Secure Big Data and Analytics Platform

Solution Brief
September 2015

Cisco UCS Integrated Infrastructure with Vormetric Software

Highlights

Cisco UCS Integrated Infrastructure for Big Data

- Deploy an industry-leading platform that integrates computing, networking, and management capabilities into a unified, fabric-based architecture that is optimized for big data workloads.

Vormetric Data Security Manager

- Benefit from enhanced encryption of data at rest and centralized key management.

Standards Compliance

- Support standards such as Federal Information Processing Standards (FIPS) 140-2 L3, the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry (PCI DSS) Data Security Standard.

Deploy Cisco UCS® Integrated Infrastructure with Vormetric software to help secure your critical business data.

As big data gains importance, your organization must take measures to secure accumulated information. That's why organizations in every industry—including healthcare organizations, financial institutions, and government agencies—are encrypting data at rest to protect it from unauthorized access and help ensure compliance with regulatory standards such as Federal Information Processing Standards (FIPS), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

Data Security Challenges

The emergence of big data adds a new dimension to data management and brings with it new challenges. Simply protecting data by prohibiting access to outside users and trusting users within your organization is not enough. That's because data no longer originates from predetermined sets of devices and applications that are approved by your IT staff, nor does data solely reside on your enterprise-managed servers and storage arrays. The presence of this dispersed data, in combination with tools that lack inherent security features such as data privacy and built-in user authentication, blurs the lines of control for data management and access.

Sensitive Data Is Under Attack

Information is the foundation of any organization. When data security is compromised, it directly affects the business and puts the business at risk. Enterprise security teams continue to fight the battle, spending a significant amount of time and money to safeguard their organizations' sensitive assets, including card-holder data, employee and customer data, health information, and intellectual property. Unfortunately, as evidenced by the nonstop barrage of devastating breaches reported in the news, existing defenses have failed.

The Time for Security is Now

Today, your organization must have the capability to manage, control, and secure data in multiple ways:

- Encrypt data at rest.
- Provide access policies and OS-level privileged user controls to protect against insider threats, malware, and advanced persistent threats (APTs).
- Comply with the standards.
- Detect and react to alerts during complex threats and data breaches.

Cisco UCS Integrated Infrastructure for Big Data

A popular choice for enterprise deployments, Cisco UCS Integrated Infrastructure for Big Data is a highly scalable architecture that is designed to meet a variety of scale-out application demands. It offers transparent data and management integration capabilities for the enterprise applications that are deployed on the hardware.

Cisco UCS 6200 Series Fabric Interconnects

Fabric interconnects establish a single point of connectivity and management for the entire system. Deployed in redundant pairs, Cisco UCS fabric interconnects offer the high-bandwidth and low-latency connectivity, active-active redundancy, high performance, and exceptional scalability needed to support the large number of nodes that are typical in clusters serving big data applications.

The system integrates and unifies management for all connected devices. Cisco UCS Manager supports rapid and consistent server configuration using service profiles and automates ongoing system maintenance activities, such as firmware updates, across the entire cluster as a single operation. It also offers advanced monitoring capabilities with options to raise alarms and send notifications about the health of the entire cluster.

Cisco UCS C240 M4 Rack Server

Cisco UCS C240 M4 Rack Servers support a wide range of computing, I/O, and storage-capacity demands in a compact design. Based on the Intel® Xeon® processor E5-2600 v3 family and supporting 12-Gbps serial-attached SCSI (SAS) throughput, these rack servers deliver significant performance and efficiency gains for a variety of applications.

Cisco UCS C240 M4 servers use dual CPUs, support up to 768 GB of main memory (128 to 256 GB is typical for big data applications), and support a range of disk and solid-state-disk (SSD) drive options. Twenty-four small-form-factor (SFF) disk drives are supported in the performance-optimized option, and 12 large-form-factor (LFF) disk drives are supported in the capacity-optimized option.

Available for Cisco UCS C-Series Rack Servers, the Cisco UCS Virtual Interface Card (VIC) 1227 implements Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which unifies virtual and physical networking into a single infrastructure. This innovation provides virtual machine visibility from the physical network and a consistent network operations model for physical and virtual servers.

Compliance with Standards

Federal Information Processing Standard (FIPS) 140-2 L3: Specifies the security requirements that must be satisfied by a cryptographic module used by a security system that protects sensitive but unclassified information

Health Insurance Portability and Accountability Act (HIPAA): Defines the standard for protecting sensitive patient information.

Privacy rule: Addresses the ways that the medical and personal information of any individual can be saved, accessed, and shared

Security rule: Mandates and outlines a standard to protect stored and electronically transmitted health data (electronic protected health information [ePHI])

Vormetric Data Security Platform

The Vormetric Data Security Platform offers the detailed controls, robust encryption, and comprehensive coverage that your organization needs to secure sensitive data across your big data environments (Figure 1).

Core product technologies: The The Data Security Platform helps you efficiently manage security for data at rest across your entire organization.

Built on an extensible infrastructure, the Data Security Platform includes several products that can be deployed individually or together. Through the platform's centralized key management and flexible implementation, you can address security policies and compliance mandates across databases, files, and big data environments—whether your assets are located in the cloud or in virtual or traditional infrastructures. With this platform's comprehensive and unified capabilities, you can efficiently scale to address your expanding security and compliance requirements while significantly reducing your total cost of ownership (TCO).

Transparent encryption: The platform supports encryption of data at rest, privileged-user access control, and the collection of security intelligence logs without the need to reengineer applications, databases, or infrastructure.

Tokenization with dynamic data masking: Your security teams can address compliance objectives while achieving breakthroughs in operational efficiency, including the removal of databases from the scope of PCI DSS audits with little disruption or administrative overhead. By helping ensure persistent security controls over data—no matter where it resides—Vormetric tokenization can help your organization get the most from your cloud services, big data analytics, and outsourced environments.

Cloud encryption gateway: This encrypted gateway helps you safeguard files in cloud environments. The solution encrypts sensitive data before it is saved to the cloud storage environment, helping security teams establish the visibility and control they need to protect sensitive assets.

Application encryption: You can simplify the integration of application-level encryption into your existing corporate applications. The application encryption library provides a set of documented standards-based APIs that perform cryptographic and encryption-key management operations. Vormetric application encryption eliminates the complexity and risk entailed in implementing an in-house encryption and key management solution.

Security intelligence: The solution works with security information and event management (SIEM) solutions to accelerate behind-the-perimeter threat detection and produce detailed file access and security information logs for auditors and compliance officers.

Key management: The solution delivers consistent policy implementation between systems, enabling you to reduce training and maintenance costs.

Essential data: Data is provided in RFC5424, Common Event Format (CEF), and Log Event Extended Format (LEEF). This data can be analyzed using the security intelligence capabilities of a SIEM solution to identify use patterns that may represent a threat.

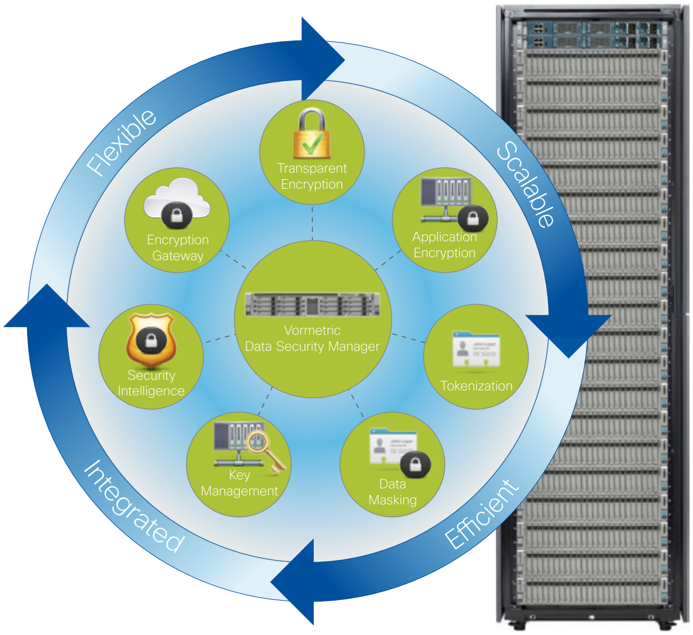

Figure 1. Cisco UCS Integrated Infrastructure with Vormetric Software

Performance That Delivers

Cisco tested the solution to understand whether and how data encryption affects performance, with workloads derived from the TPC Express Benchmark HS (TPCx-HS). Tests were run with Vormetric data encryption enabled and then disabled. Because the benchmark results were not officially audited and published but only used for analysis purposes, they cannot be compared with any published results.

Tests were conducted at scale factors of 1, 10, and 30 terabytes (TB) on a Cisco UCS Integrated Infrastructure for Big Data rack with 16 Cisco UCS C240 M4 servers running Red Hat Enterprise Linux 6.4 and one server running Vormetric Data Security Manager and a leading Hadoop distribution. The test results show a slight (6 to 7 percent) performance degradation with data encryption enabled for an end-to-end run (data generation, data sort, and result validation), due to enhancements in the Intel Advanced Encryption Standard New Instructions (AES-NI) used in the server's processor (Figure 2). Although the performance impact of data encryption depends on the workload and data set, in general the effects of the small amount of performance degradation are outweighed by the security benefits achieved.

Conclusion

Cisco UCS Integrated Infrastructure running Vormetric Data Security Platform provides a modular framework that can rapidly scale to meet demand. By deploying this solution, you can take advantage of an integrated big data architecture, protect data, and comply with regulations without sacrificing performance.

For More Information

For more information about big data solutions using Cisco UCS, visit http://www.cisco.com/go/bigdata.

For more information about Cisco Validated Designs, visit http://www.cisco.com/go/bigdata_design.

For more information about Vormetric software visit http://www.vormetric.com.

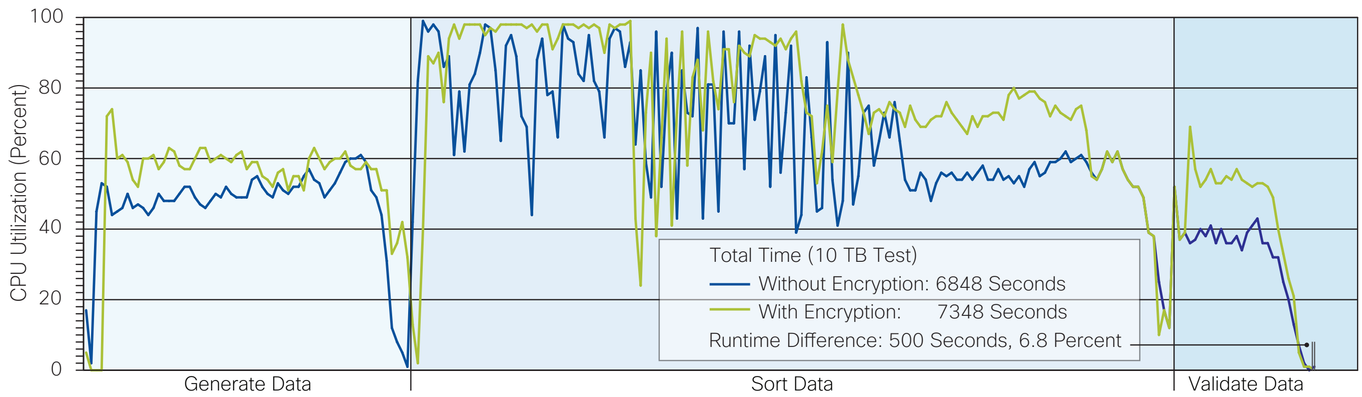

Figure 2. Test Results Show Little Impact Due to Encryption

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.