Executive Summary

High-speed data analytics is changing the way companies compete, enabling them to generate real-time insights to support their most important business processes. The SAP HANA* platform is a clear leader in this arena, providing a uniquely fast and adaptable platform for real-time business on an enterprise scale.

Cloud computing offers a complementary technology that also provides game-changing capabilities for business computing. Yet many companies have been reluctant to deploy mission-critical applications, such as SAP HANA, in hosted cloud environments. Although they would like the potential benefits, they have understandable concerns about security and compliance. Virtustream answers those security and compliance concerns with a global cloud infrastructure that is designed specifically for hosting mission-critical workloads.

Now Virtustream is taking cloud security to even higher levels by integrating Vormetric Data Security* into its cloud infrastructure and utilizing a variety of security technologies that are built into the latest Intel® Xeon® processor E7 v2 family. Intel, Vormetric, Virtustream and SAP have been working together in the SAP Co-Innovation Lab (COIL) to integrate and test the combined solution.

With this enhanced security architecture, customers can implement even stronger data encryption and more granular access controls for SAP HANA. Importantly, they retain complete control over their data in this enhanced cloud environment. And with SAP HANA running on the latest Intel Xeon processor E7 v2 family, they can experience real-time performance across very large data sets—up to three times larger than could be supported using previous-generation platforms1.
The Goal: Real-Time Business with Cloud-Based Efficiency

Two major trends are converging in business computing. First, companies are moving to in-memory analytics to drive better business outcomes through real-time, data-driven decision making. Second, they are adopting cloud computing technologies to transform the way they deliver IT services. Many companies want to combine these two approaches to achieve the competitive advantages of real-time business with the agility and cost efficiencies of cloud computing.

A third trend in business computing can help them do exactly that. The scalability and reliability of industry-standard server platforms have been advancing rapidly. The latest systems based on the Intel Xeon processor E7 v2 family have eclipsed today’s RISC/UNIX*-based systems by delivering better performance at lower total cost and with comparable levels of reliability, availability and serviceability (RAS). These servers deliver the performance and scalability needed for in-memory computing on an enterprise scale—and they do this on a cost-effective, industry-standard platform that fits seamlessly into today’s public and private cloud computing environments.

Intel and SAP collaborated to bring these trends together in SAP HANA. The result is a unique, real-time business platform based on an in-memory database that supports both transactional and analytical applications on the same platform. With its data-agnostic design, SAP HANA can ingest data in real time from all available data sources. For example, SAP HANA supports cost-effective, petabyte-scale Big Data integration using the Intel® Distribution for Apache® Hadoop software.

Companies are using SAP HANA to perform sophisticated predictive and prescriptive analytics on all their data—structured, unstructured, historical, and fresh operational. They are identifying market trends and opportunities, personalizing customer engagements, streamlining operations, and closing financial books in seconds, all while converging infrastructure and data onto a single, simplified in-memory platform.

SAP HANA is available as an appliance for onsite implementations and also as an on-demand service from public cloud providers. Cloud solutions can help simplify deployment and reduce up-front costs. They also allow companies to scale SAP HANA up or down as needs evolve. Since customers pay only for the resources they use, this approach can make it easy to align IT investments with business needs as requirements change.

The Roadblocks

Security Gaps in Public Clouds

Achieving full value from SAP HANA requires integrating and analyzing core business data, which typically includes both private customer information and valuable intellectual property. Hosting such sensitive data in the cloud raises security and compliance concerns that must be addressed.

Many cloud service providers (CSPs) focus primarily on helping their customers optimize infrastructure agility and IT cost models. Businesses can use these clouds to spin up resources quickly and affordably for non-mission-critical functions and non-sensitive data. However, such clouds are typically a black box to the businesses that use them. Customers have little or no visibility into the data center environment, and their workloads and data may reside on physical infrastructure that is shared with many other customers.
There is another security risk in most public clouds. The CSP administrators who manage the infrastructure typically have access to the entire solution, including applications and data. Although there may be operational safeguards, the potential for insider attacks exists, not only from CSP administrators, but also from advanced persistent threats (APTs) that use sophisticated, long-term strategies to exploit insiders.

In this environment, trust between cloud providers and their customers is no longer enough. Businesses need to know that they, and only they, can access their data. They also need to know that protections are in place to guard against both internal and external threats, including APTs.

Data Residency Requirements
Data mobility raises additional concerns about cloud hosting solutions. Data protection and privacy laws vary around the world, and many jurisdictions have strict requirements regarding data residency. Yet, in many public cloud environments, customer applications and data are often moved without notice to maximize data center efficiency. Your data could potentially be moved across the data center, across the country, or even around the world. If you have sensitive data, this raises serious security concerns. If you have data residency requirements, it may put your business at risk for non-compliance.

For example, the European Union Data Protection Regulation makes it illegal to transfer data in response to an overseas court order without authorization from the European Commission. However, if a service provider is incorporated in a non-EU country or has a data center in a non-EU country, the provider is required to comply with a subpoena for data from that non-EU country, even if the data resides in the EU. This and many other global regulatory issues create a tough decision matrix for CSPs and introduce significant potential risks for their customers.

To manage risk in such a complicated regulatory environment, enterprise customers must retain full control over their data. Data must not only be encrypted in the cloud, but the customer—and only the customer—must have access to the encryption keys. With this approach, the CSP can respond appropriately to court orders (by sending the encrypted data), without putting the customer at risk (since the data cannot be “unlocked” without the customer-controlled encryption keys).

Achieving Security and Compliance for SAP HANA in the Cloud
Providing strong security and compliance in any computing environment requires robust capability at every level of the solution stack. Security and compliance for SAP HANA begins with the built-in controls. Vormetric, Virtustream, and Intel build on this foundation to deliver enterprise-class security and compliance without sacrificing performance or generating excessive administrative overhead.

SAP HANA: Built-In Security for Enterprise Environments
SAP HANA provides integrated support for establishing and enforcing strong security policies. Built-in capabilities include:

- **Role-based access and authorization for SAP HANA users and administrators.** SAP HANA supports strong authentication security using the customer’s method of choice (basic authentication, Kerberos, SAML, SAP* login and assertion tickets, X.509, and so on).
- **Data encryption.** Encryption is supported for both data on disk and data communications across the network.
- **Transaction logs and reporting mechanisms.** SAP HANA provides the information and governance support that businesses need to monitor and audit user access and operations.


Vormetric: Enhancing Security While Keeping Customers in Full Control of Their Data
The security protections described above are sufficient for many customers, as evidenced by the success of SAP HANA in supporting mission-critical workloads for large businesses. However, companies with particularly stringent data security requirements are sometimes looking for an even higher level of control.

In typical SAP HANA implementations, encryption keys are colocated with the data. With this approach, IT maintenance staff has access to the keys and potentially to the data. When the implementation is hosted in the cloud, this means that the CSP maintenance staff has access to the customer’s encryption keys and data. Vormetric Data Security closes this security gap. CSP maintenance staff can access the application and the infrastructure, but only the customer’s authorized users and security administrators can access the encryption keys, the data, and the access policies.
Vormetric Data Security is deployed and managed using the Vormetric Data Security Manager, which can be located either in the customer's data center or in the cloud. Encryption keys are stored in a secure vault (see Figure 1).

In addition to ensuring that data and access policies are secured against unauthorized users and administrators, Vormetric Data Security:

- **Extends encryption beyond SAP HANA data volumes** to include logs and configuration files. This extension provides stronger protection against more sophisticated insider attacks.

- **Provides more flexible and granular decryption access controls** based on the requestor, time, data type, and data location (drive, device, disk, and so on).

- **Provides additional granular logs for monitoring, reporting, and in-depth security analysis.** Logs can be monitored and analyzed using governance, risk management, and compliance (GRC) applications to provide continuous assessment of the security environment and to generate alerts if potential issues arise. This approach is recommended, as advanced analytics is increasingly valuable for detecting the subtle departures from normal usage patterns that might indicate an insider attack or a sophisticated APT.

Virtustream: Enterprise-Class Security and Compliance in the Cloud

Virtustream is a global CSP that focuses specifically on hosting mission-critical workloads for large businesses. Customers vary in size from midsize enterprises to Fortune 500 and Global 2000 companies, and they represent a broad range of industries, including financial services, healthcare, retail, manufacturing, and many others. Virtustream currently hosts production SAP landscapes for more than 100 businesses, including many that are using SAP HANA for real-time analytics and for supporting SAP Business Suite applications.

Customer-Controlled Data Security

[Vormetric Data Security Manager
(Physical or Virtual)]
Centralizes policy and key management

[Vormetric Data Security Manager
(Physical or Virtual)]
Centralizes policy and key management

Intel® Data Protection Technology
with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
and Intel® Secure Key

Server (Intel® Xeon® processor E7 v2 family)

Optimized cloud services for mission-critical applications

Data encryption and access control policy enforcement

Scalable server platform with hardware-enhanced security

Figure 1. Vormetric provides advanced data encryption and access controls and ensures that only the customer has access to data, access policies, and encryption keys.
With its global scale and mission-critical focus, Virtustream has the resources and expertise to provide levels of security and compliance that are as good as or better than many businesses are able to provide in their own data centers. Some of the key safeguards that Virtustream provide include the following:

- **Enterprise-class data center security**, including both physical and logical safeguards. Customers access their systems and applications through VPNs and advanced firewalls block digital attacks and unauthorized users at multiple levels throughout the data center (see Figure 2).

- **Advanced data protection and residency control**, since Virtustream maintains physical separation of customer data, enabling strong, disk-level security protections that are not possible in many cloud environments.

Customers can also stipulate data residency requirements, so that their data is restricted to specified geographies or data centers. Vormetric Data Security adds to these protections by extending encryption coverage to transaction logging and access controls, and by ensuring that only the customer can access the data.

- **Predictable backup and replication services** in accordance with published terms and conditions or as specified in customer service level agreements.

- **Trusted infrastructure for application workloads**. Virtustream takes advantage of Intel® Platform Protection Technology with Intel® Trusted Execution Technology (Intel® TXT). Intel TXT cryptographically verifies platform and hypervisor integrity when systems are booted. The system can launch only into a “known good state,” which helps ensure that no malware of any kind has been inserted during or prior to launch. Intel TXT also provides information that can be used to enforce and validate compliance.

- **Monitoring of infrastructure and transaction logs** with GRC applications. These applications use sophisticated, real-time analytic algorithms to identify and alert IT staff to a wide range of potential security breaches, including APTs.

- **Full audit capability**. Customers can validate compliance with their own requirements and with government and industry regulations.

Virtustream also provides complete professional services and support for feasibility assessment, migration and onboarding, and application support. A key component of this service is to ensure that the security and compliance solution takes into account the unique needs of the customer in a verifiable manner.

**Figure 2.** The Virtustream enterprise cloud provides multiple layers of security to protect customer applications and data, including continuous monitoring and analysis of logs to identify sophisticated attacks, such as advanced persistent threats.
Intel: Providing the Foundation for Strong, High-Performance Encryption

Intel worked closely with SAP to develop the SAP HANA platform, and security continues to be an important area of collaboration. Intel provides hardware-based security technologies in Intel Xeon processors that help strengthen the security of the Virtustream and Vormetric solution, while sustaining the performance levels that are required to support real-time business processes.

Intel TXT was discussed previously. Intel also provides Intel® Data Protection Technology with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and Intel® Secure Key.5

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

In the past, customers had to sacrifice application performance if they wanted to encrypt their data. Encryption and decryption are compute-intensive processes that can add latency to data access times and consume substantial computing resources. In the real-time business environments supported by SAP HANA, such delays and overheads are not acceptable.

Intel solves this challenge with Intel AES-NI, which provides seven instructions to accelerate the most compute-intensive AES algorithms. By offloading this processing to dedicated circuits within the processor, much of the latency is eliminated, and server processors are free to focus on their primary data-processing functions. Intel AES-NI is supported in all current Intel Xeon processors, including the Intel Xeon processor E7 family, which is used in the SAP HANA platform.

Tripling Data Capacity for SAP HANA*

The SAP HANA platform was developed jointly by SAP and Intel to deliver unprecedented performance and scalability for complex analytics acting on large data sets. More recently, Intel and SAP have collaborated to optimize SAP HANA for a new generation of Intel® server components.

• The Intel® Xeon® processor E7 v2 family provides dramatic performance and scalability enhancements versus previous generation processors, including up to 2x faster performance for complex, ad hoc queries,6 and up to 3 times the memory capacity6 (up to 6 TB per 4-socket server and up to 12 TB per 8-socket server). For more information, visit: www.intel.com/content/www/us/en/processors/xeon/xeon-processor-e7-family.html

• The Intel® Solid-State Drive DC S3700 Series provides high-performing persistent storage for SAP HANA, which is essential for implementing high availability with zero data loss and without sacrificing in-memory performance. Configuring SSD-to-memory capacity in a four-to-one ratio allows the in-memory database to spill over into a high-speed RAID array for logging, user space requirements, extended data capacity, time series data, and warm cache solutions. For more information, visit: www.intel.com/content/www/us/en/solid-state-drives/solid-state-drives-dc-s3700-series.html

• The Intel® Ethernet Converged Network Adapter X520 Family offers some of the most flexible and scalable Ethernet adapters available for today’s data centers. These adapters support unified networking and data center bridging (DCB). DCB enhances the network-attached storage and Internet small computer interface (iSCSI) by offering traffic differentiation at the link layer. DCB can be used to converge a variety of applications, such as local area networks, storage area networks, and high-performance computing. For more information, visit: www.intel.com/content/www/us/en/network-adapters/converged-network-adapters.html

Together, these advances dramatically increase the per-node scalability of SAP HANA, so enterprise customers have more headroom for supporting large-scale SAP Business Suite* applications and other mission-critical workloads.


b On a 4-socket natively-connected platform: Intel® Xeon® processor E7 family supports 64DIMMs, max memory per DIMM of 32GB RDIMM; Intel® Xeon® processor E7 v2 family supports 96DIMMs, max memory per DIMM of 64GB RDIMM. This enables a 3x increase in memory.
Intel AES-NI not only accelerates encryption, but also strengthens it. Software-based encryption algorithms can be vulnerable to sophisticated side-channel attacks that use indirect methods to decipher encryption keys. Offloading key encryption processes to dedicated circuits within the processor provides better protection against such attacks.

Intel® Secure Key

Encryption is only as secure as the keys that are used to encrypt the data. If an encryption key is stolen or compromised, the associated data is at risk. Traditionally, security vendors have relied on the software-based pseudo random number generators (RNGs) in today’s operating systems to generate encryption keys. However, flaws have been found in pseudo RNGs that can be used to compromise data security using side-channel attacks to decipher encryption keys.

Intel Secure Key provides high quality keys using a hardware-based RNG that is included in the latest generation of Intel Xeon processors. Intel Secure Key generates truly random numbers based on unpredictable thermal fluctuations within the chip. The RNG is automatically detected and used by leading operating systems. It is completely transparent to applications and supports scalable key generation for demanding enterprise applications.

By supporting both Intel AES-NI and Intel Secure Key, the Vormetric Data Security Manager increases encryption security while simultaneously reducing the performance impact on both applications and the supporting infrastructure.

Notes on platform support:

- **Intel AES-NI** is supported in the Intel Xeon processor E7 v2 family, as well as the previous-generation Intel Xeon processor E7 family, both of which are certified for the SAP HANA platform. (Intel AES-NI is also supported in the Intel Xeon processor E5 and E3 families.)

- **Intel Secure Key** is supported in the Intel Xeon processor E7 v2 family (and also in the Intel Xeon processor E3 v2 and E5 v2 families).

Proven Performance Gains

Vormetric Data Security is optimized for Intel AES-NI and Intel Secure Key, so strong data encryption can be implemented pervasively without sacrificing application performance. In 2012, Intel conducted a Transaction Processing over XML (TPoX) benchmark to test Vormetric encryption technology using the Intel Xeon processor E5 family with Intel AES-NI. Results showed that implementing data encryption in a traditional relational database reduced peak transaction throughput by less than 4% compared with a similarly configured server that did not encrypt data. According to the report, “...the performance overhead for encrypting this mission-critical workload at heavy system utilization was almost negligible.”

More recent performance tests were performed in the SAP Co-Innovation Lab (COIL) using servers based on the Intel Xeon processor E7 v2 family. The results of these tests show additional and dramatic performance gains versus previous-generation processors. The Intel Xeon processor E7 v2 family provides up to 50% more execution resources and supports up to 3 times the memory capacity of the previous-generation Intel Xeon processor E7 family (see the sidebar, “Tripling Data Capacity for SAP HANA”). In performance tests with Vormetric Data Security, Vormetric engineers demonstrated that this new processor family improves data encryption performance by up to 75% (see Figure 3). These performance gains offer significant value in SAP HANA environments, enabling strong data encryption without significantly impacting the performance that is so critical in real-time business environments.

Faster, Stronger Encryption with the Intel® Xeon® processor E7 v2 family

![Graph showing performance comparison](image)

Figure 3. Performance tests have shown that the Intel® Xeon® processor E7 v2 family increases Vormetric Data Security® encryption performance by roughly 75% versus the previous-generation Intel Xeon processor E7 family. These dramatic gains make it even easier for businesses to encrypt sensitive data without slowing performance for data-intensive applications, such as SAP HANA.
Security in the Cloud for SAP HANA*

Summary

SAP HANA is transforming the way companies compete, allowing them to analyze all available data almost instantly and integrate the resulting insights into real-time business processes. With on-demand infrastructure solutions from Virtustream, businesses can combine this breakthrough business capability with the agility and cost efficiencies provided by a hosted cloud environment, without compromising performance, availability, security, or compliance.

Virtustream is already hosting more than 100 SAP landscapes for enterprise customers. With the addition of Vormetric Data Security and the support of Intel® security technologies, Virtustream will provide even better security and compliance for SAP HANA implementations. Data encryption and access controls will be extended and enhanced, and customers will maintain complete control over their data, encryption keys, and access policies.

About the SAP® Co-Innovation Lab

SAP collaborates with a large community of hardware, software, and service providers to develop, test, and showcase multi-vendor solutions based on SAP HANA and other SAP products. Much of this collaboration takes place in the SAP Co-Innovation Lab (COIL). This global network of laboratories provides infrastructure, expertise, and other resources that help vendors come together with SAP development and business teams. By fueling collaboration across the global SAP ecosystem, COIL helps to speed the delivery of proven solutions that meet the real needs of business customers.

For more information, visit: http://scn.sap.com/community/coil

1On a 4-socket natively-connected platform: Intel® Xeon® processor E7 family supports 64DIMMS, max memory per DIMM of 32GB RDIMM. Intel® Xeon® processor E7 v2 family supports 96DIMMs, max memory per DIMM of 64GB RDIMM. This enables a 3x increase in memory.

2Better performance at lower total cost claim based on Intel estimated SPECint_rate_base2006 results and pricing of comparable 4-socket rack server using Intel® Xeon® processor E7-4890 v2 (37.5M Cache, 2.8 GHz, 15-Core) to IBM POWER® 750 using POWER® (IBM Cache, 4.0 GHz, 8-Cores) as of December 2013. SPECint_rate_base2006 benchmark results: 4-chip IBM POWER® (1329 baseline score) source: www.spec.org/cpu2006/results/res2013q3/cpu2006-20130805-26129.html 4-chip Intel Xeon processor E7-4890 v2 (2280 baseline score estimated)


4No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software, may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your Service Provider for availability and functionality. For more information, visit www.intel.com/go/auththeft. Consult your system manufacturer and/or software vendor for more information.

5No computer system can provide absolute security. Requires an enabled Intel® processor and software optimized for use of the technology. Consult your system manufacturer and/or software vendor for more information.


7On a 4-socket natively-connected platform: Intel® Xeon® processor E7 family supports 64DIMMS, max memory per DIMM of 32GB RDIMM. Intel® Xeon® processor E7 v2 family supports 96DIMMs, max memory per DIMM of 64GB RDIMM. This enables a 3x increase in memory.

8Results are based on SAP COIL preliminary tests. The tests were performed on a single, preproduction server platform configured with the Intel® Xeon® processor E7 family and then with the Intel® Xeon® processor E7 v2 family running the SUSE Linux® Enterprise Server 11 SP2 operating system with the Vormetric kernel module. The test was activated by a command to the Vormetric kernel module on a single-threaded, quieted system (Intel® Hyper-Threading Technology was not used and there was no I/O activity). Encryption and decryption were applied to in-kernel memory buffers ranging in size from 8-512K. Measurements were performed after cache warming, and a very fast memory copy procedure was used as the baseline test.

Software and workloads used in performance tests may have been optimized for performance only on Intel® microprocessors. Performance tests, such as SYSMark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

Information in this document is provided “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or noninfringement of intellectual property. Intel disclaims any representation or warranty that this document and/or the information contained herein will be error-free, complete, accurate, or without omission of material information, or that the information or services will be available at any particular time or location.

Intel does not undertake any duty to update any information in this document. Intel reserves the right to make changes to this document and/or the products described in it at any time without notice, and hereby disclaims any liability to do so.

Specifications and other information concerning the products described herein are provided by Intel Corporation and its subsidiaries (“Intel”) purely as a convenience to the reader, and are accurate and reliable only to the extent provided by Intel. Intel assumes no responsibility for any errors that may appear in this document, nor does it make or convey any representation or warranty, express or implied, relative to the accuracy, reliability, completeness, or usefulness of the information contained in this document. Intel assumes no liability for any damages or loss that may arise from the use of, or reliance upon, any statement or representation contained in this document or in any other document related thereto.

Intel recognizes and respects the intellectual property rights of others, and we have been advised that the products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to:
www.intel.com/design/literature.htm

Copyright © 2014 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.

Printed in USA 0214/RAS/9651/PDF Please Recycle 33016-001US