shelbysystems

Azure Datacenter Overview

Product Overview and Data Sheet

DOCUMENT CONTROL

DOCUMENT INFORMATION

Title	Shelby Systems Azure Datacenter Overview
Revision	1.0
Issue Date	November 14, 2016
Filename	Shelby Systems Data Center Security Revision.docx

DOCUMENT HISTORY

Version Number	Date	Responsible Individual	Summary of Change
1.0	November 14,2016	J. Litton	Initial standards document

DOCUMENT REVISION

This document will be reviewed and updated on an annual basis and, if necessary, as required to correct or enhance information content and following any organizational changes or restructuring.

Product Data Sheet

Maintaining a Software as a Service (SaaS) environment with market leading availability and security is something that Shelby Systems considers a core strength, and it's what sets us apart from the competition. Our commitment is to consistently maintain a state-of-the-art data center and application infrastructure that is supported by a team of highly skilled, highly trained, technology professionals to keep your data "always on", safe, and secure.

This document is intended to provide an overview into the various capabilities of our hosted SaaS product. Areas of focus are:

Datacenter	Datacenter
Security	Physical Security Network Security Data Security Testing PCI Compliance
Operations	Monitoring and Response Data Protection (Backups)
Product Design	Redundancy
SLAs	SLA

Data Center Overview

Shelby Systems has partnered with Microsoft Azure as our primary provider of Infrastructure as a Service and Platform as an International Service vendor.

Datacenter Capabilities

Microsoft Azure datacenters are designed to meet ISO/IEC 27001/27018, SOC 1, SOC 2, CSA, PCI DSS, HIPPA, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS.

Our primary datacenter is designed to meet the Uptime Institute's Tier IV datacenter standards and incorporates multiple active power and cooling distribution paths, has redundant components, and is fault tolerant; providing 99.95% availability of those functions. Power availability is enabled by a facility-wide uninterruptable power supply (UPS) and on-site generators. In the event of any local/regional blackouts or disaster, the datacenter would continue to provide uninterrupted power to systems for several days without refueling of the generators. Cooling at Switch is a patented; state-of-the-art system that completely separates cold and hot air flows. This proprietary design allows for highly dense computing environments that many other datacenters cannot support.

Security

Physical Security

Windows Azure is designed to have all system maintenance and incident handling be remote from our datacenters except for hardware maintenance. This allows us to lock down access to the hardware to a minimum number of staff, and allows us to configure the hardware without any on-site privileged access based on physical proximity. Windows Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24 x 7 x 365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability and they are managed, monitored, and administered by Microsoft operations personnel. Further details of Windows Azure's physical security are discussed below.

Facilities Access

Microsoft uses industry-standard access mechanisms to protect Windows Azure's physical infrastructure and datacenter facilities. Access is limited to only the required number of operations personnel. Datacenter access, and the authority to approve datacenter access, is controlled by Microsoft operations personnel in alignment with datacenter security practices and audited in accordance with established frameworks such as SOC 3. Data in Windows Azure is stored in Microsoft datacenters around the world based on the geo-location properties specified by the customer using the Windows Azure Portal. This provides a convenient way to minimize compliance risk by actively selecting the geographic locations in which regulated data will reside.

Network Security

Digital traffic into and out of the facility goes through multiple layers of firewall and denial-of-service hardware based protection using best-in-class equipment from manufacturers.

All network communication to the Azure Network environments is via SSL cryptographic protocol. This ensures that information is secured at the transport layer, end-to-end, using 256-bit encryption keys. Application and data servers for each of our environments reside in its own segmented network separated from network access by a DMZ that is protected. Our team of CISSP certified professionals uses a comprehensive suite of software and hardware tools to inspect network activity, watching for and protecting against any external threats.

Data Security

All customer account information is encrypted in the database and strong passwords are enforced by the application interface. Data access is only allowed through specific service accounts that have server and process specific permissions. The entire operating system layer security is protected by the extended symmetric key cryptography, developed by MIT, built into Microsoft's Active Directory security architecture.

Our integrated application security architecture prevents anyone but the customer from accessing their data. This security model is reapplied with every request and enforced for the entire duration of a user session.

Systems Security

Our information security team is constantly apprised of new vulnerabilities from our technology vendors and security forums. We additionally utilize frequent scans of our infrastructure to detect and notify of potential risks in our environment. Upon discovery new risks are ranked in accordance to the National Vulnerability Database Common Vulnerability Scoring System. Remediation is prioritized according to the risk and can be fully tested and deployed within a matter of days if needed.

Anti-virus software is utilized on all company computers and servers and managed via a central management console that continually keeps the software and virus definitions up to date.

Testing

Our products are regularly tested from the Internet for vulnerabilities with industry leading audit review and penetration testing expert Sword & Shield®. They test our sites to ensure we pass the highest published payment industry and government standards. Sword & Shield ® Secure certification is fully accredited to meet the scanning requirements for the Payment Card Industry (PCI) standard used by Visa, MasterCard, American Express, and other consumer credit providers.

Shelby Systems also conducts internal vulnerability scans to identify potential areas of risk and drive remediation on an ongoing basis independent of our external scans.

Last Updated 11/14/2016

PCI Compliance

In addition to the many different security measures we take, we are required to participate in Visa's Payment Card Industry (PCI) data security standards compliance audit and hold a current Level 1 Payment Processor Certification for all our payment processing. The PCI standards cover everything from network security, to application security, to background screening of our employees. For further information on our FDC payment service please refer to the document FDC *Data Sheet.*

Operations

Monitoring and Response

All systems that are required for supporting the application and services are fully monitored by a suite of tools. We perform monitoring, alerting and notification on multiple tiers of the technology architecture.

Core Infrastructure Monitoring

Our entire technology stack, which includes Storage, Network and Computers are monitored 24x7. System metrics such as CPU, memory, disk space and services are continually monitored to ensure that they are operating within the defined ranges. When certain thresholds are reached or exceeded our monitoring systems notify IT professionals to take action.

Customer Experience Monitoring

We also monitor for many aspects of the customer experience. To do so, we implement a separate 3rd party service that continuously tests our web facing products for key functions from a variety of geographic locations, beyond our own data centers. Should error conditions occur in any of our monitoring tools, alerts are immediately forwarded to engineering staff for investigation and resolution.

Data Backup

Critical customer data contained in the database is backed up on a regular basis, differential backups performed nightly and full backups weekly. We utilize an online form of backup storage vs. tapes, restoration of data, should it be required, can be done in near real time vs. the hours or days it may take to recover from tape based media.

Disaster Recovery

By default, Shelby Systems continuously replicates the critical data for all of its products to a secondary, stand-by disaster recovery site. In the event of a condition such as a regional disaster that would prevent recovery of services within the primary datacenter for 3 days or more, recovery operations in the secondary datacenter could begin. Contact your service delivery manager for which products have live disaster recovery capabilities today.

Product Design

Redundancy

All systems associated to hosted products are part of fully redundant pools of devices. This means that the loss of a single web server or network device, for example, would not impact functionality and the majority of device failures would be completely transparent to the user. In many cases multiple devices could be lost or removed from service to perform maintenance activities without user disruption. Load balancers are utilized to spread customer load across web and application servers and continuously optimize end-user performance and availability. The critical database tier is also part of a clustered pair enabling maintenance activities as well as failure recovery with a minimum of customer interruption.

Power Redundancy and Failover
Each Azure datacenter facility has a minimum of two sources of electrical power, including a power generation capability for extended off-grid operation. Environmental controls are self-contained and remain operational as long as the facility and contained systems remain online.
Physical security controls are designed to “fail secure” during power outages or other environmental incidents. In case of fire or situations that could threaten life safety, the facilities are designed to allow egress with appropriate alarming and security measures.

Service Level Agreements (SLAs)

Hours of Operations	7/24/365
Scheduled Maintenance Window	Depends on hosted product
Datacenter Uptime Objective	99.95%
Hosted Product Uptime Objective	99.9%