Securing SAP Clouds

Version 1.1
Date: February 6, 2017

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report is licensed by Onapsis.

Onapsis cybersecurity solutions automate the monitoring and protection of your SAP applications, keeping them compliant and safe from insider and outsider threats. As the proven market leader, global enterprises trust Onapsis to protect the essential information and processes that run their businesses.

Headquartered in Boston, MA, Onapsis serves over 200 customers including many of the Global 2000. Onapsis' solutions are also the de-facto standard for leading consulting and audit firms such as Accenture, Deloitte, E&Y, IBM, KPMG and PwC.

Copyright

This report is licensed under Creative Commons Attribution-Noncommercial-No Derivative Works 3.0.

http://creativecommons.org/licenses/by-nc-nd/3.0/us/

Securing SAP Clouds

Table of Contents

Introduction

Every enterprise uses cloud computing services to some degree. Tools such as Gmail, Twitter, and Dropbox are ubiquitous; as are business applications like Salesforce, ServiceNow, and QuickBooks. Cost savings, operational stability, and reduced management effort are all proven advantages. But IT and security professionals feel considerable trepidation at the prospect of moving moving back-office infrastructure – systems at the heart of business – into the cloud. For several years now cloud service providers have offered comprehensive security controls, tackling the largest impediment to adoption, and — when properly architected — offer better overall security than on-premise solutions. But how to assemble a security strategy for complex applications such as SAP is far from clear, nor how to adapt existing security controls to an unfamiliar environment where only partial control is available.

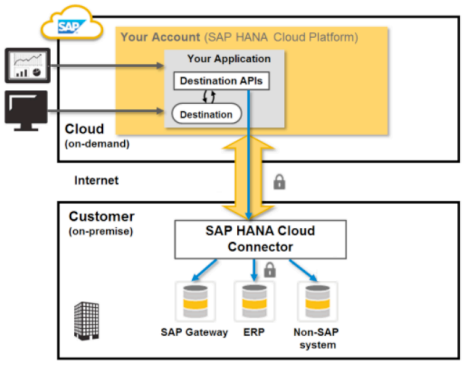
We have been receiving an increasing number of questions on SAP cloud security, so this research paper tackles the main security issues for SAP cloud deployments. When we originally scoped this project we intended to focus on the top five questions we heard, but we quickly realized that would grossly under-serve our audience, and instead we should help to design a more comprehensive security plan. So we chose to instead examine a broad range of concerns, including how cloud services differ, and then map existing security controls to fit cloud deployments. In some cases this is as simple as changing a security tool, while in others it means negotiating directly with your cloud provider. In this research paper we will highlight the division of responsibility between you and your cloud vendor, which tools and approaches are cloud-viable, how to adapt your security model, and advice for putting together a complete security program for SAP cloud services.

The Need for a Security Strategy

Cloud computing infrastructure faces many of the same challenges as traditional on-premise IT. We are beyond legitimate worries that the cloud is “less secure”. Properly implemented, cloud services are as secure as on-premise applications – in many cases more so. But their *proper implementation* is tricky – if you simply “lift and shift” your old model into the cloud, we know from experience that it will be less secure and cost more to operate. To realize the advantages of the cloud you need to leverage new features and capabilities – which demands a degree of re-engineering for architecture, security program, and process.

SAP cloud security is tricky. The central issue is that there is no single model for what an “SAP Cloud” looks like. From many, it’s HANA Enterprise Cloud (HEC), a private cloud within the existing on-premise domain. Customers who don’t modify or extend SAP’s products can leverage SAP’s Software as a Service (SaaS) offering, or adopt a ‘private cloud’ variant in HCE. But a growing number of firms we speak with are instead moving to SAP’s HANA Cloud Platform (HCP), a Platform

as a Service (PaaS) bundle of the core SAP HANA application with data management features (see diagram). Alternatively, various other cloud services can be bundled or linked to build a cloud platform for SAP – often including mobile client access 'enablement' services and supplementary data management, typically focused on big data analytics and data mining.



But our researched showed many customers do not limit themselves only to SAP software – they blend SAP cloud services with other major IaaS providers, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure to create 'best-of-breed' solutions. In response SAP has published widely on its vision for cloud computing architectures, so we needn't cover that in detail here. The point is SAP promotes multi-cloud — *as opposed to hybrid on-premise pictured above* — deployments centered around HANA Cloud Platform (HCP) in conjunction with public IaaS clouds which are better suited to real time event processing and generic application services. There is a lot to be said for the flexibility of this model – it enables customers to deploy applications into the cloud environments they are comfortable with or to choose the best for their applications. But this flexibility comes at the price of added complexity, making it more difficult to craft a cohesive security model. So we will focus on use of the HCP service, discussing security issues around hybrid architectures as they come up.

These topics address the major concerns we hear from customers. But cloud security needs to be integrated into many or most aspects of a cloud platform (including identity, encryption, key management, authorization, assessment, logging, and monitoring) so this subject is both broad and deep. We cannot possibly cover all this material in detail so we will limit discussion to key focus areas: highlighting major differences between cloud and on-premise approaches, providing guidance for most scenarios.

Service Contracts

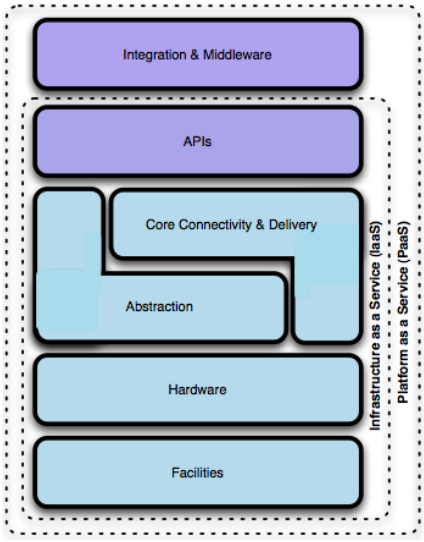
Contracts determine the division of responsibility between a cloud provider and you as tenant, highlighting specific concerns which you must address in your cloud service contract. Renting a platform from a service provider does not mean you can afford to cede all security responsibility. Cloud services unburden your team from many traditional IT jobs, but you must still address security. The cloud provider assumes some security responsibilities, but many still fall into your lap, while others are shared. The administration and security guides don't spell out all the details of how security works behind the scenes or what the provider *really* provides. Grey areas should be defined and clarified in your contract up front. Incident response is a terrible time to discover what SAP actually offers.

SAP's brochures on cloud security imply you will tackle security in a simple and transparent way. That's not quite accurate. SAP has done a good job providing basic security controls, and they have obtained certifications for common regulatory and compliance requirements on their infrastructure. But you are renting a platform, which leaves a lot up to you. SAP does not provide a good roadmap of what you need to tackle, or a list of topics to understand before you deploy into an SAP HCP cloud.

Our first goal for this section is to help you identify which areas of cloud security you are responsible for. Just as important is identifying and clarifying shared responsibilities. To highlight important security considerations which are generally *not* discussed in service contracts, we will guide you through assessing exactly what a cloud provider's responsibilities are, and what they do not provide. Only then does it become clear where you need to deploy resources.

Division of Responsibility

Readers who have worked with SAP HANA already know what it is and how it works. Those new to cloud may understand the Platform as a Service (PaaS) concept, without full awareness of what it means structurally. To highlight what a PaaS service provides, we'll borrow Christopher Hoff's cloud taxonomy for PaaS; this nicely illustrates what SAP provides.



This diagram includes the components of IaaS and PaaS systems. Obviously the facilities (such as power, HVAC, and physical space) and hardware (storage, network, and

computing power) portions of the infrastructure are provided, as are the virtualization and cluster management technologies to make it all work together. More interesting, though: SAP HANA, its associated business objects, personalization, integration, and data management capabilities, are all provided – along with APIs for custom application development. This enables you to focus on delivering custom application features, tailored UI, workflows, and data analytics, while SAP takes care of everything else.

The Good, the Bad, and the Uncertain

The good news is that this frees you up from lengthy hardware provisioning cycles, network setup, standing up DNS servers, cluster management, database installations, and the myriad things needed to stand up a data center. And all the SAP software, middleware components, and integration are built in and available on demand. You can stand up an entire SAP cluster through their management console in hours instead of weeks. Scaling up and down is far easier, and you are only charged for what you use.

The bad news is that you have no control over underlying network security; nor do you not have access to network events to seed your on-premise DLP, threat analysis, SIEM, and IDS systems. Many traditional security tools therefore no longer function, and event collection capabilities are reduced. The net result is that you become more reliant than ever on the application platform's built-in security, but you do not fully control it. SAP provides fairly powerful management capabilities from a single console, so administrative account takeovers or malicious employees can cause considerable damage.

There are many security details your cloud vendor may share with you, but wherever they don't publish specifics you need to ask. Things like segregation of administrative duties, data encryption and key management, employee vetting process, and how they monitor their systems for security events. You'll need to dig in a bit and ask for details of the security capabilities they have built into the platform.

Contract Considerations

At Securosis we call the division between your security responsibilities and your vendor's "the waterline". Anything above the waterline is your responsibility, and everything below is your vendor's — in this case likely SAP. In some areas, such as identity management, both parties have roles to play. But generally you cannot see below the waterline – how the provider performs their work is confidential. You have very little visibility into what they do, and very limited ability to audit it – for both SAP and other cloud services.

This is where your contract comes into play. If a service is not in the contract, there is a good chance it does not exist. You might think you know how a service will work and what data will be provided, but there is a good chance you're wrong. Unfortunately you often only find out when something goes wrong. It is critical to avoid assumptions about what a cloud provider offers or will do, if or when something like a data breach occurs. Get everything in writing.

The following are several areas we advise you ask about. If you need something for security, include it in your contract.

Event Logs: Security analytics require event data from many sources. Network flows, `syslog`, database activity, application logs, IDS, IAM, and many others are all useful. But like most cloud providers, SAP's HCE does not provide these sources. Further, as HCE is inherently is multi-tenant, logs may include activity from other tenants and therefore cannot be available to you. For platforms and applications you manage in the cloud, event logs are available. Catalog what sources you rely on today to determine what is available and what's missing. In most cases you can switch to more application-centric event sources to collect required information. You also need to determine how data will be collected – agents are available for many things, but some logs must be gathered via API requests.

Testing and Assessment: SAP states they conduct internal penetration tests to verify common defects are not present, and attempts to validate their own business logic functions as intended. This does not extend to your custom applications. Additionally, SAP may or may not allow you to run penetration tests, dynamic application security testing, or even remote vulnerability assessment – against your applications and/or theirs. This is a critical area you need to understand, to determine which of your application security efforts can continue. Most cloud service providers allow limited external testing with advance permission, and some scans can be conducted internally – against only your assigned resources. You need to specify these activities in your contract — including which tests will be performed, how permission is obtained if needed, timeframes, and test scopes. The good news is that some of your existing application scanning responsibility is reduced because your provider takes care of it. The bad news is the extra work to set up a new assessment process in the cloud.

Breach Response: If a data breach occurs, what happens? Will SAP investigate? Will they share data with you? Who is at fault, and who decides? If federal or local law enforcement becomes involved, will you still be kept in the loop? We have witnessed cases where other cloud service vendors have not assisted tenants with event analysis, and others where they declined to share event data – only confirming an event took place. This is an area your security team needs to be comfortable with, especially if your firm runs a Security Operations Center. Because you won't control the platform or infrastructure, your analysis is limited. This shared responsibility must be spelled out in your contract.

Certifications: SAP obtains periodic certifications on their infrastructure and platforms. Things like PCI-DSS, ISO 9001, ISO 27001, ISAE 3402, and several others we won't bother to list here. The key is whether SAP has the certifications you need, and exactly which *parts* of their service are certified — only certain elements of their cloud service are certified. This will give you a good idea of where their efforts ended and yours must pick up. Additionally, some audits only cover what the service provider lists as important, omitting items you consider relevant. You can compare their certification reports to your current certifications for on-premise systems to ensure you will be sufficiently covered.

Segregation of Duties: SAP's administrators have access to your platforms. Most cloud services consumers worry about admins accessing data stores, so database encryption is needed. You will need to decide how to encrypt data and where to store encryption keys. In most cases we find in-cloud offerings insufficient, so a hybrid model is employed.

Data Privacy Regulations: Additional data privacy concerns may arise, depending on which data center you choose. SAP will correctly say you need to understand which laws apply to *you* because both compliance and legal jurisdiction change depending on your data center's geographic region and your organization's footprint. SAP states they adhere to German government and EU requirements for data processors, as well as US/EU Privacy Shield regulations, but you will need to independently verify that these meet your requirements, and develop a mitigation plan for any unaddressed items. Additionally you need to reconsider these issues if you select fail-over data centers in different regions. Some compliance and privacy laws and requirements follow the data, meaning they continue apply even with a change in jurisdiction.

Keep in mind that public cloud service providers don't like what we suggest here, and make it difficult to obtains some details, and are typically not open to negotiations unless you're spending large sums of money with them. They are not really set up to provide custom security and compliance offerings, are reluctant to share data, and don't like to go into detail on operations. We encourage you to ask for clarification on what the service offers, but don't expect tailored security or compliance service. It's set up to be on-demand and self-service, with standard pricing.

As Henry Ford once said, "Customers can have their car painted any color they like, so long as it's black." With cloud services customers can have anything they want, so long as it's already on the menu. Wanting something different is a bit like arguing with a vending machine – trying to get a Pepsi from a Coke machine rarely works. Cloud vendors are designed to provide a basic service, assuming *you* will build any needed customization on top of their basic service. Unless you spend absurd amounts of money, which is why custom services are unusual. This goes for general features as well as security add-ons, but you need to understand what is actually provided, and at least *ask* for what you need.

You will have less control over infrastructure and no physical access to hardware. The people managing the platform don't report to you. To compensate for this lack of control you will rely more on contracts, service level agreements, and audit reports from the provider on their service. Be aggressive in requesting documentation on which security controls are provided and how they work; some documents are not provided to the general public. Request compliance reports to see where your cloud vendor was tested, and where they weren't. There are many things you cannot bargain for, but you will have more success requesting data and clarification on what SAP provides. But for anything critical (and anything non-critical, too), if it's not spelled out in the contract, don't expect it to work as you want or need. This is a lot of up-front work to do, but it pays for itself down the line.

Cloud Security Architecture

We need to discuss several keys differences in cloud architecture which directly impact security – aspects you need to consider when migrating to cloud services. Taking full advantage of these native cloud characteristics makes security both easier to implement and more effective.

You're Doing It Backwards

In our experience, as most companies move business-critical applications to the cloud, they typically do it backwards. Firms begin to get familiar with the cloud by investigating cheap cloud storage options. With a toe in the water they next place some development, testing, and failover servers in the cloud to backstop on-premise systems. These are less critical than production servers, where firms do not tolerate missteps. By default firms design their first cloud systems and applications to mirror what they already have in existing data centers. That means they carry over the same architecture, network topology, operational model, and security models. Developers and operations teams work in a familiar model, leverage existing skills, and focus on learning the nuances of their new cloud service. More often than not, once these teams are up to speed, they expect to migrate production systems fully to the cloud. Logical, right? It's all good until you move production to the cloud, when it goes very wrong.

This is the "Lift and Shift" model of cloud deployment, where you create an exact copy of what you have on-premise, just running on a service provider's platform. The issues are many and varied. This approach fails to take into account the inherent resiliency of cloud services. It doesn't embrace automatic scaling up and down for efficient resource usage. To us, the most important failures are around security capabilities. This approach fails to leverage hyper-segregation, failover, granular IAM capabilities, automated patching, or agile incident response – all of which enable companies to respond to security issues faster, more efficiently, and more accurately than possible with pre-cloud systems.

Network and Application Segmentation

Most firms have a security 'DMZ', an untrusted zone between the outside world and their internal network, and a flat internal network inside that. There are good reasons this less-than-ideal setup is common. Segregating networks in a data center is hard – users and applications leverage many different resources. It often requires special hardware and software, and becomes expensive to implement and difficult to maintain. Attackers often jump from where they initially breach a company network, either "East/West" between servers, or "North/South" to gain control of additional applications. We segregate networks and applications to prevent 'pivoting' this way, and to contain breaches.

But this is exactly the sort of capability provided by default with cloud services. If you're leveraging SAP's HANA Cloud Platform, or running SAP HANA at an IaaS provider like AWS, network segregation is built in, with 'default-deny' being the norm. For example, AWS offers VPC and security zones for segregation, and disables inbound ports and protocols by default, eliminating many avenues attackers use to penetrate severs. You open ports and protocols only as you need them. Additionally, SAP HCP is inherently multi-tenant services, so individual accounts and their assigned resources are fully segregated and protected from other users. This enables you to limit the "blast radius" of any compromise to the resources in a single account. Application by application segregation is not new, but greatly improved ease of use makes it newly feasible in the cloud. In some cases you can even leverage both PaaS and IaaS simultaneously – letting one cloud serve as an "air gap" for another. Your cloud service provider offers added advantages by running under different account credentials, roles, and firewalls. You can specify exactly which users can access specific ports, require TLS, and limit inbound connections to approved IP addresses.

Immutable Servers

"Immutable servers" have radically changed how we approach security. Immutable servers do not change once they go into production. You can completely remove login access to the server. PaaS providers leverage this approach to ensure their administrators cannot access your underlying resources. In HANA, for example, your team only logs into the application layer, and the underlying servers only offer administrator logins for the service provider – for customers that capability is disabled. In IaaS it is far more powerful, as it means there can be *no* administrative access to servers. Your operating systems and applications cannot be changed, and administrative ports and accounts are disabled entirely. If you need to update an OS or application, you alter the server configuration or select a new version of the application code in a cloud console, and then start new application servers and shut down the old ones.

SAP does not yet leverage immutable servers in HCP, but it is on their roadmap. Regular automated replacement is a huge shock, which takes most IT operations folks a long time to wrap their heads around, but something you should embrace early for security and productivity gains. Preventing hostile administrative access to servers is a key advantage, and auditors love that third parties do not have access.

Blast Radius

This concept limits which resources an attacker can access after successful compromise. We reduce blast radius and preventing attackers from pivoting elsewhere by reducing the number of accessible services. There are a couple approaches. One is to use VPCs and the cloud's native hyper-segregation. Most vulnerable ports, protocols, and permissions are simply unavailable. Another approach is to deploy different SAP features and add-ons in different user accounts, leveraging the isolation capabilities built into multi-tenant clouds. If a specific user or administrative account is breached, your exposure is limited to the resources in that account. This sounds radical but it not particularly difficult to implement. Some firms we have spoken with manage hundreds – or even thousands – of accounts to segregate development, QA, and production systems.

Network Visibility

Most firms we speak with have a firewall to protect their internal network from outsiders, and identity and access management to gate user access to SAP features. Beyond that most security is not at the application layer – instead it is at the network layer. Intrusion detection, data loss prevention, extrusion filtering, user behavior monitoring, and similar security capabilities all work by inspecting network traffic. In the cloud you must rely much more heavily on application-layer security, along with application logs and agent-based monitors, to collect events for security analysis. You need to understand which network-oriented security measures become obsolete because the attack vectors they address have become non-issues, and find suitable replacements to address threats which remain.

Cloud Security Operations

Patching and Change Management

In general, all organizations hate to patch. It requires server downtime, synchronizing different teams to schedule installation, and then testing before applications and servers can go back into production. Small manual fixes and configuration changes are often needed to make the new code work, and all too often they never make it outside administrator skulls into change management systems. And there is always a chance a patch may break an application, requiring patch rollback and recovery to a previous state.

In PaaS clouds, infrastructure and application patching is handled for you on a regular basis. It occurs quietly behind the scenes, without service interruption, often without the customer aware of any changes. Providers can manage this because each logical server is actually multiple virtual servers, behind a load balancer, regularly cycled to keep current and healthy. But the platform is fully API-enabled so you can also leverage these capabilities to roll out patches for your own applications using the HCP cloud.

Under IaaS you run multiple instances of your applications in an autoscale group behind your load balancer, rolling out new patched instances as needed. You can leave un-patched versions up and running, allowing load balances to steer traffic away from them, until you are satisfied and ready to terminate the older instances. When something goes wrong with a server or application instance, it's easiest to replace it with a fresh image. You can automatically scan for misconfigurations in metadata, the network, or applications across your HANA instance, and remediate with vendor APIs.

In some cases cloud providers roll out one or more patches per day, so there is a shrinking window for attackers to exploit known flaws. As a reference for how effective this can be, some cloud providers were able to patch hundreds of thousands of servers against the Heartbleed vulnerability in under 48 hours, before attackers could weaponize the exploit. This is a tremendous security advantage. It means we do not need to be three, six, or twelve months behind on security patches – to SAP, servers, and our own applications. Most attackers leverage known vulnerabilities which have not been patched, so fast-flux patching is generally too fast for them react. It also means that if an attacker does manage to compromise a server or application instance, they cannot "camp out" there long before their victim servers are replaced.

Incident Response

When a company discovers malware on its network, the long process of discovering which servers are infected begins. For each infected server, most organizations physically quarantine the machine, make backups, bring the physical server or image to the Security Operations Center for analysis,

and then requisition a new server. We bring up incident response because it needs to be entirely re-examined for the cloud. If you are using SAP's PaaS server for HANA and believe there has been a compromise, you are limited to application-layer logs and whatever SAP has contractually guaranteed to provide – typically not much. But IaaS and PaaS enable you to automate most of your response, which had traditionally been highly labor-intensive.

With IaaS you have even greater control over resources. With a very small set of API calls to your cloud service you can isolate a server, pull instance metadata, snapshot all storage and memory, change ownership and access rights of the live running instance to the security group, launch analysis tools, and launch a replacement server. It all runs within seconds. One of the most time-consuming security tasks for IT operations can be reduced to a background utility script. This is self-healing infrastructure, with operations and orchestration capabilities to make it reality.

To achieve fundamentally better security at lower cost you need to redesign application deployments a bit. Realizing the benefits of Agile cloud operations requires investing some time. You need to understand how cloud services work and to create automation scripts which embody your processes for automated patch management, secure deployment, and incident response. You will need to move much of your operations to a continuous integration model – code, scripts, and manifests must be automatically assembled; security credentials must be issued; and deployment must become automatic. Hopefully by now we have made clear that in the cloud there is considerable convergence between what security teams prescribe and how operations teams work. Leveraged properly, this convergence produces both productivity and security advantages. The best part is that these features are included in the cloud service you are already paying for.

That said, there is still a lot of work to do. To implement segregated application stacks and/or segregated networks, you need to alter your deployment model for applications to leverage granular isolation. To leverage "best of breed" cloud services you will re-architect or even break apart applications into smaller services, each running on the cloud best suited to its task. To take advantage of immutable servers you need to standardize application configurations, and for HANA on IaaS to script your server startup and configuration processes. To patch with agility you must evolve how you apply and test patches along with the rest of your patch management process. Most of Operations' work to support incident response moves into a straightforward script. This will save hours of manual labor – once you script the process and set up connections for Security Operations to receive server images. But over the long term it requires much less work, and integrates security into process.

Security Services Integration

It is time to discuss the foundational elements of an application security program for SAP HCP deployments. Without direct responsibility for hardware and physical networks you lose the traditional security data capture points for traffic analysis and firewall technologies. The net result is that *your application security program becomes more important than ever* as the area you still control. Yes, SAP provides some network monitoring and DDoS services, but *your* options are limited, they don't share much data, and what they monitor is not tailored to your applications or requirements.

SAP provides many of the core security features you need, but their model is largely based on built-in identity management and access control capabilities. The following items are core features of SAP HCP:

Identity Management: The SAP Hana Cloud Platform provides robust identity management features. It supports fully managed HCP identities, as well as many on-premise identity services (*i.e.:* Active Directory) and third-party cloud identity management services. These services store and mange user identities along with role-based authorization maps to define authorized user access to your resources.

Federation and Token-based Authentication: SAP supports traditional user authentication schemes (*e.g.:* user name and password), but also offers single sign-on. In conjunction with the identity management services above, HCP supports several token-based authenticators such as Open Authorization Framework (OAuth), Security Assertion Markup Language (SAML), and traditional X.509 certificates. A single login grants users access to all authorized applications from any location, from any device.

Encryption: Despite being an in-memory database, HCP leverages persistent (disk-based) storage. To protect this data HCP offers transparent Data Volume Encryption (DVE) as a native 'persistence encryption' capability for your database, as well as its transaction logs. When using persistence you will need to configure the encryption options because they are not enabled by default. If you run SAP HANA in an IaaS environment, several third-party transparent data encryption options are also available, or you can use your IaaS provider's encryption services. Each option has cost, security, and ease-of-use considerations.

Key Store: If you are encrypting data, somewhere there are encryption keys and some systems have access to them. Anyone or any service with access to keys can encrypt and decrypt data, so careful selection of a key store to manage keys is critical to both security and regulatory compliance. HCP's key store is fully integrated into its disk and log file storage capabilities, which makes it very

easy to set up and manage. Organizations who do not trust their cloud service provider, or subject to data privacy regulations which require they maintain direct control over encryption keys, need to integrate their on-premise key management solution with the HCP installation. If you are running SAP HANA in an IaaS environment you have access to several third-party key management services – both in the cloud and on-premise – as well as whatever your IaaS provider offers.

Management Plane: A wonderful aspect of HANA's cloud service is full administrative capabilities through the 'Cockpit' web interface, API calls, or a mobile application. You can configure, specify deployment characteristics, enable logging, etc. This is a wonderful convenience for administrators, but a potential nightmare for security because an account takeover means your *entire cloud infrastructure* can be taken over and exposed. It is critical to disallow password access and leverage token-based access and two-factor authentication to secure your admin accounts. If you are leveraging an IaaS provider you can disable the `root` administrator account and assign SAP sub-components and functions to individual administrators.

These are foundational elements of an application security program, and we recommend leveraging the capabilities SAP provides. They work, and reduce the cost and complexity of managing your cloud infrastructure.

Application Security

SAP's overarching security model leaves several large gaps which you need to address with third-party capabilities. SAP publishes many of the security controls they implement for HCP, but they do not share these capabilities with customers. So for many security controls you must still provide your own. Areas you need to address include:

Assessment: This is one of the most effective means of finding security vulnerabilities with on-premise applications. SAP's scope and complexity make it easy to accidentally misconfigure insecurely. When moving to the cloud SAP takes care of many of these issues on your behalf. But even with SAP managing the underlying platform there are still add-on modules, configurations, and your own custom code to be scanned. Running on IaaS, assessment scans and configuration management remain a central piece of an application security program. You will need to adjust your deployment model because many of the more effective third-party scanners run as standalone machines (in AWS, an AMI), while others run on a standalone central server supported by remote 'agents' which perform the actual scans. You will likely need to adjust your deployment model from what you use on-premise, because in the cloud you should not be able to address all servers from any single point within your infrastructure.

Monitoring: SAP regularly monitors their own security logs for suspicious events, but they don't share findings or tune their analysis to support *your* application security efforts, so you need to implement your own monitoring capability. Monitoring system usage is one security control you will rely on much more in the cloud, as your proxy for determining what is going on. Your traditional IDS, IPS, firewalls, and network monitoring systems don't work well on cloud infrastructure, because software-defined networks don't provide the events or access these security platforms are designed around.

It is important to understand that SAP HANA is very different than many other enterprise applications, so generic tools don't work very well with HANA to begin with. Some security monitoring products from third parties which we recommend are specifically designed to understand SAP functions, programs and transactions. They show you how HANA is being used and by whom, and can perform behavioral assessments to detect anomalies activities. They can see API calls and usage and compare these requests against security policies to make dynamic estimation if a request is legitimate or not. Monitoring also captures events which do not appear in audit logs or cloud provider logs, which makes it particularly useful for auditing, compliance, and forensic investigation.

Logging and Auditing: HCP provides database logs, default trace logs, and HTTP access logs. But logs from things like Cockpit and administrative activity are unavailable. As mentioned above,

you may need to supplement activity logs with monitoring services. In IaaS, basic event logs of API calls and resource requests are captured by the service if you choose to enable logging; logs can be saved to disk, raw storage (such as S3 buckets), Splunk, your SIEM, or logging tools of your choice.

Configuration Management: To promote consistency across the cloud SAP records deployment and configuration data in a proprietary XML document so that resources instantiate with the consistent platforms, patch revisions, and configurations. But this is a proprietary document and SAP does not share the specifics with HCP customers. That said, the approach provides consistency, giving each application server the same modules, versions, and configuration. For PaaS and IaaS environments we recommend capturing settings into a standard template and using it to launch new services.

Penetration Testing: We are big fans of penetration testing at Securosis. Pen testers commonly discover unknown defects in applications and deployments, because they examine and probe applications in ways developers and operations teams do not. So you may be disappointed to learn that you cannot test cloud services. Many cloud providers prohibit it altogether; others allow you to test only your own applications, with prior approval. SAP performs penetration testing on their own services, but does not currently allow customers to do the same. This could change in the future, so we encourage you to ask SAP and see if they will allow it under controlled circumstances.

Securing Your Code

Several other aspects of application security fall under application *development*, which we cannot address in depth here, despite its importance to your security program. SAP advocates use of Cloud Foundry – either open source or commercial variants – for application development. Cloud Foundry is what we call "security neutral": it can be made secure but does not inherently provide security, so code integrity is up to you. Similarly, for containers like Docker you need to ensure you pull apps from trusted repositories and ensure your container build process is secure.

SAP offers the App Center as a secure repository, with add-ons and full applications to enhance and extend your SAP applications, but it also helps ensure you don't accidentally download infected software. And as many organizations quickly discover when developing applications for the cloud, breaking apps into smaller micro-services produces dividends in scalability, reduced complexity, and resiliency. Finally, development teams using Continuous Integration can leverage on-demand cloud resources to stand up replicas of your production environment, perform private functional and security testing, and shut down resources when finished.

To recap, you will focus more security resources on application security than ever before. Even so, the potential loss of penetration testing data on your environment requires greater focus on monitoring application usage. Regardless, leveraging a combination of third-party tools and cloud-native features, your cloud applications can be far more secure than the on-premise variants. It requires up-front planning but rewards you with improved security *and* the operational benefits of better scalability, easier management, and lower cost.

Summary

Securing SAP's Hana Cloud Platform requires much more thought than the on-site installations you are familiar with. Cloud services can accommodate traditional security models, but reward those who move away from a "Lift and Shift" approach to embrace their native capabilities. Most customers we spoke with during our research leverage a hybrid model, with on-premise systems supporting HCP, and in some cases a third-party IaaS cloud, so there are clearly a lot of moving pieces to account for. But there is good news: fewer controls to worry about, as you are responsible for less of the system. The security approaches across SAP and IaaS services such as AWS are very similar, so you can employ consistent controls across multiple cloud services. Finally, once you understand how security controls change in the cloud and retool to take advantage of it, security becomes faster, more efficient, and more effective.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com.

About the Analyst

Adrian Lane, Analyst and CTO

Adrian Lane is a Senior Security Strategist with 25 years of industry experience. He brings over a decade of C-level executive expertise to the Securosis team. Mr. Lane specializes in secure application development, database and data security. With extensive experience as a member of the vendor community (including positions at Ingres, Unisys and Oracle), in addition to time as an IT customer in the CIO role, Adrian brings a business-oriented perspective to security implementations. Prior to joining Securosis, Adrian was CTO at database security firm IPLocks, Vice President of Engineering at Touchpoint, and CTO of the secure payment and digital rights management firm Transactor/Brodia. Adrian also blogs for Dark Reading and is a regular contributor to Information Security Magazine. Mr. Lane is a Computer Science graduate of the University of California at Berkeley with post-graduate work in operating systems at Stanford University.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.
- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.
- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.
- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and speak for a variety of publications and media.
- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.