

Vendor Round Table

Cloud Security

Vendors Answer IT's Questions about Cloud Security

Why you should read this document

This guide is designed to help you better evaluate different cloud technology vendors and service providers based on a series of questions posed to three cloud infrastructure providers, three managed or hosted infrastructure providers, and three cloud technology providers. Their answers include:

- Descriptions of the security components of the current offerings, including solution architecture and user benefits
- How the current offerings protect data and infrastructure and simplify compliance
- The way their solutions establish or enforce trust in the cloud
- How return on investment is demonstrated

Vendor Round Table Cloud Security

Vendors Answer IT's Questions about Cloud Security

OCTOBER 2011



Content

- 3 Introduction
- 4 Participating Vendors
- 5 Intel Guidance on Vendor Selection
- 6 Vendor Responses to IT Questions
- 42 Intel Resources for Learning More

Introduction

Compare answers from nine vendors to common IT questions to help you evaluate security products and services for the cloud.

IT departments are paying close attention to developments in cloud computing technology. The cloud offers the promise of large potential savings in infrastructure costs and improved business agility, but concerns about security are a major barrier to implementing cloud initiatives for many organizations.

Security challenges in the cloud are familiar to any IT manager—loss of data, threats to the infrastructure, and compliance risk. Cloud security is a complex topic with considerations ranging from protection of hardware and platform technologies in the data center to enabling regulatory compliance and defending cloud access through different end-point devices. The vendor landscape is equally complex. We created this guide to help you better evaluate different cloud technology vendors and service providers.

We asked nine companies to respond to a standard set of questions developed based on our own experience implementing cloud security at Intel. We posed these questions to three cloud infrastructure providers (Cisco, Citrix, and Virtustream), three managed or hosted infrastructure service providers (Carpathia, Expedient, and OpSource), and three cloud security technology providers (HyTrust, McAfee, and Trapezoid Information Security Services). This document compiles their responses.










Cloud Security Resources from Intel

The Cloud Security Vendor Round Table is part of a series of documents produced by Intel to help IT professionals plan security into cloud implementations in their organizations. This series includes the following:

- [Cloud Security Planning Guide](#). Seven steps to build security in the cloud from the ground up
- [Cloud Security Insights for IT Strategic Planning](#). Survey of IT professionals that discusses the business and technology drivers behind security in their cloud implementations, investment levels, return on investment, and outsourcing

Participating Vendors

Throughout this guide, vendors are listed in alphabetical order.

Vendor	Product	For More Information
	Carpathia* InstantOn*	www.carpathia.com
	Cloud Security Solutions	www.cisco.com/en/US/netsol/ns1066
	Cloud infrastructure solutions	www.citrix.com/cloud
	Expedient* cloud computing solutions	www.expedient.com/products/cloud-computing.php
	HyTrust* Appliance	www.hytrust.com/products
	McAfee* ¹ Cloud Security Platform	www.mcafee.com/cloudsecurity
	OpSource* Cloud Hosting	www.opsourc.net/services/cloud-hosting
	SecRAMP cloud security solutions	www.trapezoidsecurity.com
	Virtustream* xStream* Cloud Solution	www.virtustream.com

¹ McAfee is a wholly owned subsidiary of Intel.

Intel Guidance on Vendor Selection

Choosing a cloud security provider is complicated on many levels. The cloud delivery model you choose dictates what type of solution vendor or cloud services provider you will engage. Even with that decision made, the vendor landscape is characterized by countless interdependencies and relationships, both technological and business related, among vendors. And some companies offer not only software, but also hardware and services.

Whether you are implementing a private cloud on- or off-premises or a hybrid model that includes access to public cloud services, security must be a strong component of your solution. You need to evaluate how security is built into your cloud solution and what security measures are provided to protect data, platform, and access to the cloud.

General considerations related to security include:

- What is the cloud architecture?
- Does the solution enable you to meet industry or regulatory compliance requirements?
- Does the solution deploy hardware-based security to support trusted server pools?
- How are systems, data, networks, management, and provisioning segmented?
- What type of attack monitoring and reporting is available?
- What is the company's long-term strategy for the product you are evaluating?
- Is the vendor financially stable?

In addition, considerations for hosted or managed cloud solutions should also include:

- What are the provider's data center risk management and security practices?
- What auditing capabilities are provided?
- How does the provider predict and manage system availability and performance?
- How quickly does the provider respond to attacks, and what recovery methods are used?
- Are the limits of responsibility for security by the provider clearly defined?

Cloud Security Planning Guide

For more detailed information about choosing the right cloud services provider, and for additional information on planning security in the cloud, see Intel's [Cloud Security Planning Guide](#).

In 2009, Intel IT began moving the Intel enterprise to a private cloud and exploring the use of external cloud services for certain applications. The *Cloud Security Planning Guide* is the result of our experiences during our ongoing cloud journey, as well as working with cloud providers, virtualization and security solution vendors, OEMs, and large enterprise customers.

Vendor Responses to IT Questions

1. Briefly describe the security components of your cloud offering, including end-user benefits.
2. What is your solution architecture, and how is security integrated into your cloud offering?
3. How does your security offering help in either establishing or enforcing trust in the cloud?
4. What unique and differentiated capabilities do you offer that help protect data and infrastructure in the cloud?
5. How does your solution work with other providers' solutions to help build a chain of trust from the application user's interfaces to the underlying hardware?
6. How does your security offering simplify auditing and regulatory compliance?
7. How does your solution take the anxiety out of moving to the cloud?
8. Why should I select your solution over the others?
9. Do you have a method for demonstrating ROI for your cloud offering?
10. Are there security concerns that your solution doesn't address that you think the industry still needs to solve?
11. I'm just beginning to investigate cloud security. What advice can you give me, and what steps should I take to make sure I'm covering all my bases?
12. What tools do you offer to establish, maintain, and protect identity in the cloud?
13. What services do you have for federating identity between clouds (public and private)?

Q1:

Briefly describe the security components of your cloud offering, including end-user benefits.



Carpathia* InstantOn* has two discrete cloud platforms, federal and commercial. Each has a different set of security components and compliance controls. In both solutions, we adopted a defense-in-depth approach. Starting from the edge, this includes:

- Ingress and egress firewalls, an intrusion protection system (IPS), and distributed-denial-of-service (DDoS) protection
- Hardened hypervisor builds and integrity checking
- Multifactor authentication for privileged operations
- Private networking for traffic isolation
- Detailed system and application monitoring delivered near real time to a correlation engine
- 24-7 monitoring of the entire platform
- Proactive security scanning and continuous risk assessment in support of Federal Risk and Authorization Management Program (FedRAMP) standards
- Benchmarking of platform against cloud audit standards

Along with these controls, Carpathia offers a high degree of transparency to end users, including the ability to view audited controls and reports from Statement on Auditing Standards No. 70 (SAS 70) Type II, and in the federal cloud, the ability to view related security content.



Cisco offers a [cloud security solution](#) to help secure private, public, or hybrid clouds. The Cisco product portfolio includes the following components that enable cloud security for logical separation, policy consistency, automation, and access control in the cloud infrastructure; enable multitenancy; and provide network traffic and activity visibility for cloud governance processes:

- Cisco* ASA 5585-X Appliance and Cisco Catalyst* 6500 Series ASA Services Module
- Cisco Nexus* 1000V Series Switches
- Cisco Virtual Security Gateway (VSG)
- Cisco IPS 4200 Series Sensors

The Cisco ASA 5585-X Appliance protects the virtualized data center and extended cloud with firewall and IPS capabilities at the cloud data center distribution layer, providing protection for high-value cloud resources and services.

Continued on next page.

Q1) Continued

The Cisco Catalyst 6500 Series ASA Services Module is deployed as a plug-in module for Cisco Catalyst 6500 Series Switches. Cisco also provides another IPS deployment option with IPS sensors to enable distributed and intelligent detection with precision response to network attacks.

The Cisco VSG works with Cisco Nexus 1000V Series Switches to provide zone-based and policy-driven security at the virtual machine (VM) level, extending existing security policies into virtual and cloud environments. Cisco VSG provides secure segmentation to achieve logical separation at the VM level. Because VSG uses security-zone-based policy implementation rather than static IP addresses, it can consistently enforce security policies even as VMs move from one physical host to another. This support of VM mobility is critical to ensuring policy consistency in an automated cloud environment where workloads can be processed anywhere in the cloud.



The security components include NetScaler* Cloud Gateway, which provides single sign-on (SSO) and secure provisioning for the cloud, and the NetScaler Web Application Firewall for securing clouds from attacks.



Expedient implements advanced security mechanisms throughout its cloud platform to ensure the confidentiality, integrity, and availability of data. These security components are implemented at each layer of the technology stack and include, but are not limited to, two-factor authentication, network and host-based intrusion detection, platform attestation using Intel® Trusted Execution Technology (Intel TXT) and a Trusted Platform Module (TPM), and complete physical segregation where necessary.

All components are managed and monitored around-the-clock by multiple geographically diverse operations centers.



HyTrust* Appliance is a VMware* vSphere*-compatible virtual appliance that supports secure multitenant environments without resorting to "air gaps" to segregate each tenant. This enables you to get the maximum return on investment (ROI) in your virtualized environment. Air gaps create a significant amount of wasted resources in the form of a completely new, completely redundant silo of software and hardware.

HyTrust Appliance delivers these key capabilities to support private cloud environments:

- Authenticates and verifies administrator identity to tie all access to the environment to a specific individual
 - Verifies platform integrity at the hypervisor level and at the hardware level
 - Validates all change requests to the infrastructure for complex, higher-level use cases, such as compliance and private cloud, so that organizations can maximize their ROI in virtualization while supporting these initiatives
 - Provides the system of record that makes it easy to manage compliance audits and forensic investigations
-

Q1) Continued



McAfee provides enterprises with our McAfee* Cloud Security Platform, which helps customers secure their data as it leaves the organization and moves into the public cloud. McAfee Cloud Security Platform builds a secure bridge from the enterprise to the public cloud. It protects the three primary channels of traffic leaving the organization where data loss and threat intrusion can occur: Web traffic, authentication traffic, and e-mail traffic. The security components include data loss prevention, web security, e-mail security, web services security, and identity access management.



The [OpSource* Cloud Hosting](#) service offers a unique approach to security by enabling organizations to customize a cloud networking environment to look and feel like a network they would set up on their own premises. OpSource [Cloud Servers](#) are deployed on dedicated OpSource Cloud Networks (virtual LANs [VLANs]), and each [Cloud Network](#) can be customized by configuring firewall access control lists (ACLs), load balancing, network address translation (NAT), and multicast to support secure n-tier architectures in the cloud.

Security components include (but are not limited to):

Customer-Controlled Network Configuration

- Configurable Layer 2 VLANs based on Cisco-based switching fabric
 - Segmentation of public and private IP space (servers are assigned only private IPs when deployed)
 - NAT and virtual IP (VIP) functions that expose only those private IP addresses customers want exposed to the public Internet
- Customizable ACL-based firewall rules to enable access control into each network VLAN
 - Ability to build multitier network architectures to separate data tiers from front-end web tiers, thus providing an additional layer of firewall rules to protect data

Role-Based Administrative Control

- Unique user name and password for multiple administrators
- Role-based permissions to enable administrator to limit sub-administrators to managing only certain resources

Additional

- Edge-to-edge security visibility
 - Intrusion detection system (IDS)
-

Q1) Continued



Trapezoid Information Security Services offers SecRAMP, security services focused on protecting systems and data being deployed or on-ramped into a private or public cloud environment.

In public clouds, SecRAMP provides host-based services and virtual security appliances within the limitations of the infrastructure provider, including intrusion protection, data leakage prevention, file integrity monitoring, and application performance monitoring.

In private clouds, SecRAMP provides security design, implementation, and monitoring services for network, system, and hypervisor security.



Virtustream provides every customer with dedicated resources assigned to them that offer performance guarantees and varying levels of resource and network isolation, depending on the customer's security and data protection policies. Technologies such as VLANs, virtual routing and forwarding (VRF), and storage logical unit numbers (LUNs) are all utilized to this effect, keeping customer resources separated from all other customers.

In addition, a combination of network firewalls and hypervisor-based firewalls are utilized to isolate traffic flows within different security zones, and even within a given network, according to any security policy of the customer's choosing. Our hypervisor-based firewall product has the capability to perform intrusion detection on all network flows entering or leaving each VM, to find malicious attempts at compromising a customer's applications.

Our roadmap includes integration of key Intel technologies, such as Intel TXT, Intel Advanced Encryption Standard New Instructions (Intel AES-NI), and Intel cloud-aware technologies, to provide chip-level security as well as the network, physical, and logical security already offered.

Q2:

What is your solution architecture, and how is security integrated into your cloud offering?



Our architecture is hardware and hypervisor agnostic. This allows for the right hardware (for example, commodity or enterprise) and the right hypervisor (Citrix* XenServer* or VMware vSphere) to be applied to workloads. The hypervisor is managed by a policy-based orchestration system, which supports many advanced security policies that permit isolation (limit customer to servers 1 to 10) and sandboxing (promote to published only after a positive security scan and very detailed accounting records). We also enable customers to inspect traffic between VMs by using our private networking technology (VLAN based) to create n-tier architectures and deploying IPS instances and firewalls between VMs in the architecture.



Cisco SecureX Architecture* is a context-aware security framework that meets customer needs as they embrace a mobile, dynamic, and cloud-based working environment. The framework is a solid foundation composed of technologies that ensure a trusted network infrastructure. Cisco SecureX Architecture is led by context-aware policy that enables customers to easily define and manage business-relevant security policies. It provides further security enforcement elements in the form of appliances, modules, and cloud services.

Cisco cloud security consists of three key solution components that are direct implementations of Cisco SecureX Architecture:

- Secure Cloud Infrastructure
- Cloud Security Services
- Secure Cloud Access

Within the SecureX cloud framework, security solutions can be delivered as stand-alone, scalable, multipurpose appliances; network-embedded modules that leverage existing infrastructure; or virtual service nodes that deliver security features in a virtual form factor. This gives customers the flexibility to implement cost-efficient security at the right point of the network.



Citrix solutions support the building of cloud architectures by providing the foundational aspects, including secure networking, hypervisors, and a secured and supported OpenStack* cloud platform.

Q2) Continued



The solution architecture deployed at Expedient consists of smaller self-contained pods containing compute, storage, and I/O. This building-block design reduces the potential exposure of a significant site-wide outage by providing POD-level isolation.

All aspects of the platform, including compute, storage, network, and power, are redundant. In all instances and across all components, an N+2 or N+N redundancy model is implemented to ensure ultrahigh availability.

Security components are integrated at every layer of the Open Systems Interconnection (OSI) model, from the physical through the application layer. Gates and monitors, such as Layer 2 VLAN segregation, Layer 3/4 firewalls, Layer 7 application firewalls, and host-based IDSs, are deployed using standards-based technology, ensuring reduced complexity and enhanced security. Environment security is furthered by overlaying more advanced mechanisms, such as platform attestation using Intel TXT technology, to ensure good known running platforms.

Each component provides enhanced reporting capability to ensure proper monitoring and tracking of potential issues and threats.



Despite its name, the HyTrust Appliance is not a physical piece of hardware. It's a VMware vSphere-compatible virtual appliance that's deployed right alongside the rest of your virtual infrastructure. It can be deployed on the same hypervisor that it is actively protecting.

HyTrust Appliance sits in the management plane of the virtual infrastructure. In other words, it sits between the administrators of the virtual infrastructure—the virtualization administrators, the network administrators, and the application owners—and the virtual infrastructure itself. From this centralized vantage point, HyTrust Appliance intercepts all administrative requests for the virtual infrastructure, determines whether the request is in accordance with the organization's defined policy, then permits or denies the request as appropriate.



The McAfee Cloud Security Platform is modular, providing customers with the flexibility to start with the solution that most appropriately fits their needs, whether it is data-loss prevention, web security, or so forth. Our solutions can be deployed as software as a service (SaaS), on an appliance, as virtual software, or in combination.

Our solutions are integrated into McAfee's ePolicy Orchestrator* (ePO), advanced and scalable security management software. McAfee's end-point and network solutions are also managed by ePO, and its open platform allows customers to connect management of McAfee and third-party security solutions to their Lightweight Directory Access Protocol (LDAP), IT operations, and configuration management tools.

Finally, all McAfee solutions leverage our Global Threat Intelligence to provide superior protection against impending security threats. Our visibility across key threat vectors—file, Web, e-mail, and network—and a view into the latest vulnerabilities across the IT industry enable McAfee to correlate real-world data collected from millions of sensors around the globe and deliver real-time protection via our suite of McAfee security products.

Q2) Continued



The OpSource Cloud architecture enables configuration and lockdown of the compute and storage environments. With [OpSource Cloud Networks](#), customer-controlled networks with configuration services, customers are able to configure VLANs between servers, configure ACL-based firewalls, and control and track administrative usage. Data is encrypted while being transferred and at rest.

[OpSource Cloud Servers](#) and [OpSource Cloud Files](#), cloud-based compute and storage services, can be linked by OpSource Cloud Networks. Rather than implementing network security on top of the OpSource virtualized servers, OpSource Cloud Networks is a truly network-based implementation running within Cisco switching fabric. Customers manage and configure OpSource Cloud Networks via the web-based OpSourceCloud.net user interface or [Open API for the OpSource Cloud](#).

OpSource utilizes Cisco ASA, Cisco ACE technologies, and carrier-class switching infrastructure to provide a "defense-in-depth" enterprise security architecture to provide multiple layers of security, including IDS, VPN, encryption (in flight and at rest), firewall, and NAT to protect information assets. Additionally, customers can implement host-based security as an added layer of security.



The solution architecture depends on the type of customer. For end customers with private clouds, SecRAMP implements and manages security tools that deliver visibility and automation from the hypervisor layer up through web applications.

For service providers, SecRAMP architects solutions that allow them to offer multitenant security services that they can deliver to their customers.

SecRAMP takes a three-phased approach:

Assess and evaluate the customer's current security environment. The security architecture designed and managed by SecRAMP will depend on the customer's security strategy and current cloud implementation plans.

Architect and enhance the security stack. SecRAMP bridges the gaps in coverage, such as hardware trust, policy, and incident response capabilities. SecRAMP enables customers to effectively address security architecture regardless of the cloud strategy. The end result is a more secure environment and an integrated view that leverages the unique capabilities of each of the security tools that are implemented to monitor and secure the environment.

Operationalize and manage on an ongoing basis. After implementation, our expert staff continuously tunes, manages, and monitors the security.

Q2) Continued



The Virtustream* xStream* Cloud Solution was custom-built from the ground up with security as a primary consideration. Most notably, our solution architecture is comprised of air-gapped internal and demilitarized zone (DMZ) environments with multiple layers of security checkpoints.

Virtustream implements an air gap of all compute and storage resources between the enterprise and DMZ platforms. This enforces inbound access from the Internet only on the DMZ platform, keeping the enterprise platform free of external DDoS-type attacks from the public Internet.

The first security layer consists of network firewall appliances, providing a layer of protection between security zones (for example, where enterprise applications reside) in a customer's cloud infrastructure.

The second security layer consists of hypervisor-based firewalls that perform additional packet filtering and intrusion detection. This is where intrazone communication can be monitored and controlled.

The last layer of security is hardening of the operating system and enterprise applications. Virtustream uses best practices to harden applications at the source. Also, our platform offering performs antivirus, anti-rootkit, and compliance checks from the hypervisor.

We are currently evaluating the capabilities of Intel TXT, which promises to increase the security of xStream by enabling hardware-driven software integrity and data authenticity assurance.

Q3:

How does your security offering help in either establishing or enforcing trust in the cloud?



Carpathia offers a range of information assurance and compliance services that enable the base controls in the cloud to be extended to meet compliance requirements. The key to trust is transparency, both in terms of the design of the platform and its operation. The combination of our core cloud security, managed services, and full transparency helps support a trust-based model in our cloud.



Cisco TrustSec* architecture helps to secure customer networks by building and enforcing identity-based access policies for users and devices while protecting critical data throughout the network. In this way, Cisco TrustSec architecture helps establish trust in the cloud by:

- Identifying users and providing differentiated access in a dynamic, borderless environment
- Enforcing compliance for an expanding array of consumer and network-capable devices
- Enforcing access policy for users and devices located anywhere in the cloud
- Establishing, monitoring, and enforcing consistent global access policies



Citrix XenServer, along with a fully OpenStack* cloud platform (Project Olympus), provides a multitenant trust framework for building trusted clouds. NetScaler* Cloud Gateway extends trust services from the cloud user through to hosted and third-party SaaS offerings for authentication, authorization, and provisioning management. NetScaler Cloud Bridge connects data center and public clouds utilizing an encrypted trust fabric. And NetScaler Application Firewall enforces the trust between cloud users and cloud services.



The most important element of Expedient's security offering that establishes trust in the cloud is Expedient's openness to audit and accountability. Expedient believes that simply providing a SAS 70 or like document is not enough to satisfy auditing needs; the cloud provider must be open and able to satisfy audit requirements as if it were an extension of an organization's IT group.

In short, Expedient allows for customers to audit their environments and makes its personnel, policies, and practices available for audit, which helps build trust in the cloud.



HyTrust can ensure that certain virtual workloads are only permitted to boot up on specific hosts or specific clusters, which is critical for compliance with the Payment Card Industry Data Security Standards (PCI-DSS). Through our partnership with Intel, HyTrust can verify the integrity of the physical hardware of the host to ensure that the underlying platform is fully trusted. HyTrust Appliance offers flexibility and control through its unique ability to label virtual objects and then apply policies to those labels.

Q3) Continued



The McAfee Cloud Security Platform enables customers to understand what information should be moving into cloud environments and to regulate the movement of that data. It also secures the channels of traffic that are being used to communicate with the cloud, ensuring that these channels are not open to potential threats or intrusions, particularly new channels such as the communications of private cloud applications to public cloud applications.



OpSource provides enterprise-class security in our cloud. By enabling our clients to easily configure VLANs, firewalls, and VPNs, we are able to provide the security and control of a trusted network within the enterprise boundary but within a cloud environment.

Additionally, the OpSource Cloud holds these certifications: SAS 70 Type II, European Safe Harbor, and Health Insurance Portability and Accountability Act (HIPAA) Business Associate. Our Managed Hosting environment is PCI-DSS Level 2 certified.



Our platform provides visibility into public and private cloud platforms, enabling full monitoring and auditing capabilities of the entire infrastructure. Designing a trusted cloud platform in a private cloud starts at the hardware level, ensuring that the system is authenticated at the chip level up through the hypervisor, operating systems, networks, applications, and databases.



Virtustream xStream Platform is designed, from the ground up, to establish customer trust in our xStream enterprise cloud offering.

Our service starts with the Virtustream Advisor process, which includes professional, enterprise-caliber advice from application, network, and security experts to ensure that the transition to the cloud follows a proper security model. Based on customer need, we can also benchmark the maturity level of their IT environment and define an action plan to improve, if necessary.

Our on-boarding methodology integrates the security architecture recommendations into the cloud deployment. Examples include isolation of public-facing services into their own security zone, allowing only necessary connectivity between security zones or a security zone, and hardening the applications.

We also provide assurance with our industry certifications, including Federal Information Security Management Act (FISMA) and Statement on Standards for Attestation Engagements No. 16 (SSAE 16). We are also pursuing HIPAA compliance and other relevant certifications.

Continued on next page.

Q3) Continued

At a product and platform level, we constantly evaluate new network, hardware, processor, chipset, and platform security capabilities and provide our customers and prospects with education about the evolving industry best practices and their benefits.

Using this process, Virtustream can address security concerns around our cloud infrastructure by conveying our many years of expertise and adherence to industry-accepted security models and practices.

Q4:

What unique and differentiated capabilities do you offer that help protect data and infrastructure in the cloud?



Probably the key area for our cloud to differentiate versus traditional public clouds is our network capabilities. Carpathia supports full private networking in the cloud. This enables customers to create n-tier applications versus simple flat network topologies. In support of our network capabilities are a number of specialized VMs, such as those from Vyatta, that also provide firewall, VPN, and IPS services.

Carpathia's cloud also supports hybrid deployments where certain applications and workloads run in the cloud and a private network can be extended into the cloud over a secure Layer 2 network. This also allows customers to keep some workloads in the cloud while others run in a different control domain.



Securing virtual applications and the virtualization layer of the data center is the most challenging obstacle to achieving the benefits of data center consolidation and virtualization and moving to a cloud cost model. The Cisco VSG firewall enforces detailed security policies that are VM aware and helps ensure isolation of traffic and applications in a way that traditional security devices cannot, without limiting scalability of the overall data center or complicating the delivery of virtual applications in the cloud.



NetScaler Cloud Gateway is an innovative solution for connecting users to cloud services in a secured fashion, whether those resources are onsite, hosted, or outsourced. Full life-cycle provisioning management and automated credential management ensure that only authorized users can access cloud services. And passwords are constantly changed in an automated way that improves user productivity and security.



In addition to adhering to security best practices and regular internal audits, Expedient's openness to participating in our clients' external audits is a key differentiator from other cloud providers. This, along with Expedient's continued research, development, and deployment of new security technologies such as platform attestation, provides a rich security complement to any IT organization.



Authenticate and verify administrator identity: With HyTrust Appliance in place, there are no anonymous changes to the virtual infrastructure. All administrative access must first be authenticated. HyTrust fully supports two-factor authentication with RSA* SecurID* or smart cards. In the event that root access is required, HyTrust Appliance features root password vaulting, which enables certain administrators to check out a temporary password for one-time access.

Continued on next page.

Q4) Continued

Verify platform integrity: The integrity of the entire infrastructure stack rests on the premise that the hypervisor is trusted and fully hardened. HyTrust Appliance provides verification of the hypervisor by assessing the hypervisor configuration against industry-standard configuration templates. Unique to HyTrust is the additional ability to verify the trust of the hardware layer via Intel TXT.

Validate all change requests: From its unique vantage point, HyTrust Appliance inspects every virtual infrastructure change request, approving or denying it in accordance with your defined policies. These policies are fully customizable and flexible enough to handle any complex situation.

Serve as the system of record: As the central authority over all change requests, HyTrust Appliance provides granular, user-specific log records that can be used for regulatory compliance, troubleshooting, and forensic analysis. It offers a deep visibility into the state of and changes to cloud infrastructure.



With the McAfee Cloud Security Platform, customers can identify, classify, and protect critical data while it moves between their enterprise and the cloud—all e-mail, Web, and authentication traffic. McAfee Cloud Security Platform has a modular, open platform that customers can build upon to extend their enterprise security policies into the cloud.

McAfee Cloud Security Platform leverages our Global Threat Intelligence, which collects threat intelligence from more than 100 million nodes and across file, e-mail, and Web and network threat vectors. It then leverages McAfee Labs' more than 350 researchers to correlate that data, identify new threats, and deliver protection back into the Cloud Security Platform in real time.



Hardware-based Layer 2 VLANs built on Cisco switching fabric: This allows for customer-controlled network configuration (see details in question 1).

- Segmentation of public and private IP space (servers are assigned only private IPs when deployed)
- NAT and VIP functions that expose only those private IP addresses you want exposed to the public Internet
- Customizable ACL firewall rules that allow:
 - Load balancing and port translation across multiple virtual servers, with the ability to take servers in and out of service manually, programmatically, or based on monitoring probes
 - Layer 2 multicast support for clustering implementations

Sophisticated role-based administrative controls: With unique user names and passwords for multiple administrators and role-based permissions that enable administrators to limit sub-administrators to managing only certain resources, such as servers, storage, or networks

Continued on next page.

Q4) Continued

Detailed reporting: For complete insight into who is doing what and when in your cloud environment—audit logs of all environmental changes

Data encryption: Stored with 256-bit encryption at rest and 128-bit Secure Sockets Layer encryption while in transit



SecRAMP unifies the management and monitoring of multi-cloud environments with the same best-of-breed security technologies that are commonly deployed in any customer-operated data center or managed hosting environment. SecRAMP represents the customer as they work with their cloud provider to properly validate and help implement security measures that the cloud provider may not provide but are necessary for the protection of the customer's key data. Our team has expertise implementing and managing the leading security tools and commercial products in extremely large and complex multitenant cloud environments.



Virtustream enables full security monitoring, protection, and auditing at the most granular level by providing the ability to perform firewall, intrusion detection, antivirus, anti-rootkit, and compliance checking from the hypervisor. This comprehensive approach ensures the security of each virtual machine. Gathering this data into a security correlation engine is most efficiently done using a single point of presence at the hypervisor.

With the Virtustream security correlation engine, we are able to take the traffic and event logs from all of the security checkpoints outlined above and generate concise, actionable alerts out of the mountains of log data available. This ensures that customers are alerted to any actionable security event that arises.

To accomplish the same level of security monitoring, protection, and auditing, many solutions require the installation of software agents or the implementation of a network-wide appliance. Managing software agents requires yet another layer of management overhead and usually requires multiple tools to accomplish the same feature set described above. Network-wide appliances do not typically see intranetwork communications between servers and cannot look as closely into a system to discover threats such as rootkits.

Q5:

How does your solution work with other providers' solutions to help build a chain of trust from the application user's interfaces to the underlying hardware?



We work closely with our hardware and software partners to show a chain of trust from procurement to production. We integrate and take full advantage of capabilities provided by the underlying hardware and software infrastructure and work closely with our partners around roadmap items.



Organizations looking to migrate sensitive data and applications to the cloud need to trust that the cloud security infrastructure can address the complexities brought about by virtualization, massive scale, and application mobility.

Cisco addresses these problems by securing the virtualization layer of the network with unique security solutions built into the virtual switch and the hypervisor layer. These virtual security nodes allow for the creation of security policies that are aligned with attributes of the VM, not the network topology, so that the policies are enforced independently of the application location, even when coresident on a server with an untrusted application. Read a [Cisco case study about providing trust for cloud-based virtual desktop applications](#) all the way from a thin client, to the virtual desktop in the data center, through to the back-office application in the cloud.



Security partners provide solutions and security extensions through the Citrix Ready* program to ensure tested and trusted integration.



Today the use of Intel TXT and TPM allows for the chain of trust from the hypervisor to the hardware. Expedient feels that solutions that provide that same level of security to the application user interfaces for infrastructure as a service (IaaS) are not yet production ready. However, Expedient continues to monitor technology, and once that technology is stable and available, it will be incorporated into the overall platform.



The integrity of the entire infrastructure stack rests on the premise that the hypervisor is trusted and fully hardened. HyTrust Appliance provides this verification with the ability to assess the hypervisor configuration against industry-standard configuration templates, such as PCI-DSS, the Center for Internet Security (CIS), and VMware Best Practices. Unique to HyTrust is the additional ability to verify the trust of the hardware layer via Intel TXT.



The modular design and open APIs of the McAfee Cloud Security Platform enable McAfee and partners to build additional security services and solutions to integrate into the platform, including solutions that allow companies to extend more policies and greater control into the cloud.

Q5) Continued



The OpSource RESTful API enables our cloud to integrate easily with third-party authentication, monitoring, configuration management, and security management tools.

Additionally, clients can configure VLANs and firewall ACLs to explicitly limit access to specific servers by IP address, port, or protocol. For example, clients can set up web servers in a DMZ accessible via the public Internet on port 80. Application servers, sitting on a separate VLAN, could be accessed only by the web-tier or database-tier servers. The database servers could only be accessed by the application tier. This approach to security provides for application access and server access control.

Lastly, OpSource controls permissions of multiple end users of a specific client account and logs activities critical to administering a trusted cloud environment.



SecRAMP has developed several use cases around integration with Intel TXT servers and VMware. Intel TXT integration enables customers to benefit from a root of trust that can be extended from the hardware through the hypervisor and up to the application interface. Data is then provided to a security information and event management system to validate, audit, and report on trust status.

Implementing strong policies and procedures can also aid in improving the overall level of trust. For example, with server deployments, we typically identify every piece of firmware on the system, such as the BIOS, the RAID, and the video card—anything that can be updated at the hardware level prior to the operating system installation. We then build an internal repository of relevant firmware, validate it with vendor-provided hashes, and flash the firmware predeployment. While this is not a 100 percent solution, it does reduce the risk of compromise at the hardware level. On blade systems like the Cisco Unified Computing System platform, features such as Service Profiles make this type of operation much quicker and easier, especially for private cloud deployments.



Because Virtustream dedicates the network, compute, and storage resources for every customer, each application can trust that the infrastructure presented to it is not shared or seen by any other customer. This ensures routing and data segregation through secure swim lanes, even when a customer introduces integration points with other service providers.

In order to avoid vendor lock-in, many organizations subscribe to the services of two or more cloud service providers—increasing the importance of secure data management and movement of data between physical locations. Secure data management will be enabled by technologies such as Intel TXT, which provides launch verification and attestation, both of which are tremendously important in cloud implementation scenarios, where machines may reside in different geographic regions.

Continued on next page.

Q5) Continued

Virtustream's xStream Platform is already designed for on-premises, cloud, and hybrid environments, enabling closely held federated cloud environments and dynamic movement of data across those trusted networks. Our near-term objective is to open cloud environments to become more flexibly and dynamically responsive to a customer's changing environments, including cross-location enterprise clouds accessible by any device. Intel's client-aware technologies will be increasingly important as we expand our platform and open it to the emerging diaspora of computing devices.

Q6:

How does your security offering simplify auditing and regulatory compliance?



Carpathia believes that as a service provider, we should be part of the equation when it comes to supporting customer compliance requirements rather than simply a platform. We have developed our operating procedures to exceed all common regulatory compliance requirements for moderate-impact-level systems. This allows us to extend a compliance umbrella around the platform in support of customer business goals. We also routinely enter into business agreements to further solidify delivery partnerships, such as Business Associate agreements for our customers with HIPAA mandates.



The Cisco SecureX security framework is context aware, and SecureX-enabled products can apply different policies and separate data streams from different clients or business processes. This makes it easier to verify that the client or process has the correct security applied, rather than attempting to make a one-size-fits-all policy that tries to meet the needs of all. Context-aware security policies simplify auditing and regulatory compliance and allow for fine-grained control of security. When policies are centralized and virtualization aware, auditing and compliance become easy to verify and maintain, so that security reviews can be done from a client or business process standpoint.

From a product perspective, the Cisco Virtual Security Gateway logs all allow and deny traffic activities for auditing purposes. Cisco ScanSafe Web Filtering includes an advanced web reporting system, detailing usage and threats blocked. Cisco ISR Web Security with Cisco ScanSafe is a new hybrid cloud security service that enables centralized enforcement and reporting for branch offices.



Foundational aspects of compliance, such as strong authentication, mutual certificate authentication, encryption, and advanced logging are inherent to the platform. The Citrix Ready program provides for deep integration with compliance partners.



Expedient's security offering has been honed to stand up to the most rigorous of audits after participating in hundreds of client-specific audits. With its open auditing nature, Expedient continues to refine its cloud platform to ensure that the environment meets the most stringent audit and regulatory compliance needs.

Q6) Continued



As the central authority over all change requests, HyTrust Appliance provides granular, user-specific log records that can be used for regulatory compliance, troubleshooting, and forensic analysis. It offers deep visibility into the state of the virtual infrastructure. Unlike VMware vCenter* Server, HyTrust Appliance not only records valid requests but invalid attempts as well—which is critical for security purposes. Additionally, every request is tied to the identity of a specific user, and all relevant information—actual request, source IP, target IP, and so forth—is collected. With total visibility from HyTrust, organizations can handle audits easily and rely on their logs for forensics if there is ever a need for investigation.



The McAfee Cloud Security Platform enforces data protection policies for information leaving the network through e-mail, web mail, instant messaging, wikis, blogs, portals, and Web 2.0 technologies. Customers can take a variety of remediation actions—including encrypting, redirecting, quarantining, and even blocking—to ensure compliance with regulations governing the privacy of sensitive information and reduce the data risk to the business. The McAfee Cloud Security Platform also provides comprehensive incident reporting and monitoring to gather all needed data, such as sender, recipient, time stamp, and network evidence, for proper analysis, investigation and audit, remediation, and risk assessment.



OpSource tracks each activity or change to the cloud environment. Every change made to the system (adding a user, deleting a user, adding a server, changing the CPU on a server, deleting a server, and so forth) is tracked and logged. Usage is also logged. Logging and the ability to create reports are critical to providing the audit trail necessary to meet strict audit and compliance requirements.

OpSource is also SAS 70 Type II certified, enabling our customers to simplify and accelerate their own certification processes.



One of our core strengths is consolidating security data and audit logs in a single location for a unified reporting view of the entire organization's security posture. SecRAMP's team provides security audit support as part of our managed service, which makes it easy to tune, automate, consolidate, and report on security events and audit logs. These services are provided to cloud security customers to help simplify the tasks involved in proving regulatory compliance to the various certifying bodies. Our architecture allows us to easily provide supporting data for audits such as Payment Card Industry (PCI), Sarbanes-Oxley (SOX), and FISMA.



Our hypervisor security monitoring tools include compliance auditing of all of a customer's systems. Compliance audit rule sets can either be custom defined, or we can use prebuilt compliance assessments based on common industry best practices and leading regulatory standards. The tools provide reporting capabilities that facilitate third-party auditing requirements for SSAE 16, FISMA, Federal Financial Institutions Examination Council (FFIEC), PCI-DSS, National Institute of Standards and Technology (NIST), and so forth.

Q7:

How does your solution take the anxiety out of moving to the cloud?



Our approach to cloud, as with other services we offer, is very solution oriented. While it's not possible to completely remove anxiety from cloud deployments, it is possible to engineer a solution that follows a risk-based approach. This, plus transparency, helps build confidence in the solution. This contrasts with many IaaS solutions where the relationship is somewhat at arm's length and mediated by the credit card used to purchase services.



The first step in relieving anxiety in regard to the cloud is to fully understand the security issues unique to the cloud environment and to create a comprehensive and detailed plan to address those issues. Cisco and its partners have long-time experience in security and work closely with customers to identify security issues unique to the customer's business and implement the SecureX architecture. Furthermore, Cisco has significant investment in security and security-related R&D and an extremely broad customer base from which to gather ongoing security issues. Customers who engage Cisco gain from our wisdom and experience in the security market and have a clear understanding of the security risks involved in a move to the cloud, as well as how to mitigate them.



NetScaler Cloud Bridge connects data centers to the cloud so that cloud bursting and other cloud services can be securely configured and managed. NetScaler Cloud Gateway ensures that users have the most simplified and secured connectivity, while giving IT control over access to SaaS applications that they otherwise may not have known were in use. Visibility and control reduce anxiety in moving to the cloud.



Anxiety is reduced with an Expedient* platform that offers the ability to independently audit and review data and control processes. In many cloud topologies, the underlying platform, security technologies, and even data locations may be obscured, making that platform a "black box" of sorts. The Expedient solution, however, is transparent and can be regularly reviewed and tested. This, along with the inherent security controls throughout the platform, allows customers to have a high degree of confidence that their data will be protected with similar if not better controls than currently exist in their organization. Expedient also can implement a proof of concept of a specific client environment so that the effectiveness of the solution can be tested, and performance can be verified. During the design of a client's environment and throughout their use of Expedient's services, they have direct access to the engineering staff to provide guidance and live support.



With HyTrust Appliance, organizations can build truly private clouds on VMware-based virtual infrastructure. Through a unique method of labeling virtual objects and placing controls over changes in the environment, HyTrust Appliance enables multiple entities to have complete control over their own slice of the infrastructure without compromising the integrity of their neighbor's environment.

Q7) Continued



The McAfee Cloud Security Platform can help customers understand where data resides in their organization, and its level of importance or sensitivity. That is the first step in ensuring that the right data moves to the cloud, and it helps to minimize the anxiety of losing key data to traffic through various channels. Also, McAfee's Cloud Identity Manager enables customers to control access to cloud applications, which is integral to reducing the anxiety around potential data loss.



OpSource believes that giving IT professionals more granular control over their cloud environment takes a lot of the anxiety out of moving to the cloud. The OpSource Cloud allows IT professionals more control than many public clouds and enables them to:

- Expose only those private IP addresses they want exposed to the public Internet
- Customize ACL firewall rules
- Grant access to certain areas of the cloud only to certain people
- Monitor usage with detailed reporting
- Add or remove CPU, RAM, and storage from servers, on the fly
- Gain access through easy-to-use user interfaces (UIs) or RESTful APIs

In addition, security is a key component of our offering. OpSource is built on enterprise-grade infrastructure, and we have taken a layered or "defense-in-depth" approach to security to build an enterprise-class secure public cloud. Where typical public cloud offerings have a perimeter-based security solution, OpSource bakes security into the OpSource Cloud platform at every step.



There can be anxiety moving to any new platform, especially when on-ramping into a new platform that is not completely owned or managed by the customer.

Education and planning can significantly reduce anxiety and should include due diligence in all aspects of the migration. SecRAMP helps customers identify key security strategies and creates detailed project plans to help implement all possible security measures required for a successful and secure cloud on-ramping experience. After the ramp-up, SecRAMP provides monitoring and tuning to protect the customer's data moving forward while it resides on a service provider platform.

Q7) Continued



The Virtustream Advisor process is a structured, multidimensional analysis and reporting solution with an integrated suite of software tools and professional services to prepare companies for cloud computing deployments. It includes a full review of compute/storage performance needs, application design, and security review. Taking the time to undergo this consultative process up front helps assure customers that moving to our enterprise cloud will result in the required performance with the same (or better) security and integrity as the customer's systems. Many other solutions do not involve this comprehensive approach to making sure all concerns are addressed.

Following the Advisor exercise, Virtustream adheres to a structured on-boarding methodology to execute a migration plan tailored to each client's unique needs and virtualization state (for example, whether they are virtualized or physical, on premises or in a third-party facility).

Q8:

Why should I select your solution over the others?



Customers should look at their business goals, compliance requirements, and support requirements before any deployment. Carpathia specializes in two areas with our platform: complex solutions (customers typically deploying many VMs using advanced networking techniques) and compliant solutions (customers mandated to comply with standards such as FISMA, Department of Defense Information Assurance Certification and Accreditation Process [DIACAP], FedRAMP, PCI, and HIPAA). Our platform is optimized for these solutions.



Cisco's years of experience, deep product lines, and thought leadership in the security market give it a competitive edge over competitors. Virtually no other competitor in the market can claim the wide experience with customer environments in the cloud or standard IT environments. Cisco also offers one of the best support centers in the industry, with 24-7 access, fast escalation, and knowledgeable support staff that are the standard of the industry.

Cisco has a history of very good investment protection for customers and clear product transitions. Cisco's engineers see data and data traffic from nearly every source: data centers, cloud environments, campus environments, video, collaboration, WAN, storage area network (SAN), service providers (SPs), and Voice Over Internet Protocol (VoIP). Because we produce products in each of these markets, we know the security concerns and can offer significant insight in addressing them. An end-to-end security solution from Cisco offers a single point of support and a proven track record of initial and long-term success in customer deployments.



Citrix provides comprehensive solutions for the cloud from end point to server to orchestration for small to large organizations. In addition, Citrix has deep cloud experience with our industry-leading SaaS offerings, which include GoToMeeting*, GoToWebinar*, GoToAssist*, GoToTraining*, and GoToManage*.



You shouldn't select Expedient's solution or any other before reviewing your business needs and criteria. Each cloud provider has different capabilities, functionality, and cost. Depending on your business need, a particular cloud provider or the cloud in general may or may not be the appropriate fit. However, Expedient feels that the capability, functionality, security, and auditability it provides, combined with the cost-effectiveness of its solution, make it a compelling option for many production environments.



HyTrust is the only solution on the market that authenticates and verifies administrator identity, verifies integrity of the cloud infrastructure, validates all change requests, and provides a complete system of record for the state of and changes to the cloud infrastructure.

Q8) Continued



The McAfee Cloud Security Platform allows enterprises to operate with more efficiency and flexibility by consolidating data-loss prevention and e-mail and web security with identity and access management under a single modular-based platform. By having these solutions integrated into a single platform, customers get a unified view of the data that is leaving the organization and the ability to streamline workflows to manage that data.



The OpSource Cloud is an enterprise-class, highly secure platform. We've taken an integrated approach that considers networking and security together and provides highly customized and granular functionality.

Just as important is the fact that it's price competitive with less robust offerings. You can utilize the OpSource Cloud in a public, pay-as-you-go model—sign up online and pay only for what you use on an hourly basis—and still get all of the enterprise-class security features described previously.

In addition, we offer the OpSource Cloud on a private-label basis to be implemented in your own data center on the VMware, Cisco, and EMC (VCE) stack if you prefer a private cloud. OpSource is not only a highly secure, but also a highly flexible solution.

Last, but certainly not least, the OpSource Cloud is easy to use, with a friendly graphical user interface (GUI) or RESTful APIs.



SecRAMP has built significant expertise and experience around public and private cloud infrastructure. The SecRAMP team has been involved with security implementations on multitenant IaaS security solutions since before cloud was a buzzword.

Unifying security operations in hybrid environments that cover multiple cloud providers, data centers, and hosting solutions with integrated best-of-breed security tools is SecRAMP's core business function, not an ancillary product or service.



Virtustream's xStream platform is the only cloud available today that offers the elasticity and cost savings of true multitenant cloud service with the guaranteed security, availability, and management required for mission-critical enterprise applications. Our cloud is more than just outsourced virtualization. It is a full cloud platform, management portal, on-boarding engine, and the surrounding expertise and methodologies—designed to instill trust in enterprise customers for hosting their production, back-office, and mission-critical applications.

The Virtustream Advisor is also a unique offering, analyzing a customer's environment for the most efficient computing method for each individual application. Every enterprise has different needs and requirements, and the Virtustream Advisor process details and catalogs these to custom-tailor each customer's cloud security model. The Advisor process includes security advice and custom on-boarding deployments to suit an enterprise's security model. During this process, security is addressed as one of the primary areas.

Q9:

Do you have a method for demonstrating ROI for your cloud offering?



Yes, again through the solution and consultation approach, we help customers understand ROI. We should note that cloud is often more expensive than other solutions for supporting long-running infrastructure, so it is not uncommon for customers to come to Carpathia for a cloud solution but end up purchasing a hybrid of cloud and traditional-hosted infrastructure. This often yields the best ROI.



Yes. We help our customers calculate cloud security ROI by evaluating their initial financial investments plus ongoing operational and other associated costs over a given time period versus the financial benefits generated by such investments. These financial benefits include (but are not limited to):

- Increased productivity of both employees and IT team
- Better business agility
- Cost savings due to reduced security incidents and attacks
- Improved protection of sensitive information and data

See a specific [cloud security ROI example](#) for the Cisco IronPort* e-mail and web security solutions.



Yes; in addition to existing methods, the Citrix cloud team is developing specific tools that demonstrate ROI for cloud initiatives.



Expedient can effectively demonstrate the ROI for its cloud offering. Taking into account real-world values, specific to the individual customer or interested business, Expedient can work to develop a clear and concise ROI study to help an organization determine the benefits of the cloud.



The HyTrust ROI is no different from that of virtualization or cloud computing. The benefits of better hardware utilization (or utilization of third-party hardware platforms in the cloud), the ability to enable self-service for interdepartmental private clouds, backup and restoration savings, and so on are identical.

The primary difference, however, is that HyTrust delivers the ability to virtualize more workloads and/or offload them into the cloud. HyTrust enables organizations to virtualize workloads once deemed too mission critical, too sensitive, or too risky. With controls in place from HyTrust, more organizations are finding that these systems are no longer removed from cloud consideration.

Q9) Continued



Yes. Since every organization's environment is different, a McAfee representative would be happy to walk a customer through the process.



We commonly compare the costs of cloud hosting to dedicated server hosting, whether it be internal server management or traditional collocation in an outside data center. In either case, we have a detailed methodology that we follow with prospects to capture information on their current spending, covering both operating expenses and capital expenditures. We then compare their current delivery model and cost structure to a deployment within the OpSource Cloud to show the cost savings and ROI on the decision to migrate to the cloud.



We don't currently have an ROI calculator or absolute method of demonstrating ROI. Our goal is to ease the pain of migrating to the cloud and unify the view of security across the enterprise by tying together the security tools across the platform so that organizations can focus on their core business and leverage economies of scale.



The Advisor tool uses a proven financial framework, including hard costs of computing and soft costs of business, security, and regulatory requirements to compare total cost of ownership (TCO) under the current scenario to private cloud and multitenant cloud options. Virtustream's Cloud Advisory Services works with our clients to provide extensive, customized business cases, ROI, and TCO analyses as appropriate.

Q10: Are there security concerns that your solution doesn't address that you think the industry still needs to solve?



We would like to see hypervisors take more advantage of trusted extensions appearing in modern CPUs and chipsets. This, paired with a policy engine controlling orchestration, opens up many interesting possibilities for trusted cloud computing. While we have made great strides in furthering cloud networking, this is also an immature area and in need of continued innovation to extend trust throughout the cloud ecosystem.

Carpathia is also following with interest the integration of hardware security controls such as Intel TXT to allow a chain of trust from the hardware to the hypervisor to the operating system. Intel TXT has massive potential for trusted cloud computing. Being able to show a chain of trust from hardware to the exposed operating system is very important, especially to our Department of Defense customers.



There are many opportunities for the industry to collaborate on better and more efficient solutions. Automation is a specific example. From a cloud security perspective, automation presents two challenges: (1) how to secure an automated environment and (2) how security service provisioning can be automated in a cloud environment. Cisco is working actively on solutions to address these challenges. The industry also can work together to establish awareness and technologies and standards for better visibility, efficiency, and interoperability.



Some of the biggest security concerns in the cloud are administrative mistakes and lack of approved workflow. Citrix solutions are workflow enabled to reduce the likelihood of administrative-induced errors.



End-to-end chains of trust are still in need of development; we see Intel as continuing to push the envelope, and we're looking forward to being able to provide that type of security technology to our customer base. Additionally, we continue to do research into better encryption key management to help our customers because that is a weak point both in and out of the cloud.



HyTrust is laser focused on delivering a security solution for virtualization and cloud computing within four critical areas: authenticating and verifying administrator identity, verifying integrity of the cloud infrastructure, validating all administrative change requests, and providing a complete system of record for the state of and changes to the cloud infrastructure. This is only one piece of the greater security puzzle.

Many of the original security challenges in the physical data center—patch management, antivirus, vulnerability management, security event and information management, and so forth—still exist in the cloud and still require vigilant attention. While numerous solutions are available to address each of these challenges, the integration between and among these solutions is wanting. Tighter integration would undoubtedly present a more unified view of cloud security and enable a simpler and more straightforward means of managing these complex environments.

Q10) Continued



Enterprises want and need greater transparency and assurance from cloud computing providers. An organization needs to know where its data is stored, how it is managed, and who has access to it while it is in a third-party cloud provider's environment. And the organization needs the reassurance that if or when it switches cloud providers, no data is left behind. The industry needs to continue to work on providing cloud computing customers with the ability to track and monitor data when using cloud computing, which will help ensure against data loss.



As a provider who has been serving the needs of enterprise IT for more than 10 years, we address the vast majority of our clients' key security demands and have evolved our practices over time to keep pace with constantly changing security requirements.

One area in cloud security that can create confusion for clients is the vast array of potential security standards that a cloud vendor could choose to adopt. SAS 70, PCI, SSAE 16, International Standards Organization (ISO) 27001 and 27002, and FISMA are just a few. There are groups like the Cloud Security Alliance (CSA) forming to attempt to organize the disparate set of rules into a cloud-specific standard. Until there is a widely accepted security standard, clients and vendors will continue to have to choose from the variety available today.



Absolutely. There is no silver bullet in security, and it is not an easy problem to solve. Ultimately, cloud infrastructure providers must architect their solutions to provide the visibility and transparency that large enterprises need as they move more computing resources and applications to the cloud. All of us need to work on a continuous improvement in security posture to protect our data, independent of where that data happens to be hosted or is physically found at the time it is accessed.



Full demonstration of data life-cycle management is a challenge for all providers, cloud based or not. Once an enterprise's data is in the hands of a service provider, demonstrating or proving that the data has not been accessed by any outside parties, that backups are in a secure location, and that all data is erased or unrecoverable upon deletion is difficult.

Encryption of all data at rest is a possible solution, but the impact on overall system performance can be significant. Only recently have technologies such as Intel AES-NI (in the CPU) come to market to alleviate performance concerns. Additionally, enabling the customer to be the only holder of the private key to unlock their data is nearly impossible while also managing the infrastructure demands of other customers.

In addition, as we expand our closely held federated cloud into a more open, diverse environment, there are several key security areas that we will need to address, such as software integrity, data encryption in motion, and transference of application authentication.

Q11: I'm just beginning to investigate cloud security. What advice can you give me, and what steps should I take to make sure I'm covering all my bases?



Starting out, we would suggest that you look for transparency from your cloud vendor. If they have a SAS 70 standard for their platform, insist on being able to review the controls they have adopted. Also look for their involvement in industry groups such as the CSA and standards such as cloud audit. Industry benchmarks are key to educated buying decisions.



Organizations that are starting their cloud journey will need to identify how their cloud strategy helps them achieve their overall business objectives. As an integral part of the cloud strategy, they will need to ensure that their cloud security governance process can provide policies, procedures, and standards for a smooth and secure transition to the new business computing model. They need to map out their cloud security architecture and implement cloud security solutions accordingly. If they engage cloud service providers, they should also insist on a strong service level agreement (SLA) that specifies requirements for data confidentiality, integrity, and availability. In addition, they should also discuss their rights to audit.



Read the fine print. Test everything (especially failure conditions). And plan for a loss of connectivity to the cloud and ensure that your business is still operational. With the right architecture and business resumption planning, even the occasional glitch won't result in damaging downtime and loss.



Don't shy away from asking the more difficult questions regarding architectures and data controls. Don't take a SAS 70 or SSAE 16 as the end-all document guaranteeing security. Do treat cloud-based services like you would any other outsourced or hosted platform. Do inspect what you expect of your providers—how providers operate and their control and testing processes. Do thoroughly review all SLAs and ask for security elements to be included in those SLA terms. Make a physical site visit so that you can see that what is represented on paper is followed in real-world operations.



At its core, the cloud is enabled by a combination of technologies and solutions from a variety of vendors, but virtualization is perhaps the most critical element. Thankfully, a number of organizations—NIST, SANS Institute, PCI-DSS, CIS, and more—have published guidelines for securely migrating workloads onto virtual infrastructure. These same guidelines should be referenced before migrating into the cloud because the methods for securing virtual infrastructure are perfectly applicable.

Q11) Continued



The first step is to understand where your data is within your organization and decide whether or not it should be moved to the cloud. You can't protect your data if you can't accurately describe what it looks like and where it is. Then you must classify the data that flows through your networks so that you have a real-world map of all your critical information assets. This provides the insight to build policies to protect your data. These policies are then built into the security solutions so that only the data you want moves into the cloud, and sensitive and confidential data stays protected.



You should ask the same basic questions you do when dealing with internal security, such as:

- Does my cloud environment allow individual user accounts for log-in so that I don't have to share credentials with multiple people?
 - Does the cloud environment include management auditing to show who took what action and when? Without this type of auditing, many internal compliance requirements cannot be met.
 - Can I build a traditional multitiered network with firewalls and ACLs between each tier of the network? If not, am I comfortable with my database having less separation from the DMZ than I do in a traditional network structure?
 - Have I (or my vendor) performed network penetration testing and application vulnerability testing to ensure that my network and application are not vulnerable to common hacking attempts?
 - Does my cloud vendor provide network IDS?
 - Does access to my back-end environment require VPN connectivity, or is anyone on the Internet able to access it?
-



Someone just beginning to look into cloud security should get involved with organizations like the CSA and the Open Data Center Alliance (ODCA). Both are excellent organizations looking at the problem from different perspectives. The CSA has a certification program called the Certificate of Cloud Security Knowledge (CCSK). While a CCSK doesn't make you an expert on cloud security, it does help you to learn about what the CSA and the European Network and Information Security Agency (ENISA) are focusing on in cloud security.

The information provided by these organizations covers a lot of the important areas that customers will need to know about when they are ready to contract with a cloud provider. Also, it is beneficial to get involved with (or consider starting) a local chapter for one of these cloud organizations and attend some of the cloud-focused tracks at security conferences. This will enable networking with other professionals who are facing many of the same challenges and strategic decisions with cloud computing.

Q11) Continued



Partner with a provider who can cover any and all of your security concerns with a proven security model. The best advice is to ask for detailed information about:

- Service and data isolation
- Layered security checkpoints
- Security event correlation and alerting
- Application expertise
- Network security
- Data encryption in motion and at rest
- Data and software integrity and auditability

Q12: What tools do you offer to establish, maintain, and protect identity in the cloud?



We use a variety of tools and techniques to support identity in the cloud. We also focus on privacy, including Electronic Protected Health Information (ePHI) and personally identifiable information (PII). These tools are embedded in our solution and delivered as a service to our customers.



Cisco provides a number of cloud security solutions to protect data and identity in the cloud. One specific example is the [Cisco Secure Cloud Access solution](#). With this solution, Cisco cloud security provides a critical SaaS revocation capability that establishes user identity and enables secure access to cloud-based SaaS applications.

The Cisco SaaS revocation capability is delivered by the Cisco IronPort S-Series web security appliances to provide scalable access control to SaaS applications. When this capability is enabled, no direct access to SaaS applications is permitted. Instead, SaaS users are authenticated at a central place within the SaaS cloud subscriber organization. After successful authentication, security assertion markup language (SAML) is used to authorize access to SAML-enabled SaaS applications.



Citrix works with the leading identity providers in the Citrix Ready program to provide for identity management. Citrix is a thought leader in the bring-your-own-identity (BYOI) space, helping combine personal identity and corporate identities to facilitate access to multiorganizational applications and data.



Today these tools are specific to customer implementation, based on the technology deployed in their environment. Expedient helps to protect our clients' identities more through process and governance than through a tool set. This is an area where we don't publish specific details because doing so would help provide parties with ill intent with a roadmap to discover the information we are tasked with protecting.



With HyTrust Appliance in place, there are no anonymous changes to the virtual infrastructure. All administrative access must first be authenticated. HyTrust can leverage any preexisting investment in LDAP or Microsoft* Active Directory.* For even tighter security, HyTrust fully supports two-factor authentication with RSA SecurID or smart cards. In the event that root access is required, HyTrust Appliance features root password vaulting, which enables certain administrators to check out a temporary password for one-time access. All access to the environment can be tied back to a specific individual—a critical requirement in security and compliance-conscious data centers.

Q12) Continued



A key module of McAfee Cloud Security Platform is our Cloud Identity Manager, which enables organizations to enforce corporate standards for cloud application access. Cloud Identity Manager integrates with the corporation's enterprise directory to auto-provision and de-provision cloud application accounts. It also integrates with existing corporate identity systems to provide users with SSO for internal and cloud-based applications. In addition, overall application access security is strengthened and the risk of data loss is reduced through policy-based enforcement with strong two-factor authentication for cloud applications.



In the area of user management, OpSource ensures that each individual accessing the cloud environment utilizes a unique set of log-in credentials (which is not always a given in cloud environments). Each user is assigned role-based access permissions that assign read and write permissions individually to the network, cloud servers, cloud files, and cloud audit reports.

In addition, we log each action that is taken in OpSource Cloud and tie it back to the user who performed the action. These logs track changes that take place via our web-based UI, or actions taken via an API call.



We don't offer any specific identity tools for the cloud. However, we are able to leverage existing tools. There are some interesting identity and access management vendors who are developing some cloud-based identity tools, such as [Duo Security](#) and [Ping Identity](#).



Because our xStream Platform isolates a customer's cloud resources from all others and becomes an extension of their existing environment, any methods used for identity management in the existing infrastructure can be used in the Virtustream xStream infrastructure with very few changes required.

Q13: What services do you have for federating identity between clouds (public and private)?



While a lot of attention and hype has been given to multi-cloud deployment, in reality this is not the adoption we have seen for enterprise and federal customers to date. What we do see is the need for trusted interface between public and private clouds, for example, within our own data centers that support both private and public clouds. Today's bandwidth charges make "cloud bursting" between on-premises and public clouds out of reach for many customers. In addition, the effort required to support this model may be better spent on more direct initiatives to drive ROI from the cloud.



Currently Cisco does not offer federated identity service.



NetScaler Cloud Gateway is designed to federate identity between public, private, and hybrid clouds—especially coordinating access to SaaS applications.



These services are currently under development. We expect to have robust capabilities within the next 12 months. Many of the technologies that Expedient has tested up to this point limit some of the key functions and benefits that users turn to the cloud for to begin with. From the information available at this point, Expedient is confident that the second generation of these technologies will be more feature rich and deliver a better customer experience.



- **Virtual Appliance Form-Factor:** HyTrust Appliance is provided as a standard VMware-compatible virtual machine, which allows for easy drop-in deployment into any existing virtual infrastructure. Virtual Appliance Form-Factor takes advantage of benefits afforded to any virtual machine, including backup, disaster recovery, and redundancy capabilities.
- **Federated deployment:** Secure distributed system architecture allows for automated replication of policies and templates across multiple HyTrust Appliances as well as geographic boundaries.
- **Directory server bridging:** Natively integrates with Microsoft Active Directory—as well as any LDAP v3 server—so that organizations can leverage a preexisting repository of users, roles, and groups to provide unified access across heterogeneous infrastructure.
- **Two-factor authentication:** Native support for two-factor authentication solutions, including RSA SecurID, enabling organizations to achieve strong authentication without requiring manual configuration or integration of each individual virtualization host.

Q13) Continued



McAfee Cloud Identity Manager provides first-mile session look-up connectors to common identity-management solutions and enterprise platforms such as Microsoft SharePoint*, as well as last-mile session creation and account provisioning connectors to popular SaaS and platform as a service. Federated authentication and authorization protocols are based on SAML, eXtensible Access Control Markup Language (XACML), and emerging OAuth and OpenID identity standards that can connect Internet-based identity providers (for example, Facebook) with corporate identities and authorization policies.



OpSource enables customers to extend their internal network into the OpSource Cloud entirely behind the firewall through the creation of a site-to-site VPN tunnel between environments. With this capability, they can easily extend and integrate existing user-authentication and user-management systems into their cloud environment so that user credentials apply equally in all environments.



Our security services portal provides organizations with visibility into their public and private cloud security infrastructures. The portal provides SSO with a high-level security overview and direct access to the individual security tools that are deployed across the customer's entire organization.



The xStream cloud offering is often configured as just another "node" on an enterprise's network because the xStream platform isolates a customer's routing from all other customers and the enterprise platform is isolated from all inbound Internet connections. This extension can utilize existing WAN technologies deployed in the customer's enterprise, private point-to-point connections, or VPN tunnels with any sort of encryption or authentication measures required by the customer's business.

Intel Resources for Learning More

For more information about Intel and cloud security, see the following:

Understanding Cloud Security

Cloud Security Planning Guide

Seven steps to planning cloud security based on the real-world experience of Intel's IT Department. Includes recommendations for strengthening data and platform protections in cloud implementations. intel.com/content/www/us/en/cloud-computing/cloud-computing-security-planning-guide.html

Cloud Security Insights for IT Strategic Planning: Intel's IT Manager Survey on Cloud Security

This survey of IT professionals provides a benchmark for how IT managers are approaching cloud security, so that organizations can use it in their own IT planning efforts. intel.com/content/www/us/en/cloud-computing/cloud-computing-security-for-it-strategic-planning-report.html

Information Security and Cloud Computing

Intel Chief Information Security Officer Malcolm Harkins shares his perspective on security and the cloud in this short video. intel.com/content/www/us/en/enterprise-security/enterprise-security-intel-it-malcolm-harkins-best-practices-video.html

Rethinking Information Security to Improve Business Agility

To enable rapid adoption of new technologies and usage models—and provide protection in an evolving threat landscape—Intel IT has embarked on a radical five-year redesign of Intel's information security architecture. intel.com/content/www/us/en/enterprise-security/intel-it-enterprise-security-rethinking-information-security-to-improve-business-agility-paper.html?wapkw=

Intel Cloud Builders Initiative

Intel Cloud Builders Program

Get guidance from this cross-industry initiative to build more simplified, secure, and efficient cloud infrastructure. Intel Cloud Builders provides information and advice designed to simplify, secure, and increase the efficiency of cloud infrastructures. intel.com/content/www/us/en/cloud-computing/cloud-builders-provide-proven-advice.html

Enterprise Security: Laptop Anti-Theft Protection

This video describes how Intel Anti-Theft Technology (Intel AT), built into the laptop hardware, can help IT administrators outwit thieves, even when they attempt to reimage the operating system, change the boot order, or install a new hard drive. Stolen laptops with Intel AT can be remotely disabled if stolen or lost and, once recovered, quickly reactivated to normal operation. Length: 2:33 minutes.

<http://www.intel.com/content/www/us/en/enterprise-security/protect-laptop-data-with-anti-theft-technology.html?wapkw=anti-theft>

Evolution of Integrity Checking with Intel® Trusted Execution Technology: An Intel IT Perspective

In 2010, Intel began transitioning to a private cloud environment to improve efficiency and agility. The highly virtualized multitenant environment creates new security challenges, including those presented by emerging threats such as rootkit attacks. Intel evaluated Intel TXT as part of its analysis of technologies that can potentially address these issues.

intel.com/content/www/us/en/pc-security/intel-it-security-trusted-execution-technology-paper.html

Intel® Advanced Encryption Standard Instructions (AES-NI)

This article by Intel expert Jeffrey Rott is an in-depth look at using Intel AES-NI, with a specific focus on the 2010 Intel Core™ processor family and its performance and security benefits.

edc.intel.com/Link.aspx?id=5093

Intel Identity Protection Technology

Web page providing an overview of Intel Identity Protection Technology (Intel IPT)

intel.com/content/www/us/en/architecture-and-technology/identity-protection/identity-protection-technology-general.html?wapkw=identity

Regain Control ... Secure the Dynamic Perimeter

Web page with the latest on products, solutions, news and events, and content from Intel and McAfee related to cloud perimeter security.

dynamicperimeter.com/

Securing the Enterprise with Intel® AES-NI

This white paper describes AES usage scenarios, performance implications, and the cryptographic libraries that ISVs can use to replace basic AES routines with the Intel AES-NI optimizations.

intel.com/content/www/us/en/enterprise-security/enterprise-security-aes-ni-white-paper.html

What is Intel® Trusted Execution Technology?

In this 10:28-minute video, Intel security expert Jim Greene talks about the benefits of hardware root of trust with Intel TXT and TPMs, and how hardware integrity checking is a key component of cloud security.

intel.com/content/www/us/en/cloud-computing/cloud-computing-trusted-execution-technology-video.html

Share with Colleagues



No computer system can provide absolute security under all conditions. Intel Trusted Execution Technology (Intel TXT) requires a computer system with Intel Virtualization Technology, an Intel TXT-enabled processor, a chipset, a BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.2. For more information, visit intel.com/technology/security.

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

Intel AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel processors. For availability, consult your reseller or system manufacturer. For more information, see software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

No system can provide absolute security under all conditions. Intel Anti-Theft Technology (Intel AT) requires an enabled chipset, a BIOS, firmware and software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit intel.com/go/anti-theft.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. Intel disclaims all liability, including liability for infringement of any property rights, relating to use of this information. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Copyright © 2011 Intel Corporation. All rights reserved.

Intel, the Intel logo, Intel Sponsors of Tomorrow., and the Intel Sponsors of Tomorrow. logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Microsoft, Active Directory, and SharePoint are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

0911/JM/ME/PDF-USA

326281-001



Sponsors of Tomorrow.™