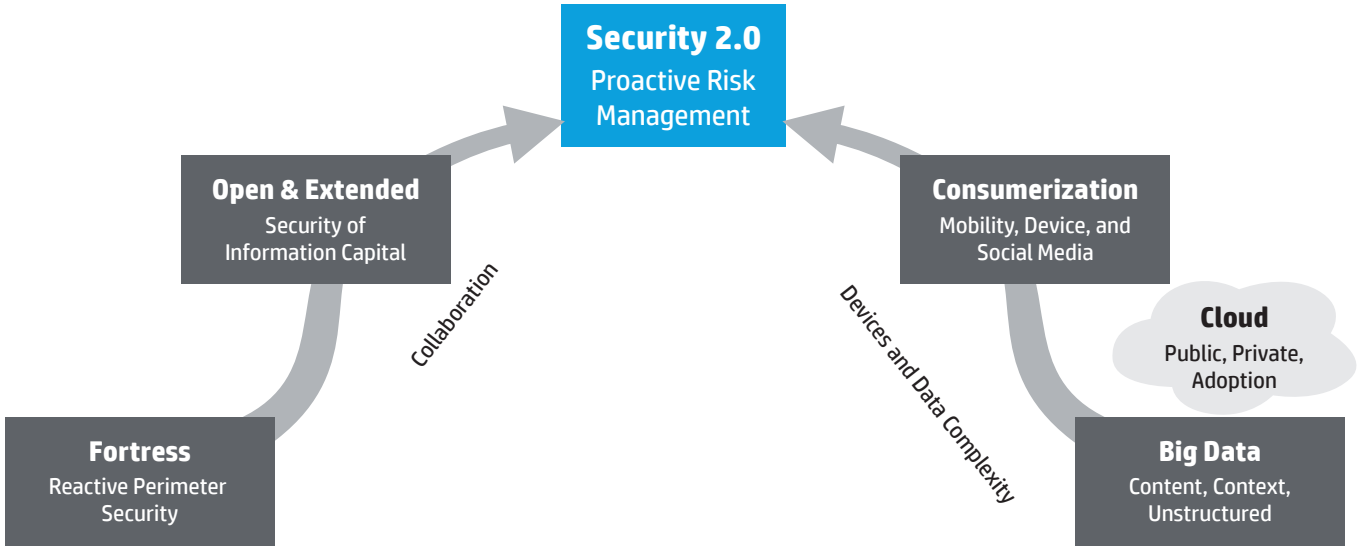
White paper

Minimize the risk of your cloud-based services

HP Enterprise Security Services

Table of Contents

Figure 1. Technology trends driving the need for Security 2.0



Introduction

The promise of the cloud is appealing: reduced costs, greater agility, flexibility, scalability, and potentially greater security. At the same time, IT organizations recognize that the cloud introduces a number of issues related to security, data integrity, compliance, service-level agreements, and data architecture that must be addressed. Therefore, the adoption of cloud services is being tempered by a significant level of uncertainty. Numerous surveys indicate that the top concerns for moving to the cloud are: 1) security, 2) performance, and 3) availability. In other words, enterprises are looking for assurances that they are not adding risk to the business by leveraging the cloud. For many, moving to the cloud is still a leap of faith.

Different cloud deployment models—public, private, or hybrid—have different security vulnerabilities and risks. Generally, risk increases from greater degrees of multitenancy among increasingly unknown participants. HP believes that cloud security begins with, and adds to, well-defined enterprise security. Although there is ample discussion of cloud security in literature and industry media, CIOs must focus on securing their own enterprise's use of cloud-based services and not whether the cloud, in general, is secure.

CIOs and CISOs should consider the following broad steps as part of a cloud security program:

- Establish a risk-based approach.
- Design (or convert) applications to run in the cloud securely.
- Implement ongoing auditing and management.
- Assess infrastructure (and platform) security during service sourcing.

These steps will help address changes to the security landscape in a new era of cloud-based services and solutions. Cloud environments have reduced or removed traditional security perimeters, which means that enterprises need to adopt an information-centric approach to security. There will always be a need to continually assess risk and be agile in appropriately adapting new cloud solutions.

"It's not about securing the cloud; it's about securing your enterprise's use of cloud-based services."

When moving to cloud-based solutions and services, enterprises must first address the definitive information-related risks associated with a shared-service model. There will be many questions and concerns that can affect enterprise risk for using cloud services. Addressing cloud security requires total business involvement from the enterprise.

It takes a new approach

Security concerns are not unique to cloud; cloud is just one of many disruptive technology trends. In today's enterprise, there's an increased drive to adopt new technologies related to devices and data in particular, all of which alter the approach to enterprise security. Traditionally, the IT security environment of most organizations was seen as a hard shell with a soft center. Security was based on creating a strong perimeter to keep threats out of the organization. Once through this shell, security was typically light. In part, this reflected the model where data and applications were essentially static. The only way to access data was via an application, so a security fortress could be built around this static pairing.

Figure 2. Various interpretations of "cloud security"

Security FOR the cloud	Security technologies, solutions, and services that allow you to secure your application and data in the cloud
Security FROM the cloud	Security technologies that are delivered to you in a "security-as-a-service" way
Security IN the cloud	Security technologies and methods that enable cloud platforms and applications to be intrinsically secure in their cloud environment
Security ACROSS clouds	Mechanisms for secure interoperability across cloud boundaries, either hybrid public/private models, or a multicloud model consisting of a cascading network of service providers

This has resulted in a common digital access tradeoff of richness versus reach—a few people can have access to rich, useful data, or a lot of people can reach limited and diluted data. Because traditional monolithic IT systems were complex and expensive to maintain and alter, few parts of an organization were supported by rich data and processes. The rest of the organization was, and often still is, "information poor"—relying on home-brewed spreadsheets fed by limited data from the core IT systems. However, as business has become faster and more global, the need to share data has increased. The traditional models do not really address the needs of mobile data and applications. Enterprises need richness and reach.

These trends also mean that the traditional corporate perimeter, with clearly identifiable boundaries, has diminished, making a perimeter approach nearly impossible to maintain. Compounding this situation is the rise of computer hacking and the rapid increase in security and privacy compliance legislation. This is creating a "perfect storm" of increased complexity. Complexity often results in significant blind spots within an organization, meaning that organizations have to force their security controls to be reactive to the latest threat or fire drill.

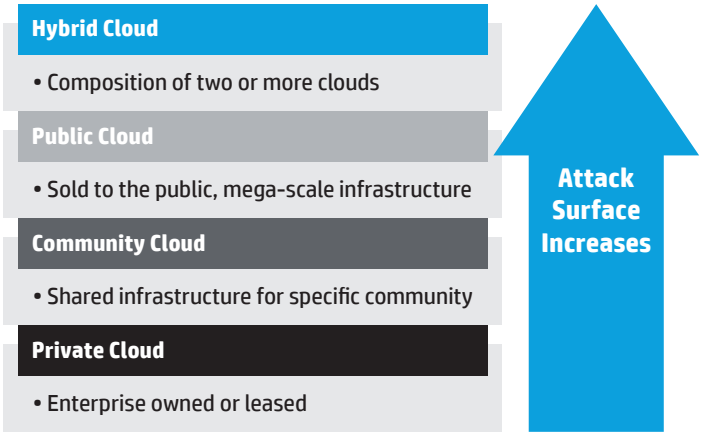
At HP, we believe security must move to the next level to meet these rising business opportunities and challenges. For security to be a more integral part of the business processes and data, effective security should be incorporated into processes throughout an enterprise, not just on the perimeter or in the cloud. A holistic and comprehensive approach is required. We work with our clients to help them take a proactive, risk-based approach. We call this Security 2.0.

For this paper, we will be addressing security *for* and *in* the cloud.

Cloud security—an enterprise focus

Attempting to define and achieve "cloud security" may be similar to trying to attain world peace. As we will briefly outline below, the cloud can mean many different things to many different people or organizations, and can be analogous to the full spectrum of IT services. Security in this complex environment, like peace, can never be 100 percent achieved and guaranteed. And security, like peace, is a journey, not a destination.

Figure 3. Cloud deployment models



There are only degrees of more or less security, which ultimately must be judged in context of an enterprise (or individual). We should strive for cloud security by addressing the issues and vulnerabilities that we can control. For this reason, we stress that your focus should be on "securing your own enterprise's use and application of cloud-based services" to set the appropriate context upon which sound business decisions can be made.

What do we mean by "cloud security?"

There are many aspects to security and cloud. It is important to understand in what context you're evaluating the security of cloud services and what your own specific requirements are within that context. To begin, we outline four broad perspectives of cloud security. See Figure 2.

Security posture of cloud deployment models

Different cloud deployment models greatly influence the potential security vulnerabilities or "attack surface," as shown in Figure 3. The increasing risks arise from an increased level of multitenancy among progressively more unknown participants.

Private cloud

The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on premise or off premise. In the latter case, this is typically known as a managed/virtual private cloud. A private, on-premise cloud solution, deployed in an enterprise-owned/operated data center, has a similar security profile to other noncloud systems that are operated in the same facility. Risks may increase by sharing resources among different business units or in the shared use of storage facilities for data (assets) with different security classifications (such as mixing an internal company blog storage area on storage used for data with requirements and regulations for PII).

Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns such as mission, security requirements, policy, or compliance considerations. It may be managed by the organizations or a third party and may exist on premise or off premise. A community cloud increases that level of shared resources by including a community of organizations with potential increases for security incidents, data exposures, or breaches. The risk profile of the community cloud is bounded by the limits upon which the community is defined, and we assume this size is less than that of a public cloud.

Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. A public cloud typically places no limits on the community of customers that may use and subscribe to the use of the shared resources that the public cloud service provider offers—other than an ability to pay for services consumed. A public cloud can be viewed as a community cloud with no limits on community membership or makeup.

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public), each of which remains unique entities but are bound together by standardized or proprietary technology that enables data and application portability (often called "cloud bursting"). A hybrid cloud is, by definition, the combined use of two or more clouds to provide services for a common business function or application that can make dynamic use of the collection of facilities. The term hybrid cloud often refers to the use of a private cloud with an overflow or capability to scale out to a public cloud.

Security expectations of cloud service models

It is important to recognize that all clouds are not created equal in terms of service levels and security. Cloud services are often described by the type of service model that is offered. This is sometimes called the "SPI" model, referring to software –as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

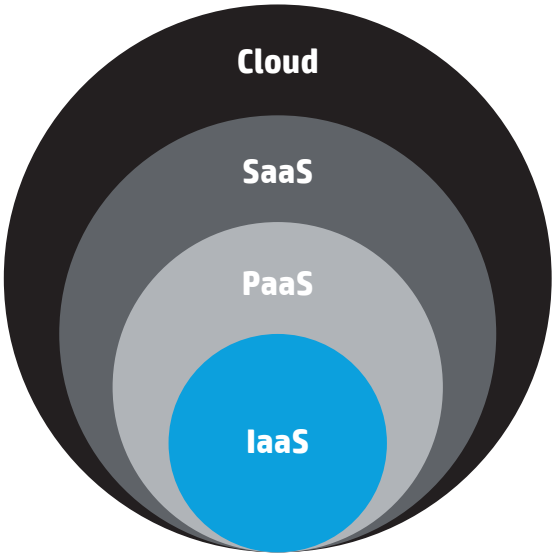
Is cloud secure?

A lot of discussion is currently going on in business and the IT sector about the security and reliability of cloud computing. High-profile service interruptions experienced by leading cloud services providers like Amazon—as well as security issues and hacking attacks that have occurred in services delivered by Sony and Google's Android operating systems—have raised questions about the overall security and, hence, the safety of cloud-based solutions. In reality, many of these attacks used web application security flaws as their attack vector and so did not occur because the target system was, or was not, in the cloud.

On the other side of this argument are those who believe that a centralized system, or cloud, is inherently easier to secure, as you have a single place to manage security. In distributed systems, it is complex to apply security patches or to manage security. In a single centralized system, patches can be applied once, and all systems will receive the new protection. The counter-argument to this is that a single centralized solution allows hackers to focus all their energy on a single point of attack.

So is there a simple answer to the question "Is cloud secure?" The HP view is that security is an enterprise issue, not just a question about cloud, and therefore, the use of cloud services must be examined in the light of enterprise requirements and needs.

The selection of a service model has a great effect on the distribution of roles and responsibilities of the cloud service provider and the cloud service consumer. In general, when using SaaS, the provider has more control and responsibility. By contrast, the consumer has more control and responsibility when using IaaS. So in many ways, organizations need to choose how much risk they want to retain and how much they are prepared to share with the cloud broker/provider.



IaaS or infrastructure as a service—Providers generally offer basic network and infrastructure security, firewalls, and some tools—but the consumer is generally responsible for implementation, operations, and monitoring.

PaaS or platform as a service—This option may provide some additional security functions for identity management and secure application development; security falls to the applications developer to properly use and configure the necessary security methods as provided by the PaaS.

SaaS or software as a service—Providers generally offer application, data, and infrastructure security, with varying degrees of compliance.

What is really new about cloud security?

Despite what is commonly reported in the industry press and other media, many cloud security incidents are actually previously known issues with web applications and data hosting, but at greater scale and frequency, due to early adoption of new cloud services. The underlying cause of many of the incidents was found to be phishing, downtime, data loss, weak passwords, or compromised hosts running botnets. This is not to say that these incidents are not "real" or important—they are. The point here is that there is nothing inherently cloud related that caused these incidents to occur.

It should be noted, however, that most clouds are shared, whether among programs, organizations, or communities. This means that "the needs of the one rarely outweigh the needs of the many." Security policies and service-level agreements can be used to manage expectations, support management decisions regarding providers, and govern performance—but cannot typically be imposed unilaterally on a shared service. Companies using cloud need to understand that they are consuming a shared resource and must, therefore, select the service that provides the levels of security and service that they need.

The following are some examples of new risks that arise from the use of cloud services, resulting from multitenancy and shared computing facilities and services:

Many traditional security concerns are recast as a "cloud problem."

Side channel and covert channels

Because cloud computing introduces a shared resource environment, unexpected side channels (passively observing information) and covert channels (actively sending data) can arise. As a result, activity patterns may need to be protected in addition to the applications and data sources themselves.

Previous research has exposed vulnerabilities that include ways to place an attacker virtual machine (VM) on the same physical machine as a targeted VM, and then to construct a side channel between two VMs on the same physical machine. Much of this depends on the security mechanisms employed by the cloud service provider—in particular, network configuration and hypervisor security hardening. For enterprises that are highly concerned with masking activity patterns and/or side channel attacks, some cloud providers offer dedicated physical machines, which may warrant additional consideration.

Reputation fate sharing

Reputation fate sharing is an academic way of saying "you are known by the company you keep." This risk entails possible blacklisting or service disruption due to "bad neighbors" in which a single subverter can disrupt many users.

For example, a group of spammers subverted Amazon's EC2 and caused Spamhaus to blacklist a large fraction of EC2's IP addresses. This caused major service disruptions for legitimate EC2 customers, impeding their ability to send outbound mail. A second noteworthy fate-sharing incident occurred during an FBI raid on Texas data centers in April 2009, based on suspicions of the targeted data centers facilitating cybercrimes. The agents seized equipment, and many businesses that were colocated in the same data centers faced business disruptions or even complete business closures.

Such incidents continue today, and the scope of impact is widening. You only need to look at the Megaupload legal case. Here Megaupload is held responsible for illegal information stored on its systems by third parties. This has created a situation where legal users of the Megaupload service seem likely to lose their data due to the actions of other users of the same service.

These incidents outline the need for "mutual auditability" in a multitenant, shared-service model. This means that cloud providers need to audit their customers' use of their services, in addition to customers (enterprises) who need to audit the cloud service provider operations for compliance. Mutual auditability may be a new concept for many enterprises that are not accustomed to being audited or monitored for a service for which they are paying. For some enterprises, this notion may be problematic for certain situations involving highly sensitive information, and this must be addressed in contracts and terms-of-service negotiations.

Longer trust chains

The issue of trust is a significant concern in cloud security. Cloud services may introduce longer supply chains and, in turn, longer trust chains. This results from the ability to create composite services using two or more discrete cloud services in a cascading chain of services. It is important for enterprises to review and understand the supply chain and trust chains of cloud services that they are seeking to use. Enterprises should assess the cloud provider's supply chain for vulnerabilities and other business implications, in the same manner that it assesses other suppliers of goods and services. Key considerations include the following questions:

- Are my security policies enforced throughout the network of service providers?
- Who is responsible and accountable?
- How is compliance measured, documented, and reported?
- What is the reporting process regarding low-level breaches that may affect my enterprise's use of your services?

Trust chains are not only longer; they are also increasingly complex and rising in number. In this setting, the security aspects of the service contract are crucial mechanisms by which the trust relationship between customer and supplier is established and maintained.

Elimination or reduction of security perimeters

The "safe harbor" of on-premise mainframes, servers, storage, and data networks does not exist in most cloud deployment models (with the possible exception of an isolated on-premise private cloud). Gone are the database and operating system models, replaced by platform as a service and the mobile application infrastructure.

The security perimeters that were established to protect critical information assets in the traditional data center do not exist in the environment of cloud services. Because of this, enterprises should pay close attention to moving existing applications and data to a third-party cloud service. The architecture used for existing applications and database designs was most likely predicated on the assumption of a "safe and secure operating environment."

The development team probably did not consider additional measures that would be necessary to protect the application, transactions, and data in a hostile environment. The typical assumption only a few years ago was something like "… security is Operations' responsibility."

What should a CIO/CISO do now?

As with most security challenges today, technical solutions are only part of the puzzle. What is needed is a well-rounded approach to the problem. HP recommends the following broad steps as part of a cloud security program:

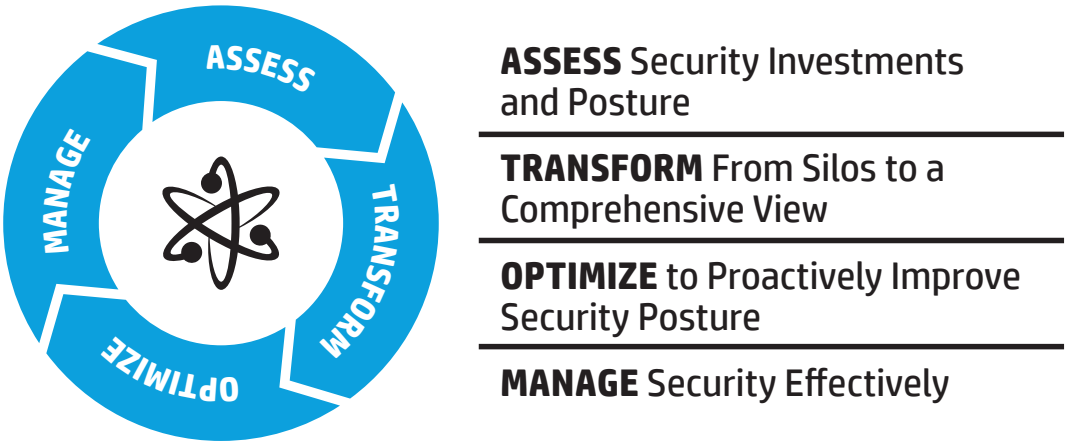
1. Establish a risk-based approach.
2. Design (or convert) applications to securely run in the cloud.
3. Implement ongoing auditing and management.
4. Assess infrastructure (and platform) security during service sourcing.

First, a risk-based approach is necessary to fully understand the risk impact of moving chosen applications and data (assets) to a particular cloud deployment model and service model. This assessment must be undertaken from a viewpoint of how it affects the entire enterprise.

Second, many existing applications were not designed to run in a potentially hostile environment—thus the need to build in security at the application and data level for new systems. Existing applications should be thoroughly reviewed, inspected, amended, and tested before deploying on a cloud platform; this exercise should be guided by the output of the risk-based assessment.

Third, a thorough program for continual and ongoing audit and compliance management is needed in a dynamic, cloud-based services environment. A traditional regime of annual or monthly audits becomes meaningless in an environment that changes completely on a daily or hourly basis.

Figure 4. ATOM risk-based methodology



Finally, the use of cloud services significantly alters an enterprise's ability to exert strict controls over infrastructure, storage, and network security measures. Enterprises should conduct rigorous due diligence through assessments of the selected service providers' infrastructure security policies as part of service sourcing and contract negotiations.

1. Establish a risk-based approach

Establishing a risk-based approach is a critical undertaking of CIOs in an era of cloud services. CIOs are responsible for selecting the services that are necessary to meet the needs of the business. This means they will need to analyze the business needs, using a risk-based approach to identify the service model and security levels necessary to support them. Essentially, this is because cloud is a consumption model for IT services, and key to this model is an understanding of the service levels that must be met.

The primary objective of the HP risk-based approach is to help an enterprise move from a reactive to a proactive stance for enterprise security, with the end goal of measurably reducing business risk. HP has developed a risk-based methodology—assess, transform, optimize, manage or "ATOM"—that helps enable enterprises to achieve these goals. HP can assist enterprises at various stages of this lifecycle, illustrated above; however, we find that enterprises benefit most by completing all four stages to achieve a more rigorous and effective risk-management strategy. The ATOM lifecycle methodology improves an enterprise's security posture while reducing risk and investment, and finds the correct balance between securing and enabling the enterprise.

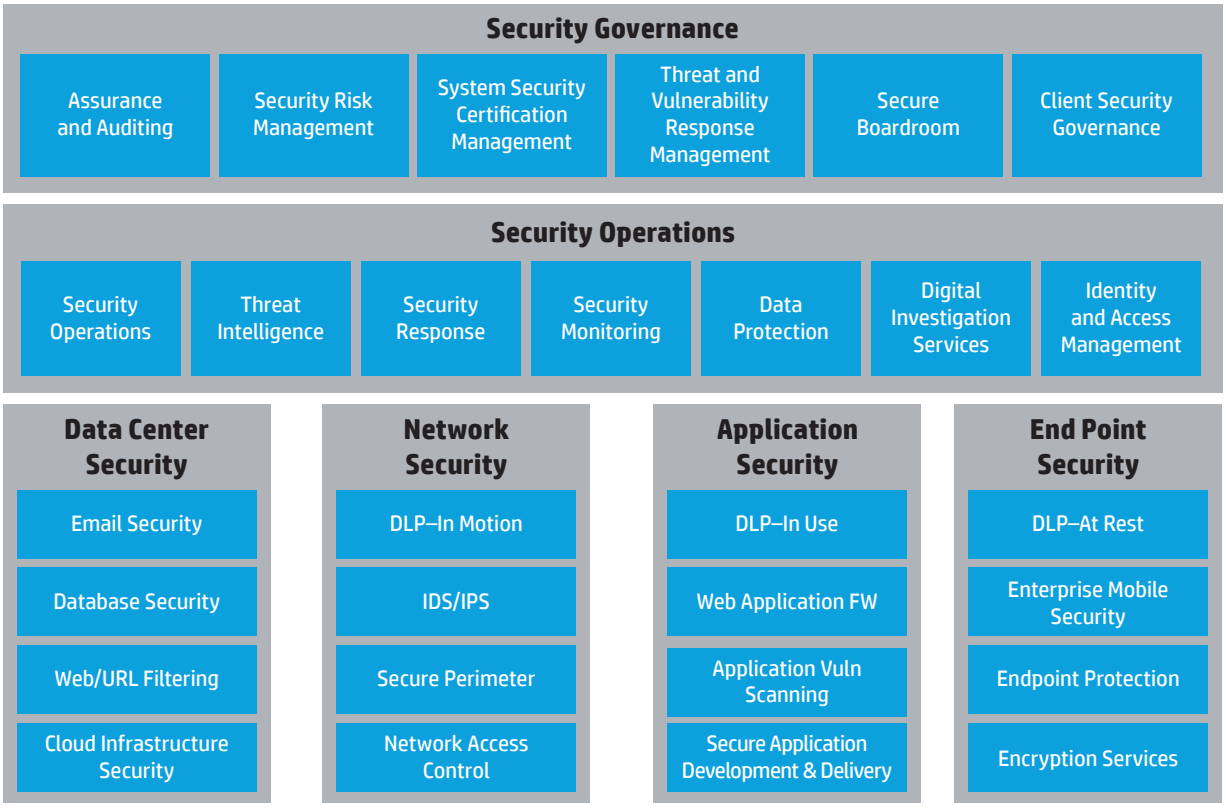
First, we assess our client's risk tolerance profile, compliance requirements, operational requirements, organizational capabilities, and resources. We typically do this within HP Cloud and HP Security Discovery Workshops with the client. We then look to transform our client's environments. We structure and prioritize the client's security issues and undertake remediation projects.

Next, we optimize the environment and also broaden our client's level of security awareness. We help the client continually monitor its environment, and our experts proactively recommend operational and process improvements that can deliver an optimized security and risk posture.

Cloud security begins with, and adds to, well-defined enterprise security.

Finally, we manage the associated security transformation programs required to deliver security in the most effective way for the enterprise, adopting proven security technologies and flexible sourcing models.

Figure 5. HP Enterprise Security Framework



HP recommends the use of our comprehensive, end-to-end HP Enterprise Security Framework, as shown in Figure 5.

This framework is guided by a Security Governance layer, shown at the top. This layer addresses comprehensive governance services that integrate and maintain your security policies and processes in alignment with your business drivers, legal and regulatory requirements, and threat profile.

The Security Operations layer is responsible for managing and delivering security functions and processes, guiding by the policies and requirements noted in the security governance layer above. The technology layers provide technologies, tools, and processes to provide secure operation and monitoring of critical areas for service delivery, including data center, network, application, and end point.

2. Design applications to run in the cloud securely

It should be noted that the cloud is a new environment and, as such, it is not yet clear what the best ways are for companies to gain the most business advantage from its use. The evolution of corporate use of the Internet, for example, has evolved from the tentative first steps of publishing corporate advertising to a website to real-time commerce and collaboration with customers. The cloud will go through a similar evolution, so it is vitally important to implement good application design and deployment practices now to allow safe use of this new and growing opportunity.

Over the past decade, enterprises and traditional IT service providers have become increasingly adept at hardening network and infrastructure through advances in perimeter security, intrusion prevention, vulnerability, and threat management. From an adversarial point of view, when the network and infrastructure are increasingly secured, attackers will move to the next weakest link—applications and data.

Additionally, in a public cloud setting, the traditional “fortress” of the enterprise data center goes away— potentially leaving assets like applications, data, and intellectual property vulnerable to theft, manipulation, exposure, and/or destruction.

We must also consider the significant changes that have occurred in the threat landscape over the past several years. A full treatment of these shifts is outside the scope of this paper, but several trends are worth examining. A significant shift has occurred in the typical threat actors, as well as their targets and motivations. A decade ago, the typical threat agent was the stereotyped “lone hacker” who was motivated to break into enterprise and/or government networks and deface or disrupt websites and services with the primary goal and reward of fame and notoriety. A generalized profile could be assumed to be that of a mischievous adolescent.

Figure 6. The HP Secure Boardroom dashboard

Today, however, we are witnessing organized cyber criminals and nation states engaging in cybercrime and cyber warfare. Not only are the actors different, but their targets and motivations are different as well. In the past, bad actors were seeking recognition; today's offenders are seeking information and intellectual property—and seek to avoid detection and capture. In short, today's threats are not aimed at destroying infrastructure but rather stealing information; hence the need for increased security at the data and application layers.

This brings up the need for a new approach to application development and data management: Applications and data now need to be able to protect themselves. This means that application developers need to adopt an information-centric approach to securing critical applications and data by focusing on the "CIA triad" of confidentiality, integrity, and availability. This implies the need for security, access control, and encryption to be "built-in" at a fine-grained level.

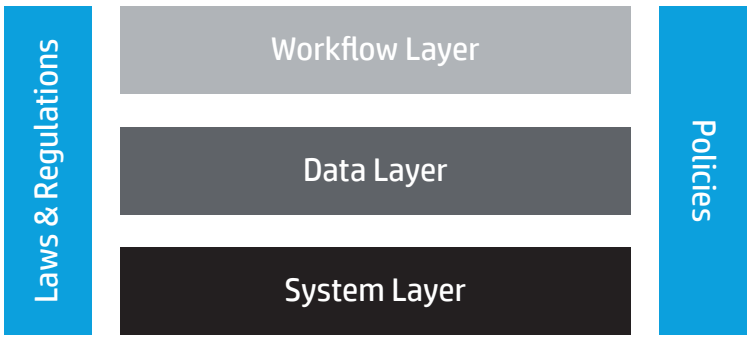
No longer can developers and database administrators rely on the infrastructure and operations teams to build walls and fences—it is a new world. Security is difficult (and costly) to retrofit to existing systems. Ideally, the best time to architect security is during the requirements and design phases of a new system. The dynamic behavior and public environment of cloud implicitly require that data and applications be self-defending.

Adopt an information-centric approach to security.

HP recommends that new cloud applications be developed with security built in. Developing applications with security already designed in dramatically reduces the risk of vulnerabilities and produces solutions that have greater security assurance at lower cost. By addressing new attack surfaces early in the design cycle with a security requirements analysis, security maintenance and remediation needs are reduced during the testing and operational phases. New cloud-based applications and data structures should be designed and built with the following considerations in mind:

- New attack surfaces addressed early in design
- Policy and compliance management
- Anomaly detection, pattern recognition for self-auditing, and self-protecting systems
- Identity management and access control

Figure 7. Abstraction layers of accountability in cloud computing



- Adoption of a new mindset to privacy—encrypt everything by default, end-to-end
- Content-aware encryption to aid data loss prevention by selective data encryption based on policy
- Encryption alternatives—tokenization, data anonymization, fine-grained access controls

Since 80 percent of security breaches happen at the application layer, enterprises should employ third-party testing services for vulnerability analyses and penetration testing. An approach like the HP Comprehensive Application Threat Analysis identifies exploitable security vulnerabilities in applications; prioritizes critical issues; identifies root cause of vulnerabilities; and aids compliance with regulations, standards, and policies.

A traditional regime of annual or monthly audits becomes meaningless in an environment that changes completely on a daily or hourly basis.

3. Implement ongoing auditing and management

Continuous compliance monitoring is essential to securely delivering cloud services and, of course, ensuring compliance. Cloud services are inherently dynamic. The dynamic provisioning and deprovisioning of resources is a key part of the cloud value proposition and business model. This makes automation of operational monitoring, continuous audit, and compliance reporting essential in this dynamic environment. To comply with policy and legislation—such as the EU Data Protection Directive, GLBA, HIPAA, and export compliance controls like ITAR—enterprises require continuously running audit and compliance monitoring.

Enterprises often lack an overall view of their security operations, risk, compliance, and budget, creating difficulties in making informed risk and security decisions. This typically results from many years of implementing specific point solutions and tools that were needed on a reactive basis. As a result, many organizations do not have the means to produce a comprehensive integrated view of the security posture, risk level, and compliance status.

Continuous monitoring and maintenance of security incident records and log files are crucial to enabling forensic examination and analysis in the event that a security breach or disclosure occurs. This information must be available in real time to facilitate rapid response, notification, and containment measures. HP Secure Boardroom provides a single, graphical, executive-level dashboard of enterprise security status that aligns information security at a corporate level. This tool provides real-time views of current security events and improves control of security projects, audits, budgets, and performance.

Communicating the value of security and addressing risk is one of the single biggest challenges for enterprise CISOs because of the difficulties in reporting on actual metrics and return on investment (ROI). HP Secure Boardroom gives users an “at-a-glance” interface, combining existing sources of security data into one central and easy-to-read dashboard. The system also enables leaders to quickly produce reports from multiple data sources, convey feedback with confidence at a corporate level, and make strategic investment decisions. This provides CISOs an enterprise-wide view of risk, cost, and security challenges to help make better informed decisions faster, govern security operations, and work more strategically.

4. Considerations for service sourcing and infrastructure security

The above sections outline the need for 1) a comprehensive approach to governance, risk, and compliance, 2) a thorough review of application level security, and 3) auditing. Next, we must address the needs for infrastructure and network security.

Cloud-based services typically are designed to implement a single unifying architecture, which enables the rapid scaling and reusability features that characterize cloud-based services. While this architecture enables the benefits that make cloud services attractive, it also generally precludes the ability to customize these services to an individual client's requirements.

When using a cloud-based service, the service consumer has much less direct control over infrastructure and network security, including operational policies and procedures, network configuration, intrusion prevention, and traffic control. This is not to say that these issues are not important and critical factors for the security of a cloud-based solution. In fact, they are all highly critical areas in cloud-based services; however, because enterprises have little or no influence on a provider's implementation of mechanisms and controls in these areas, a thorough review of the service provider's policies should be completed as part of the due diligence process during contract negotiation and service sourcing.

Should you find that a particular cloud service does not meet, or cannot meet, your requirements for certain infrastructure-related security measures, you will then need to seek an alternate provider that can meet your particular requirements, or move your application back in-house.

What about the future?

As demand for secure cloud computing continues to grow, innovations are occurring at a rapid pace in numerous areas and disciplines. HP business units and HP Labs are at the forefront of some very important developments in secure and trusted cloud computing.

HP TrustCloud—addressing accountability

A key barrier to widespread uptake of cloud computing is the lack of trust of clouds by potential enterprise users. While preventive controls for security and privacy measures are actively being researched, there is still little focus on detective controls related to cloud accountability and auditability. The complexity resulting from the sheer amount of virtualization and data distribution carried out in current clouds has also revealed an urgent need for research in cloud accountability.

The shift in focus of client concerns from server health and utilization to the integrity and safety of end-users' data further compounds this research need. Researchers at HP Labs are addressing the key challenges in achieving a trusted cloud through the use of detective controls, and have developed the HP TrustCloud framework to achieve accountability in cloud computing via technical and policy-based approaches.

TrustCloud enables all cloud stakeholders to trace their data in and out of the cloud. It adopts an end-to-end, data-centric methodology grounded on a five-layer framework—systems, data, workflow, laws and regulations, and policies. At the systems layer, data events—such as file create, write, delete, or transfer— are tracked at file- and block-level and logged as data logs via kernel-space sensors planted on all virtual and physical machines in the cloud. These logs are then securely transmitted and analyzed for end-to-end cloud data provenance at the data layer.

Workflows and audit trails linking to human users and policies are then distilled at the workflow layer and checked against the laws and regulations layer and policies layer. Data-centric cloud forensic visualizations and tools are built for empowering all stakeholders with the ability to track their data.

TrustCloud enables the collection, management, and analysis of cloud-scale data logs to empower automated transnational data policy management, cloud data forensics, cloud data governance, cloud data leakage detection, end-to-end cloud data provenance, and file violation services for cloud users and regulators.

More information is available at **TrustCloud: A framework for accountability and trust in cloud computing**.

DataPROVE—Tracking your data in the cloud

Provenance, a meta-data describing the derivation history of data, is crucial for the uptake of cloud computing to enhance reliability, credibility, accountability, transparency, and confidentiality of digital objects in a cloud. HP Labs has surveyed current mechanisms that support provenance for cloud computing, and classified provenance according to the granularities encapsulating the various sets of provenance data for different use cases, summarizing the challenges and requirements for collecting provenance in a cloud.

Enterprises need better transparency and accountability of data managed in a cloud. HP Labs has developed an approach called DataPROVE that aims to effectively and efficiently satisfy those challenges and requirements in cloud provenance, and to provide a provenance-supplemented cloud for better integrity and safety of client data. Moving forward, provenance collection must not only be restricted to a single cloud service provider's solutions. Instead, inter-cloud, cloud-to-Internet, and Internet-to-cloud data movement, and management scenarios also need to be investigated further. More information is available at: **How to track your data: The case for cloud computing provenance**.

Managing cloud communities with trusted cloud-client management solutions

The challenges to enterprises in moving to cloud computing include the inability to enforce security requirements relevant for data classification(s). By containerizing our data, we gain not only the ability to separate corporate from personal data, but can selectively introduce functionality such as remote wiping, advanced threat monitoring, or intrusion prevention.

Research promises to take containerization-based security management models to mobile devices more generally, with the appropriate cloud integration for manageability.

HP Labs has been researching systems security architectures for the next-generation cloud-based enterprise and has developed innovative technologies such as:

- **Trusted Computing**
  A system architecture for remotely verifying a device's properties to establish trust
- **Trusted Virtualization**
  A device architecture that can provide container-based security policies for multiple operating systems on a single device while supporting multiple independent IT domains to be managed securely on a single client device

HP Labs is also researching how to use such "state-of-the-art" developments to facilitate cost-effective cloud-based security management enterprise in a consumerized world.

From an IT department perspective, cloud communities could be defined and securely managed throughout, from the end-user cloud client devices to the data center. Importantly, the HP Labs approach is designed to allow end-user devices to be registered with multiple communities, rather than being limited to just one personal and one business persona. By supporting multiple personas, next-generation devices and services will allow multiple IT departments to have advanced security management control over their communities of mobile users and business applications, while end users will be able to maintain privacy and choice for their own device, within other cloud communities, or within personal applications.

Trust Economics—business-aligned decision support

Decision-making and risk assessment for cloud and data loss is very difficult because:

- There is a challenging trade-off between enablement and risk mitigation.
- Stakeholders have different views/incentives/ knowledge/ responsibilities.
- It is not just about technology—there are human factors, too.

HP Labs has developed model-based methodology to analyze risks, enabling stakeholders to instinctively build shared understanding of complex situations and explore what-if scenarios using the HP models. To better understand how HP is helping its clients better manage their risks, watch a case study (**http://bit.ly/xC9GFB**).

Conclusion

As enterprises like yours adopt cloud-based solutions and services, they must first address the definitive information-related risks associated with a shared-service model. There are many questions and concerns that affect enterprise risk for using cloud services. Just a few of these questions are:

- Who can use our services?
- How is our data protected?
- What is the availability of our services?
- How would we be harmed if our data were lost, altered, or exposed to unauthorized parties?
- Who is liable for breaches?
- How can we measure compliance?
- Are we locked in now?

Addressing cloud security requires total business involvement from the enterprise. The challenges listed below are largely common across industry sectors; however, each industry and enterprise will have some specific requirements and/or regulations to address. The following are main challenges for adopting cloud-based services for enterprises:

- Understanding any increased level of risk exposure resulting from the use of cloud services
- Ensuring the applications and data are secure in a potentially hostile environment
- Establishing mechanisms to detect and alert any potential security breaches, data loss, and/or exposure of intellectual property or personally identifiable information
- Reviewing and establishing service contracts and SLAs with service providers to address the lack of direct control an enterprise has over certain infrastructure security operations, and also clearly documenting roles and responsibilities of the service provider and the enterprise.

The security landscape has changed considerably in a new era of cloud-based services and solutions. There will always be a need to continually assess risk and be agile in appropriately adapting new cloud solutions. Enterprises that are adopting these services should keep the following points and recommendations in mind:

- Adjust for a changed and more industrialized threat landscape. Employ comprehensive and integrated approach to enterprise security and risk management.
- Conduct security threat analyses for all critical applications.
- Design in security from the beginning, especially when implementing public cloud usage.
- Be vigilant with continual compliance monitoring and audits, intrusion testing, and verifiable backups.

In summary, HP recommends that you:

- Establish a risk-based approach for assessing viability of cloud services.
- Design applications to run in the cloud.
- Implement ongoing auditing and management.
- Thoroughly assess infrastructure security mechanisms of cloud service providers during service sourcing.
- Innovate, as the cloud is fast-moving.

HP has capabilities to address all these issues. HP Labs is also working on leading-edge research in risk management and technology to address future problems, and is open to discuss this further.

About the authors

Ed Reynolds

Ed Reynolds, an HP Fellow, is a member of HP Enterprise Security Services, working on security strategy and architecture. As an HP Fellow, Reynolds helps develop enterprise-wide initiatives that shape the future of HP. He previously led the development of HP Enterprise Services' strategy for cloud computing services and has led similar strategies for Internet, utility computing, and grid computing services. He is presently a chief technologist for HP Enterprise Security Services, working on cloud security for enterprise use. Reynolds has more than 30 years of experience in information technology.

Mateen Greenway

Mateen Greenway, an HP Fellow, is the HP Enterprise Services chief technologist for the Europe, Middle East, and Africa (EMEA) Public Sector. In this role, he is responsible for overall strategy, technical direction, innovation, and leading the senior client-facing technical leaders and key account chief technologists in this major industry. As an HP Fellow, Greenway helps develop enterprise-wide initiatives that shape the future of HP. Previously, he was the chief technologist for the EMEA Manufacturing Industry. In addition, he was responsible for developing and delivering the global architecture training programs designed to grow the group of highly skilled architecture consultants to support high-profile bid engagement across all industries.

Get connected

hp.com/go/getconnected

Get the insider view on tech trends, alerts, and HP solutions for better business outcomes

Share with colleagues

4AA4-0150ENW, Created April 2012; Updated May 2012, Rev. 1