WHITE PAPER

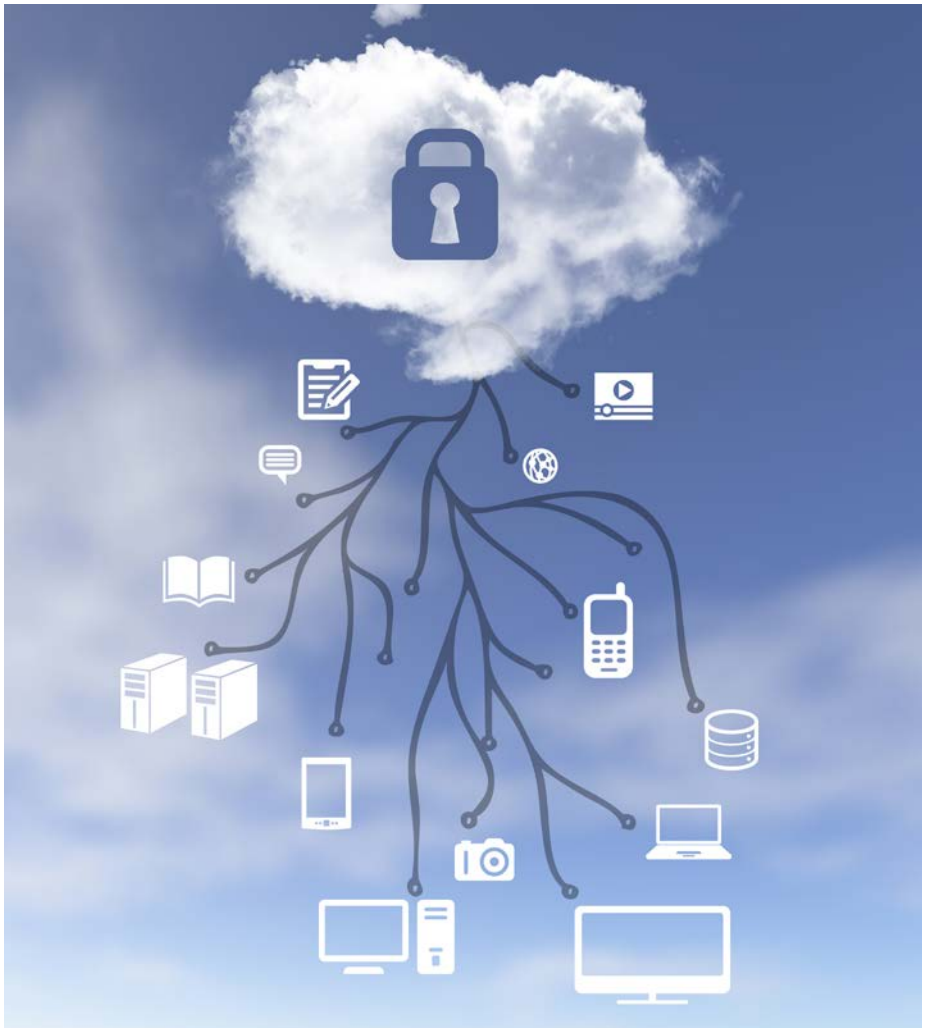
Overcoming the Security Challenges of the Cloud

Best Practices for Keeping Your Data and Your Organization Safe

we solve IT™ | PC Connection®

1.800.800.0014
www.pcconnection.com

THE cloud promises impressive gains in infrastructure agility, efficiency, and cost reduction, but the greatest barrier to cloud adoption continues to be security. In fact, a recent poll shows that 65% of organizations list security as their top concern.[1] PC Connection, in partnership with Cisco and Intel®, recently conducted a survey to learn how organizations are using the cloud, and the results are available on our website. In this white paper, you'll learn what you can do to mitigate concerns and make the most out of the cloud.



Trends Affecting Cloud Security

To manage cloud security in today's world, you need a solution that helps you address threats to your data and infrastructure, as well as the major challenges of cloud computing. These include:

- **Changing attackers and threats**—Attacks aren't coming just from isolated hackers now. More and more, organized crime is driving well-resourced, sophisticated, targeted attacks for financial gain.
- **Evolving architecture technologies**—With the growth of virtualization and rise in cloud adoption, perimeters and their controls within the data center are in flux, and data is no longer easily constrained or physically isolated and protected.
- **Consumerization of IT**—As mobile devices and technologies continue to become more common, employees want to use personally owned devices to access enterprise applications, data, and cloud services.
- **Dynamic and challenging regulatory environment**—Organizations and their IT departments face ongoing burdens of legal and regulatory compliance with increasingly prescriptive demands and high penalties for noncompliance or breaches. 90% of IT professionals are concerned about an inability to monitor governance and compliance.

Security Challenges and Risks

Moving to the cloud does present challenges and risks when it comes to securing your data and your infrastructure. The following are five of the most notable.

- **Abuse of Cloud Services:** Many Infrastructure as a Service (IaaS) providers make it easy to take advantage of their services. All you need to register and start using their cloud services is a credit card. Cybercriminals actively target cloud services providers, partially because of this relatively weak registration system that helps obscure identities, and because many providers have limited fraud-detection capabilities. Stringent initial registration and validation processes, credit card fraud monitoring, and subsequent authentication are ways to remediate this type of threat.
- **Shared Technology Issues:** Public clouds deliver scalable services that provide computing power for multiple tenants, who many not necessarily belong to the same organization. Dense virtualization can lead to multiple tenant data co-residing in the same hardware subsystems, from CPU subsystems to memory and storage. Even with a virtualization hypervisor to mediate access between guest operating systems and physical resources, there is concern that attackers can gain unauthorized access and control of your underlying platform with software-only isolation mechanisms. This is a key issue faced by

[1] 2013 Outlook on Technology—Cloud Computing Survey Results: http://www.pcconnection.com/~/media/PDFs/Brands/C/Cisco/Survey/25240_PCC_CloudSurvey.pdf

most IT organizations in achieving their virtualization goals—and subsequently in moving workloads to the cloud.

- **Data Loss:** Protecting data can be a headache because of the number of ways it can be compromised. Some data—customer, employee, or financial data, for example—should be protected from unauthorized users. But data can also be maliciously deleted, altered, or unlinked from its larger context. Loss of data can damage your company's brand and reputation, affect customer and employee trust, and have regulatory compliance or competitive consequences. In 2011, for example, 174 million records were compromised, costing organizations an average of $5.5 million—or $194 per compromised record.
- **Hijacking of Accounts or Services:** Attacks such as phishing and fraud continue to be an ongoing threat. With stolen credentials, hackers can access critical areas of your cloud and potentially eavesdrop on transactions, manipulate or falsify data, and redirect your clients to illegitimate sites. IT organizations can fight back with strong identity and access management, including two-factor authentication where possible, strong password requirements, and proactive monitoring for unauthorized activity.
- **Unknown Risk:** Releasing control of your data to a cloud service provider has important security ramifications. Without clearly understanding the service provider's security practices, your organization may be open to hidden vulnerabilities and risks. Also, the complexity of cloud environments may make it tempting for IT managers to cobble together security measures. Unfortunately, that same complexity and the relatively new concept of cloud computing and related technologies make it difficult to consider the full ramifications of any change, and you may be leaving your cloud open to new or still undiscovered vulnerabilities.

5 Steps for Building a Secure Cloud

Step 1: Plan

The best way to approach cloud security is to integrate it with your overall cloud planning early in the process. The idea is to understand your risk tolerance, identify the best deployment models for your specific needs based on security and compliance considerations, and detect potential exposure points for sensitive data and processes.

There are three primary cloud solutions: private, public, and hybrid.

Private clouds are resource pools run for a specific organization, controlled and managed by that organization (either with their own personnel/equipment or a third party's personnel/equipment). A private cloud might be a company's own data center, a fully managed and hosted off-premise environment, or some combination thereof. With a private

Cisco Unified Computing: A Winning Strategy for Your Data Center

Cisco UCS integrates industry-standard, x86-architecture blade and rack servers powered by intelligent Intel® Xeon® processors with networking and storage access into a unified system. The system is programmed through a model-based management interface to accelerate deployment and performance of applications in bare-metal, virtualized, and cloud-computing environments. A unified fabric supports network and storage I/O, while Cisco Fabric Extender Technology (FEX Technology) brings the network directly to servers and virtual machines for increased performance, security, and manageability.

Cisco UCS can be deployed incrementally, and each stage provides substantial business value:

- **Deploy virtualization-optimized server hardware, enabling server consolidation.** Cisco UCS eliminates redundant devices that populate traditional blade servers and add layers of management complexity.
- **Fully virtualize discrete network stacks across a common high-speed, low latency unified network fabric.** Cisco's unified fabric-based approach to data center infrastructure allows consolidation of LAN, SAN, and NAS over one high-performance and fault-tolerant network. It's based on the Cisco MDS 9000 Family and Cisco Nexus® Family of switches and integrated network services, which provide high-speed connectivity, high availability, security, and consistent quality of experience for data center applications. Cisco Network Services Manager enables dynamic, policy-based provisioning of network services.
- **Implement a centralized, policy-based management system, Cisco UCS Manager to manage all computing hardware and software components,** including legacy systems that will continue to exist across the data center, via its single pane of glass console.

One benefit of virtualization is the ability to abstract the hardware from the applications running on it, all the way down to the network interface. When a new server is added to the system, UCS Manager virtually eliminates manual configuration, automatically detects the new hardware and provisioning it according to pre-defined policies.

Whether you're just getting started with virtualization or you are planning a complete data center upgrade, the PC Connection family of companies can help. We are a Cisco Gold Partner and can offer you the highest possible level of support available.

Call today to learn more about Cisco solutions that offer a practical route to data center virtualization.

cloud implementation, since you own the infrastructure, security is under your own control. You establish security and compliance standards, as well as enforce and measure them.

Public clouds are built by a cloud provider, and organizations effectively rent compute capabilities in a shared environment controlled and managed by that provider. There are three main types of public clouds: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS has a neutral security posture when compared with security and regulatory concerns a customer may have with IaaS and PaaS. With potentially sensitive information passing through the hands of a third party, and with the highly fluid nature of multi-tenant environments, it can be difficult to know exactly where and how well secured your data is at all times. It may also be challenging for your organization to verify information security compliance.

In a PaaS environment, security and regulatory compliance may be a concern, as each provider delivers varying levels of control and auditability. Public and hybrid cloud environments may complicate regulatory compliance and data security, compared to fully private cloud environments that enable greater security control and auditability. More providers are finding ways to balance security and regulatory requirements with the extreme flexibility and elasticity that IaaS provides. While security continues to be an issue in the IaaS category, improvements will continue that enhance overall security. For example, division of data across tiers or encryption and obfuscation of data models when stored in a public tier can help address this challenge.

Hybrid clouds combine aspects of private and public clouds. For example, a company may host email in their own private cloud, but archive email in a provider's public cloud. Organizations who have moved to cloud or are in the process of implementing a cloud strategy are most likely to use a private cloud strategy. However, of the 39% likely to use a public cloud SaaS is the most popular choice. Not all public cloud solutions are created equal, nor do they have your risk tolerance incorporated into their plan, which makes planning your cloud strategy with a knowledgeable partner all the more critical.

Step 2: Protect Your Hardware and Infrastructure

A best practice for cloud implementation is to layer technologies to develop a strong security net that protects your data, applications and platforms, and network at all levels. This protection should start at the most basic level—the system hardware. With protection at the hardware level, you can build trust and compliance into your data center infrastructure and endpoint clients.

Cisco takes a "build-in security" approach to provide device, system, infrastructure, and services security, and is the basis of their development approach called the Cisco Secure Development Lifecycle (CSDL). Never before has the network been more relevant and ready to deliver a high-quality user experience with ample security and operational efficiency.

Application and access security must be integrated throughout the network to maintain a strong security posture. Security must be applied based on the context of the application, location, user, and device. Cisco Cloud Intelligent Network Solution includes pervasive, context-aware security features that allow granular controls over user access while maintaining a positive user experience, especially when users are mobile.

With the Cisco Cloud Intelligent Network, organizations can transparently connect users to all types of clouds—public, private, and hybrid.

The solution provides:

- An optimized experience that increases resource utilization and reliability
- Cloud security that protects business assets and meets compliance requirements
- Simplified operations for process efficiency, accelerated deployment, and lower costs

Cloud Computing: Discernment Is Our Differentiation:

We help you discern, design, and deliver the best cloud solutions for your business. There are no one-size-fits-all versions of any cloud technology when it comes to real-world applications. That's why we view cloud computing technologies as raw materials that you can combine in multiple ways to achieve your desired business outcomes.

Our 3 steps to cloud implementation:

- **Discern**—Assess requirements and technology options
- **Design**—Evaluate deployment scenarios
- **Deliver**—Execute the go-forward plan

How Do I Get Started?

Engage our cloud experts so we can assess your current environment and your specific business and IT drivers for considering cloud. We will help you determine which workloads are ideal for cloud enablement. If you have a specific goal in mind we can begin there, and our team will create a custom cloud solution roadmap for your organization. If you have a well-defined vision for your cloud project already, we can start there as well.

Put Our Cloud Expertise to Work for Your Organization

We bring a combination of unbiased expertise and best-in-class partners to our customers. As a technology company with 30 years of experience, we leverage our deep partnerships with industry veterans and born-in-the-cloud newcomers to deliver the right solution for your organization.

Contact an Account Manager today to get started.

Application and access security must be integrated throughout the network to maintain a strong security posture. Security must be applied based on the context of the application, location, user, and device. The Cisco Cloud Intelligent Network solution includes pervasive, context-aware security features that allow granular controls over user access while maintaining a positive user experience, especially when users are mobile.

Step 3: Secure Your Data

Of course, as you move workloads to the cloud, your priority is to keep your data out of the wrong hands. Here are three main targets to hit when you implement a data security plan.

Data Loss Protection: Data loss prevention (DLP) poses a serious issue for companies, as the number of incidents and the cost to businesses continues to increase. Whether it's intentionally malicious or inadvertent, data loss can diminish your organization's brand damage its goodwill and reputation. A solution for monitoring and enforcing data security across all communication channels is vital to ensure the integrity of an organization's policies. Get advanced risk management and increased data security with Cisco IronPort Data Loss Prevention.

Email Encryption: Despite the rise in text messaging, instant messaging, social networking, and other forms of communication, email continues to be the predominant business collaboration tool. The unsecured nature of email, however, has caused the inadvertent and malicious exposure of sensitive information. Cisco IronPort Email Encryption provides a solution that:

- Meets compliance requirements for email encryption
- Delivers powerful new email control features
- Is easy to use and broad reaching

Data Encryption: Encryption is an effective, well-established way to protect sensitive data. However, data encryption is often not used broadly due to the performance impact. It's possible to achieve security without compromising performance by using Intel® AES-NI, hardware acceleration for encryption/decryption, supported in the Intel® Xeon® E5 and E7 processor families.

Step 4: Plan for Compliance

With sophisticated threats and malware an ongoing and growing threat, securing both client and server platforms provides an additional enforcement point that builds trust between servers and between servers and clients.

The best way to enable a trusted foundation is to start with a hardware-based root of trust and extend the chain of trust through the critical controlling software layers, including firmware, BIOS, and hypervisor virtualization layers. A root of trust hardens the platform against attack and is extremely difficult to defeat or subvert. It substantially reduces the security risks of using a remote or virtualized infrastructure and enables a more secure platform for adding tenants and workloads, building protection into your hardware to better protect your software.

A root of trust helps ensure system integrity within each system. Integrity checking is considered a key capability for software, platform, and infrastructure security. Intel® Trusted Execution Technology (Intel TXT) checks hypervisor integrity at start-up by measuring the code of the hypervisor and comparing it to a known good value. Launch can be blocked or an untrusted launch event reported if the measurements do not match.

The root of trust enables a trusted foundation within your cloud environment so you can:

- Specify trusted server pools.
- Prove host software is good.
- Secure the server stack to ensure a trusted chain of protection.
- Respond quickly to attacks and minimize damage.

Intel® Trusted Execution Technology (Intel TXT) protects against malware, key stealth attacks, and other threats by:

- Establishing a hardware-based root of trust
- Providing a launch environment signature to enable trusted software launch and execution
- Providing the trust foundation so that policy engines can restrict or allow virtual machine (VM) and data migration based on platform security (trust) profiles
- Providing the trust foundation to enable environment monitoring for auditing function tied to a root of trust
- Enabling an IT manager to verify that the specific physical machine in the cloud is running the expected operating environment

Intel TXT technology is built into the Intel® Xeon® processor E5 and E7 family-based servers, including Cisco UCS.

Providing trusted cloud products and services are top priorities for Cisco. Cisco® SecureX is a context-aware security framework that meets your needs as you begin to implement a mobile, dynamic, and cloud-based working environment and allows 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. Core to SecureX is the Cisco® Security Intelligence Organization (SIO), a cloud-based security service offering a Web-based global network of shared resources, software, and information provided to Cisco customers and devices on demand. SIO is used for real time-insight into the global threat environment.

Step 5: Choose the Right Cloud Service Provider

Choosing a cloud service provider is complicated on many levels—from the cloud delivery model and architecture to specific applications. You'll have to ensure the security you need to protect your data and platform is part of the offering. While cloud service providers are becoming more aware of the need for transparency into their security practices, partnering with someone like the PC Connection family of companies can help take you through the entire process from discernment to deployment.