing applications. Developers can use libraries for Java, .NET, or C to facilitate communication between applications and the Vormetric Application Encryption Agent. This agent encrypts data and returns the resulting cipher text to the application, using the same proven high-performance encryption and reliable key management capabilities that are employed by Vormetric Transparent Encryption. All policy and key management is done through the DSM, simplifying the data security operations environment by reducing the number of administrative consoles that administrators have to learn and maintain.

PROTECTING DATA IN THE CLOUD

Security professionals often have concerns about moving sensitive data from traditional enterprise applications to platform-as-a-service (PaaS) environments. Vormetric Application Encryption enables you to encrypt sensitive data before it leaves the enterprise and is stored in the cloud. By leveraging this approach, you can ensure that cloud administrators, other customers, hackers, and authorities with subpoenas can't access sensitive data, which can help address relevant auditor requirements and security policies.

Key Benefits

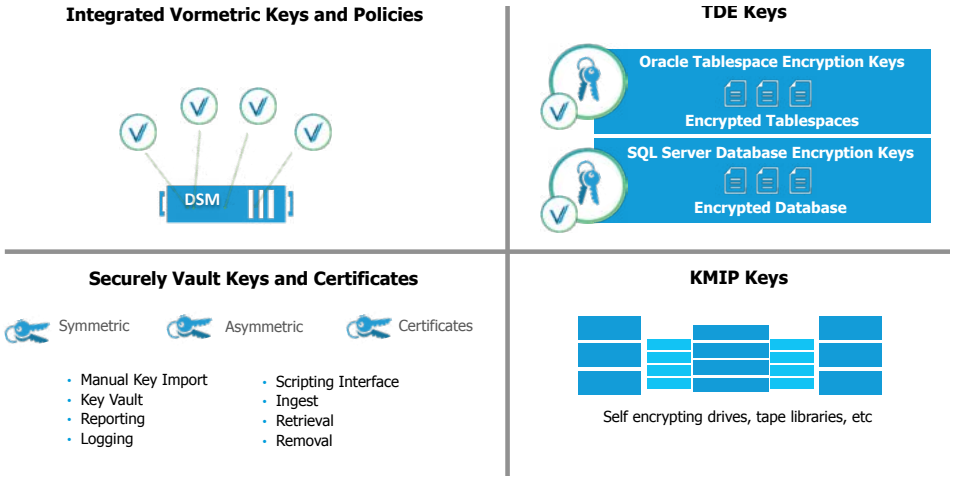
- Leverage proven, Vormetric high-performance encryption and key management
- Broad application and platform support
- Centralize control of application-layer encryption and file system encryption
- Stop malicious DBAs, cloud administrators, hackers, and authorities with subpoenas from accessing valuable data

Technical Specifications

- Supported Environments: Microsoft.NET 2.0 and higher, JAVA 6 and 7, and C
- Standards: OASIS PKCS#11 APIs
- Encryption: AES
- Operating Systems: Windows 2008, 2012 and Linux
- Performance: over 50,000 credit card size encryption transactions per second
- Policy and Key Administration: Vormetric Data Security Manager

Vormetric Key Management Specifications

With Vormetric Key Management, you can centrally manage keys from all Vormetric products, and securely store and inventory third-party keys and certificates. The product provides a high availability, standards-based, FIPS 140-2 validated key management platform that can secure keys for Microsoft TDE, Oracle TDE, and KMIP-compliant devices. By consolidating key management, this product fosters consistent policy implementation across multiple systems, reducing training and maintenance costs.



CONSOLIDATE AND SIMPLIFY KEY MANAGEMENT AND VAULT CERTIFICATES

Historically, as the number of applications and devices using encryption proliferated, there was a commensurate increase in the number of key management devices employed. This growing number of key management devices added cost and complexity to securing sensitive data. Further, these disparate key management devices often left valuable certificates unprotected, making them easy prey for hackers. Also, if these certificates are left unmanaged, they can unexpectedly expire, which can result in the unplanned downtime of vital corporate services. The Vormetric Data Security Platform extends your key management capabilities, enabling you to manage keys for Vormetric's encryption products as well as keys and certificates from third-party products.

SECURE, RELIABLE, AND AUDITABLE

Vormetric Key Management offers all the reliability and availability capabilities of Vormetric DSM. Vormetric DSM features an optional FIPS 140-2 Level 3 validated hardware security module (HSM). 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.

Key Benefits

- Operational efficiency, continuous availability, secure storage, and inventory of certificates and encryption keys
- Alerts offer proactive notifications of certificate and key expiration
- Reports provide status and characteristic information, audit support

Technical specifications

Manage Security Objects

- X.509 certificates
- Symmetric and asymmetric encryption keys

Administration

- Secure-web, CLI, API
- Bulk import of digital certificates and encryption keys
- Validates on import
- Extracts basic attributes from uploaded certificates and keys for reporting
- Command line scripts
- Retrieval and removal

Supported Key and Certificate Formats for Search, Alerts, and Reports

- Symmetric encryption key algorithms: 3DES, AES128, AES256, ARIA128, and ARIA256
- Asymmetric encryption key algorithms: RSA1024, RSA2048, and RSA4096
- Digital certificates (X.509): PKCS#7, PKCS#8, DER, PEM, PKCS#12

Transparent Database Encryption (TDE)

- Key management for both Oracle TDE and Microsoft SQL Server TDE

API Support

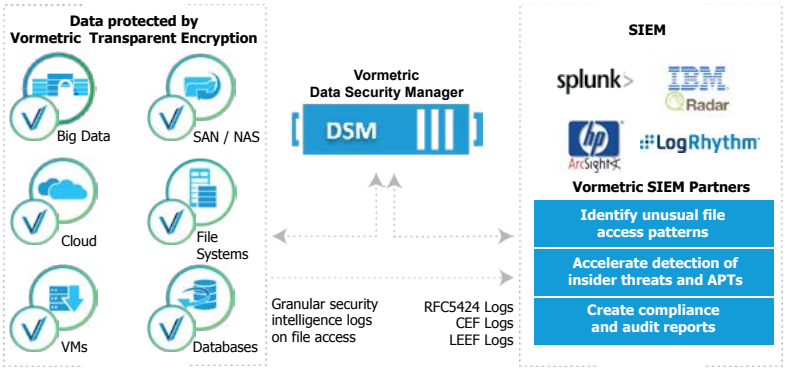
- PKCS#11, Microsoft Extensible Key Management (EKM), and OASIS KMIP

Key Availability and Redundancy

- Secure replication of keys across multiple appliances with automated backups

Vormetric Security Intelligence Specifications

Vormetric Security Intelligence are granular event logs that produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into file access activities. Logging occurs at the file system level, removing the threat of an unauthorized user gaining stealthy access to sensitive data. These logs can inform of unusual or improper data access and accelerate the detection of insider threats, hackers, and advanced persistent threats (APT) that have bypassed perimeter security. With the availability of pre-defined dashboards and reports, Vormetric Security Intelligence easily integrates with SIEM systems to produce compliance and security reports.



PROVIDING SECURITY INTELLIGENCE

Vormetric Security Intelligence provides logs that detail which processes and users have accessed protected data. Sharing these logs with a SIEM platform helps uncover anomalous process and user access patterns, which can prompt further investigation. For example, an administrator or process may suddenly access much larger volumes of data than normal, or attempt to do an unauthorized download of files. Such inconsistent usage patterns could point to an APT attack or malicious insider activities. Traditionally, SIEMs relied on logs from firewalls, IPSs, and NetFlow devices. Because this intelligence is captured at the network perimeter, these approaches leave a commonly exploited blind spot: They don't provide any visibility into the activity occurring on servers. Vormetric Security Intelligence fills this blind spot, helping accelerate the detection of APTs and insider threats.

COMPLIANCE REPORTING

In order to adhere to many compliance mandates and regulations, organizations must prove that data protection is in place and operational. Vormetric Security Intelligence is commonly used to prove to an auditor that encryption, key management, and access policies are working effectively. The detailed logs are reviewed to specify when users and processes accessed data, under which polices, and if access requests were allowed or denied. The logs will even expose when a privileged user leverages a command like "switch user" to imitate another user.

Key Benefits

- Increased visibility of sensitive data access
- Accelerated APT and insider threat detection
- Export logs in all major log formats: Syslog RFC5424, CEF, and LEEF
- Fast integration with Vormetric SIEM partners
- Consolidated and consistent compliance and audit reporting

SIEM Partner Integration

- Vormetric Splunk App
- HP ArcSight CEF Certified SmartConnector
- IBM QRadar Vormetric Device Support Module

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 over 1400 customers, including 17 of the Fortune 25 and many of the world's most security conscious government organizations, to meet compliance requirements and protect what matters — their sensitive data — from both internal and external threats. For more information, please visit: www.vormetric.com.

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