



Security Overview Technology Infrastructure

DATA SECURITY

Protecting the integrity of Affirmative’s network and the privacy of sensitive data is of utmost importance. Security is essential when extending business processes to applications hosted on the Internet, especially when these applications are used for the purposes of processing electronic payment transactions.

Affirmative Technologies has engaged SAVVIS as its’ hosting provider and is proud to be associated with the #1 market shareholder in the data hosting segment.

Affirmative Technologies’ CTO says, “SAVVIS was a natural choice based on their heritage in the financial services industry and their global network and hosting infrastructure that many of our partners, customers and prospects already use. Given their understanding of both large and small financial institutions, SAVVIS worked with us to develop a turn-key, fully managed solution that leverages the expertise and core competencies of our company.”

TRUSTED HOSTING PROVIDER

SAVVIS, Inc. (NASDAQ: SVVS) is a global IT utility services provider that focuses exclusively on IT solutions for businesses. With an IT services platform that extends to 45 countries, SAVVIS has over 4,000 enterprise customers, including more than 1,500 financial institutions, and leads the industry in delivering secure, reliable, and scalable hosting platform. These solutions enable customers to focus on their core business objectives while SAVVIS ensures the quality of their IT systems and operations. SAVVIS’ strategic approach combines resilient virtualization technology, a global network of data centers, and automated management and provisioning systems. For more information about SAVVIS, visit www.savvis.net

SECURITY FROM THE GROUND UP

SAVVIS’ security legacy dates back to 1987, with the formation of the Common Criteria Test Lab (CCTL). As such, more than 50 credentialed

security professionals now provide services to its customers, keeping abreast of potential threats, and interfacing with global law enforcement officials. Security is a core competency of the SAVVIS organization, permitting Affirmative to focus on their core competencies involving ACH payment and processing software. Affirmative builds on this secure infrastructure by using an ASP model designed expressly to ensure robust and secure operations while integrating seamlessly with Affirmative’s existing network and security infrastructure.

SECURE FACILITY

Affirmative’s Web, application, communication and database servers are hosted in a highly secured data center. Physical access to servers is restricted. The entire site sits in a locked facility cage that is monitored by SAVVIS security personnel and is protected by multiple layers of strict physical and procedural security measures.

SECURE NETWORK

Affirmative Technologies leverages SAVVIS’ network security infrastructure to deliver its clients a highly flexible and secure solution.

SAVVIS access routers are configured to watch for denial of service (DoS) attacks and to log denied connections. Multi-layer perimeter security is provided by a pair of firewalls: one between the Internet and Web servers, another that filters communications from the web and application servers to back-end databases. The security of this architecture has been independently confirmed by penetration tests and vulnerability assessments conducted by several reputable ethical hack teams. Quarterly perimeter tests ensure that Affirmative continues to adapt as new IT threats emerge and security solutions evolve over time.

ATI servers run on hardened a Windows Enterprise platform with the latest security patches installed. Servers are periodically penetration tested, and system logs are continuously audited for suspicious activity. Technology refreshes are performed periodically



to ensure top of the line performance and industry standard security.

SECURE ADMINISTRATION

Affirmative servers are administered over private links from SAVVIS and Affirmative's Network Operating Center; utilizing secure communications and procedural protocols, thereby avoiding open ports, unencrypted protocols and ensuring very tight access controls.

SCALABLE/RELIABLE INFRASTRUCTURE

The SAVVIS infrastructure is both robust and secure. Redundant routers, switches, server blade clusters, SAN and a centralized backup system are used to ensure high availability. For scalability and reliability, switches and (optional) web load balancers transparently distribute incoming requests among Affirmative Web, database and application servers.

PROTECTING CUSTOMER PRIVACY

SAVVIS understands that all enterprises that outsource service delivery are concerned about privacy. SAVVIS enforces a strong privacy policy that prohibits unauthorized disclosure of personal or information to any third party.

PRIVACY POLICY

For additional information, please review SAVVIS published privacy policy at <http://www4.savvis.net/corp/Legal+Notices/Privacy+Policy/>. The following information is included in every Affirmative service agreement. This policy identifies the information gathered, how it is used, with whom it is shared and the customer's ability to control the dissemination of information.

CUSTOMER INFORMATION

To deliver service, Affirmative Technologies must collect certain user information, including first/last name, email address and account-level passwords

Security Overview Technology Infrastructure

required by Affirmative applications. Unless expressly authorized, Affirmative will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. With its users' express consent, Affirmative sends service update messages to its users at the email addresses they provided when requesting the service.

Even when Affirmative services are accessed from a public PC, data left behind poses no privacy threat. Affirmative utilizes 128 bit SSL encryption protocols in combination with secure expiring cookies to secure web session information. The cookies used are unique for each session and contains no personally identifiable information or passwords.

ACCESS TO CUSTOMER INFORMATION

SAVVIS' Network Operating staffs are the only individuals with physical access to Affirmative's production environment and are granted such access on a need-to-know basis for the express purpose of supporting authorized Affirmative staff. SAVVIS and Affirmative's developers do not have access to production servers.

Application session logs are used by Affirmative to maintain quality of service, assist in performance analysis and perform intrusion detection. Information derived from these logs is never disclosed to anyone outside Affirmative and is used strictly to ensure its clients the highest level of performance and security.

SECURITY POLICY ADMINISTRATION

Affirmative provides a secure online Administration Center from which administrators can control the employees who are permitted application access and can block unauthorized access or features

SECURE MANAGEMENT INTERFACE

The Administration Center is accessible from any Web browser. Once an organization establishes an Affirmative account, the administrator is



Security Overview Technology Infrastructure

provided with access instructions. A top-level administrator can grant access to a second tier of plan administrators to facilitate large Affirmative deployments. All Web-site connections are protected using SSL with a minimum of 128-bit symmetric encryption and a 1024-bit authenticated key agreement. If the browser does not support a strong cipher suite, the user will be redirected to a page that explains how to upgrade the browser. The Affirmative server is authenticated with an X.509 digital certificate

MANAGING USER ACCOUNTS

Affirmative administrators can configure user account parameters to meet organizational needs, implement security policies and support privacy mandates. Administrators can limit access by users or groups to specific application features based on service and user business roll. Administrators can also enforce password update frequency and reuse policies, limit time-out periods, lock accounts and computers after authentication failure and mandate length and complexity level of passwords. Controls are also available to temporarily suspend or permanently cancel any user or group account. Fine control over these settings allows administrators to match security policies, and customizable multi-level groups enable enterprise-wide policy enforcement and rapid update, even in very large deployments.

PROTECTING CONFIDENTIAL DATA

Affirmative uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. Backups and file transfers are encrypted in 256-bit AES encryption storage and 128-bit browser AES transmission protocol.

ADVANCED ENCRYPTION

Affirmative uses 128-bit Advanced Encryption Standard (AES) in Counter Mode (CTR). In early 2001, after an extensive four-year evaluation process, the National Institute of Standards and Technology (NIST) selected AES as a successor to

DES. Originally known as Rijndael, AES was selected because of its computational efficiency, modest memory requirements, flexibility, simplicity, and, of course, security. AES is now the U.S. government's designated cipher for protecting sensitive information. Through industry-standard encryption methods, Affirmative can help an organization comply with strong security policies and conform to such privacy mandates as the Health Insurance Portability and Accountability Act (HIPAA).

STRONG PASSWORDS

Affirmative requires that every password be at least eight characters long and contain both letters and numbers. This requirement helps to prevent accounts from being configured with short, common passwords that are easily compromised with a dictionary attack. The longer and more complex the password is, the stronger the protection. With Affirmative, administrators can set password expiration and update and reuse rules to align with the existing password policies. As noted in the End-to-End Authentication section, passwords can also be combined with other stronger authentication methods.

LIMITED LOG-IN ATTEMPTS

Affirmative limits the number of times any user can attempt to log in sequentially. This measure also helps to protect against password-guessing attacks. By default, after five authentication failures, access to the user's account and computer are temporarily deactivated for fifteen minutes. With Affirmative, administrators can match existing security policies by customizing the lockout period and enabling hard lockout after a consecutive number of incorrect password entries. Optional reports allow management to view Affirmative usage and account information

MULTIPLE PASSWORDS

Affirmative uses multi-factor authentication. In addition, sensitive data is always stored in an encrypted format when at rest. Cryptographic



Security Overview Technology Infrastructure

techniques are used to ensure that transmission of sensitive data remains secure. The Affirmative web applications authenticate to browser clients by supplying a digital certificate, issued by a trusted authority. Clients authenticate themselves to the Affirmative web applications by supplying a combination of an account login/password, biometric signature, pin pad or RSA that is exchanged over SSL.

INACTIVITY TIME-OUTS

Users walk away from public PCs without logging out and leave home PCs unattended. Affirmative addresses these threats by applying inactivity time-outs. Users are automatically logged out of the Affirmative Web site if their SSL connection is inactive for several minutes. Affirmative enables its clients to configure these security features based on the mandates of their internal security policy – for example, setting a maximum time-out or preventing user modification.

MONITORING USAGE

Affirmative administrators can view connections for any given day, including those that are still active. Administrators can also use this tool to end active connections immediately if necessary. Each connection record displays details such as the name of the host PC, the IP address of the client initiating the connection, the connection start and stop time, and the connection duration.

Administrators can also generate additional reports to evaluate data such as enabled users, the features enabled for each user/group, last log-in time or the frequency of failed log-in attempts.

These standard reports can be analyzed to spot unusual access patterns, including exceptionally long connections and unexpected client IP addresses. They also serve as audit trails, making it possible to check to see who accessed a particular computer at a particular time.

ACCESS NOTIFICATIONS

Upon each browser client login, the user is always notified of his or her last log-in attempt and last successful login time. If there were unsuccessful login attempts since the last successful login an alert is displayed to the client that failed login attempts occurred against his or her username. This notification reassures the user that no unauthorized access has taken place during the interim. In addition, users can view reports that detail their own connection histories, including the number of failed log-in attempts, login times and login durations; to confirm that there has been no suspicious activity.

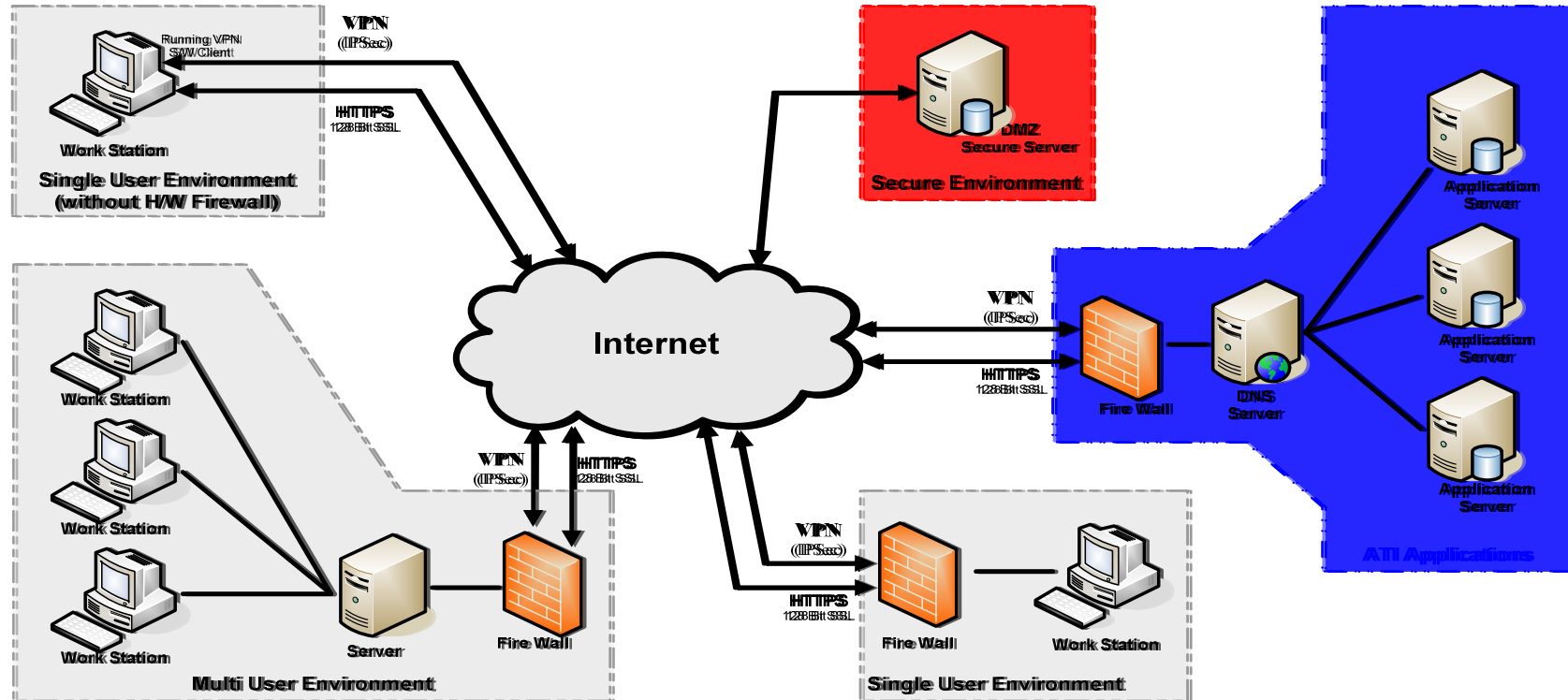
HOSTED ASP SOLUTION

Affirmative's ASP model is straightforward: Start with a secure hosted service and operational practices that preserve customer privacy. Complement this foundation with secure enterprise-class configuration and monitoring tools to control application access. Protect session connections with multi-level authentication and state-of-the-art encryption to keep traffic safe. Integrate this solution seamlessly with each company's existing network and security infrastructure. Provide flexible administrative controls to support and enforce a wide variety of security policies and hierarchical grouping to enable scalable management.

TECHNOLOGY BACKBONE

Affirmative applications are hosted on high availability blade servers, featuring secure --modern data centers in prime locations; enterprise class servers and storage platforms; within a fully managed network. This environment utilizes the latest hardware including hot swappable servers, the largest available processors including Multiple 64 Bit Quad Core Xeon Processors, broad Storage Area Network Systems scalable to 3T and Microsoft Enterprise Server 2003.

Affirmative's Data Communications Security



Definitions

- * VPN = Virtual Private Network
- * IKE = Internet Key Exchange
- * IPsec = IP Security
- * DES = Data Encryption Standard
- * 3DES = Triple Data Encryption Std
- * MD5 = Message Digest Algorithm
- * SSL = Secure Socket Layer
- * HTTPS = Hyper Text Transfer Protocol
- * HTTPS = Secure HTTP

Secure Connection Details

- * All VPN Connections are DES (56 Bit), 3DES (168 Bit), or MD5 (128 Bit)
- * All VPN Connections support AES (128 or 256 Bit)
- * IPsec is IKE using shared secret
- * Supports Diffie-Hellman Key agreement protocol

Name: **ATI Data Security**

Revision: **C**

Date: **11/02/04**

Copyright 2000-2004 Affirmative Technologies, Inc. All Rights Reserved

Affirmative Technologies Inc. 35111 U.S. HWY. 19 N. Suite 200, Palm Harbor, FL 34684-1907