

CONFIDENT PURSUIT OF PAYOFFS TRUSTED CLOUD FOUNDATIONS IN SECURITY AND TRANSPARENCY



THE VIRTUAL COMPUTING ENVIRONMENT COMPANY (VCE)

Formed by Cisco and EMC with investments from VMware and Intel to deliver the Vblock™ platform.

Vblock platform combines network, compute, and storage assets in pre-configured and pre-tested combinations tailored for cloud workloads.

CSC selected the Vblock platform as the preferred technology stack for CSC Trusted Cloud to accelerate cloud technology deployment and concentrate on the business innovation of cloud processing for clients.

VMWARE ALLIANCE

CSC established a business alliance with VMware through the VMware vCloud® Datacenter Services Program.

CSC CloudCompute and BizCloud are offered as vCloud Datacenter Services.

AN INTRODUCTION TO THE TRUST FOUNDATIONS OF CSC TRUSTED CLOUD SERVICES

IT'S ALL ABOUT ENTERPRISE PAYOFFS

Nearly every survey on cloud use identifies “security” as a major obstacle to wider cloud adoption. This ranking by industry and government leaders has been a consistent survey result since the earliest network computing services first claimed the name “cloud computing” at the dawn of the 21st century. While most cloud providers claim to offer good security capabilities and reliable results, only CSC has based its entire cloud development and delivery program on the expanded power and payoff potential of “digital trust in the cloud” as first reported in CSC’s own research results in 2009 and 2010

The CSC trusted cloud initiative has been devoted to the preparation and delivery of cloud services that not only satisfy client value expectations for enterprise agility, flexibility and economy, but also offer new payoff possibilities by combining strong security with transparency services to generate trust and open up new possibilities for enterprise value. The creation of (multi-tenant) CloudCompute and (single-tenant) BizCloud™ offerings that combine the best of public and private cloud characteristics with strong security and transparency capabilities are all aimed at generating enterprise payoffs for cloud service consumers. The selection of technology partners with rich cloud technology portfolios [see sidebar] has given CSC the most solid cloud platform available, and allowed CSC to innovate cloud services that respond to “business first” and create new opportunities to capture cloud payoffs

MORE THAN TECHNOLOGY

The CSC equation for digital trust in the cloud requires both strong security and total transparency. These characteristics are each delivered with a foundation of technologies, techniques, process attention, and partner preparation.

¹ See Knode, Ronald, “Digital Trust in the Cloud”, August 2009, www.csc.com/security/insights/32270-digital-trust-in-the-cloud

¹ See Knode, Ronald with Egan, Douglas, “Digital Trust in the Cloud: Into the Cloud with CTP – A Precip for the CloudTrust Protocol, V2.0”, July 2010, <http://www.csc.com/cloud/insights/57785-into-the-cloud-with-ctp>

¹ See <http://www.csc.com/cloud> for information about CSC cloud services

**Security Service + Transparency Service =
Compliance and Trust \implies VALUE Captured**

- Delivering evidence-based confidence
- With compliance-supporting data and artifacts
- Using the best virtualization and cloud technologies
- Within ISO27001 certified delivery centers
- Operated by trained and certified staff and partners

3403-12-001

TECHNOLOGY FOUNDATIONS

Technology matters. CSC trusted cloud services are based on the VCE Vblock architecture. The VCE trusted multi-tenancy foundation is used as a starting point for security separation and assurance in a CSC Trusted Cloud, including all of the technical attributes provided by VCE. This technology foundation is further enhanced with supplemental features from VMware and the addition of Nimsoft for cloud service performance and capacity monitoring. This tightly integrated technology foundation provides the baseline for such important technical characteristics as:

- Separation by encryption through a VPN for all traffic entering and leaving the trusted cloud
- Use of VLANs within the cloud to separate and protect traffic and data
- Use of VMware vShield Edge, End Point, and App (along with ESX) to control communications and connections within the cloud with virtual firewalls and network intrusion monitors
- VMware Configuration Manager (VCM) to establish and maintain secure configurations
- Cisco UCS to separate management traffic from production application traffic on UCS blades; UCS also provides such secure communications capabilities as SSH Version 2 (TCP port 22), HTTPS (TCP port 443), and KVM management (TCP port 2068)
- Active cloud-to-cloud backup and restore options
- Available cloud-evolved versions of such traditional server security services as vulnerability assessment, audit log capture and monitoring, trusted configuration management and host intrusion detection using technologies from Symantec, McAfee, and RSA
- Available transparency services following the CSC/Cloud Security Alliance (CSA) CloudTrust Protocol (CTP)¹ to restore important security and control information that is typically lost when workloads are placed in a cloud. For example, information about current configuration, vulnerability status, location, access rights and history, compliance with agreed delivery standards, change management, and event logs and response are requested and returned via the CTP in a standard delivery model. Commitment to the full CTP distinguishes CSC cloud services as the leader in CSA standards conformance, and sets the pace for other cloud providers to deliver the same level of transparency in configuration, operation, and process

¹ For a complete description of the CloudTrust Protocol, see Knode, Ronald with Egan, Douglas, "Digital Trust in the Cloud: Into the Cloud with CTP – A Precipice for the CloudTrust Protocol, V2.0", July 2010, http://www.csc.com/cloud/insights/57785-into_the_cloud_with_ctp. On 30 April 2011 CSC licensed the CTP to the Cloud Security Alliance (CSA) and joined the CSA steering committee for cloud governance, risk, and compliance (GRC) management. Today, all CTP work is done under sponsorship of the CSA, and is targeted at the incorporation of the CTP as part of a standard GRC stack for all cloud providers.

- Available (soon) file and file system level encryption for data at rest to further separate and segregate data being processed in the CSC cloud

TECHNIQUES

How we use the technology matters. CSC trusted cloud services take advantage of valuable and productive circumstances and techniques associated with the foundation technology choices, from our own research and experimentation, and from the successful application of Trusted Cloud Services by CSC clients.

- VMware ESX 4.0 and 4.1, ESXi 4.0 and 4.1, and vCenter Server 4.0 and 4.1 have all achieved EAL 4+ certification under the Common Criteria (ISO/IEC 15408:2005)². CSC uses the configurations and claims described in the security target and certification reports to reap the benefit of independent 3rd party examination and verification of security claims. Moreover, with benefit of the alliance with VMware, CSC can also apply specific (advanced) configuration and operating recommendations directly from VMware, even beyond the public materials such as the “VMware vSphere Hardening Guide”³ and “Architecting a vCloud@, Ver 1.0”⁴ as well as help shape the direction of future releases of virtualization technology and support from VMware.
- VCE prepares shared internal advice for its member companies to take advantage of the specific product expertise from each contributor as hardware and software components are integrated together in Vblock configurations (e.g., Vblock Infrastructure Platforms Security Guidance, 17 Dec 2010). As an alliance partner with VCE, CSC enjoys special access to such internal advice and extends the results of that advice to the “business first” configurations and operations provided by CSC to users of Trusted Cloud Services.
- While *standardization* of configuration and delivery typically bring benefits of efficiency and leveraged assets to cloud service clients, an unyielding devotion to *orthodoxy* does not. So, following the “business first” approach for our Trusted Cloud Services, we adjusted and extended conventional Vblock configurations to capture payoffs against business needs. The addition of Nimsoft for monitoring along with other orchestration technologies, alterations in networking and storage configurations, and the creative application of security and transparency technologies from Symantec, McAfee, and RSA all are driven by “business first” needs.
- Each client use of Trusted Cloud Services contributes practical workload knowledge and experience in the practical application of cloud capabilities. Examples of compute intensive workloads, storage intensive workloads, workloads that surge both to and from the CSC Trusted Cloud, development and test practices, collaboration services, regulated applications and environments, and all manner of application transformation to cloud delivery have each added to the configuration and operation knowledge base that continues to improve the capacity of CSC’s Trusted Cloud to capture real business payoffs through cloud processing techniques.

PROCESS ATTENTION

Where and when we use the technology matters. Even clouds have to sit somewhere. And consumers of cloud services typically operate within a larger business context that uses cloud services, non-cloud services, and a host of process support activities that help keep the business on target and accountable. So process maturity and facility support are important to the quality and effectiveness of cloud service.

CSC Trusted Cloud Services are delivered from cloud delivery centers around the world. Every CSC cloud delivery center is qualified for service by linking with important associated service centers (e.g., service desk, security operations) and having its own compliance standing. For example, all CSC data centers from which Trusted Cloud services are delivered are subject to annual Statement on Auditing Standards (SAS) 70 Type II audits. [Note: As of 15 June 2011 these audits will conform to the new AICPA standard of SSAE 16.] The

² See the Common Criteria product portal at www.commoncriteriaportal.org/products/

³ See, for example, www.vmware.com/files/pdf/techpaper/VMware_vSphere_HardeningGuide_May10_EN.pdf

⁴ www.vmware.com/files/pdf/VMware-Architecting-vCloud-WP.pdf



control programs in place at these chosen locations are based on a COBIT framework. Upon request, relevant portions of that annual SAS70 (or its replacement standard) report are available to customers who are receiving service from those locations under the terms of a Non-Disclosure Agreement (NDA).

Furthermore, CSC has pledged itself to a number of quality and security standards. In particular, the ISO27001 standard that requires a formal Information Security Management System (ISMS) based on the practices recommended in ISO27002. Already, more than two dozen CSC delivery facilities are certified to the ISO27001 standard, with even more on the roadmap. By October 2011, five of the seven announced global cloud delivery centers will be ISO27001 certified (three are already certified), with the remaining two on track for certification in 2012.

Cloud Delivery Center	ISO27001 Status
Chicago, IL (U.S.)	✓ Certified
Newark, DE. (U.S.)	September 2011 certification audit
Maidstone, U.K. (EMEA)	✓ Certified
Copenhagen, Denmark (EMEA)	✓ Certified
Sydney, AU (APAC)	October 2011 certification audit
Melbourne, AU (APAC)	2012 certification audit
Luxembourg (EMEA)	2012 certification audit

STAFF AND PARTNER PREPARATION

Who administers and operates the technology matters. The CSC Trusted Cloud operating model introduces service support roles and actions for both risk management and compliance issues. Building on the successful Information Risk Management Program (IRMP) model, CSC Trusted Cloud Services offers (optional) Cloud Trust Agent (CTA) operational support to the traditional Lead Information Risk Manager (LIRM) service role as a way to accelerate and improve client access to security and compliance evidence through transparency and security services. The LIRM role continues to concentrate on information risk protection and data preservation. CSC security staff are incentivized to achieve security professionalizations. Service roles targeted for information risk management are obliged to seek Certified Information System Security Professional (CISSP) certification, while compliance-oriented roles are directed at one or more ISACA (CoBIT-related) certifications.

Certified Information Systems Auditor (CISA)	Certified Information Security Manager (CISM)
Certified in the Governance of Enterprise IT (CGEIT)	Certified in Risk and Information Systems Control (CRISC)
CoBIT Foundation Certificate	

CONCENTRATE ON PAYOFFS:

Security and compliance needs and capabilities are important. But, the key to enterprise success in cloud processing is to concentrate on capturing and sustaining enterprise payoffs, while avoiding unnecessary increases in information risk. CSC Trusted Cloud services free clients to focus on enterprise payoffs by solving the equation for digital trust in the cloud. A strong technical, process, and operating foundation combined with healthy inventories of traditional security and innovative transparency services allow Trusted Cloud Service clients to establish and monitor the information control structures they need to satisfy compliance mandates. Moreover, all of these capabilities can be wrapped into standard service catalogue items that become the basis for normal configurations and operations. The service catalogue can then be used by clients to keep workload configurations attached to the right security and compliance services.

Such an approach lets CSC Trusted Cloud Services operate as a compliance partner for clients. As the data and applications owner, clients retain the official regulatory obligation. For example, supported by both cloud processing and conventional data center processing, it will ultimately be the client enterprise that achieves compliance for its operations against such regulations as the Health Insurance Portability and Accountability Act

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.

(HIPAA), the European Union Data Protection Directives, the Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes-Oxley (SOX).

The CSC Trusted Cloud provides a variety of capabilities and options for data storage and movement that support regulatory and compliance needs across a variety of compliance jurisdictions. Depending on the level of service selected, clients can request a Trusted Cloud Service that includes multiple data protection and compliance options.

- Anchoring client data within a certain cloud delivery center geography – supporting geographic obligations on data, e.g., for International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), or EU Data Protection Directives.
- Backing up client data with more copies (for resiliency and availability) or fewer locations to avoid violating geographic boundary restrictions.
- Specifying a separation of (physical or virtual) platforms for storage and processing (e.g., DBMS service versus application service) to comply, for example, with platform isolation requirements such as those described under the Payment Card Industry Data Security Standard (PCI DSS). (Note: This characteristic is also referred to as “platform anchoring.”)
- Keeping de-duping at the block level. (Note: This characteristic is also referred to as “process anchoring.”)

In addition to these example data compliance options, the CSC Trusted Cloud services also provide compliance supporting information through the CloudTrust Protocol (CTP) regarding the Trusted Cloud services architecture, configuration, access control, and operation. So, even though CSC Trusted Cloud services themselves advertise no complete certification or evaluation against any regulation, federal or otherwise, the CSC Trusted Cloud does offer a host of compliance support services and capabilities that respond to multiple compliance and regulatory mandates.

CSC is routinely requested by clients to provide data in support of compliance for such standards as SOX, PCI DSS, HIPAA, ITAR, National Institute of Standards and Technology (NIST) 800-53, Federal Information Security Management Act (FISMA), and the Gramm-Leach-Bliley Act (GLBA) as well as the client’s own SAS 70 needs. The security/trust, compliance, and transparency capabilities in the CSC Trusted Cloud provide the means by which CSC can respond to clients’ compliance data requests, no matter how those needs evolve.

The CSC solution to the equation for digital trust in the cloud lets clients *pursue payoffs with confidence* that control and compliance actions and evidence are well in place.