NOWELL
DEVELOPMENT
Application software
& services

Shalom ESX Platform v5.0

Integrated Risk Software Platform

NOWELL
DEVELOPMENT
Application software
& services

Executive Summary: Cloud Integrated Risk Security Platform

Shalom ESX Platform, software that helps manage the security issues and risks associated with cloud computing and hosted application services. Specifically Shalom ESX addresses:

- Insider Risks and Vulnerabilities
- Identity Fraud

Shalom ESX Platform looks out for suspicious, "high-risk", activity by computer users, which is always a key indicator of a possible insider security breach [Anomaly Detection]. If a user exhibits suspicious behavior, they are authenticated for identity verification. Shalom ESX can be configured to only monitor for suspicious insider activity providing reports to serve as an effective starting point for internal audit.

With Shalom ESX, identity fraud is better detected and prevented. Shalom also helps meet regulations outlined by FFIEC InfoSec, Sarbanes-Oxley, Gramm Leach Bliley, VISA-CISP, PCI-DSS, HIPAA and others. The software promotes a safer and more secure internet experience while complimenting the identity and access management strategies of enterprise applications, mitigating complex risks associated with moving enterprise workloads to cloud hosted models

NOWELL
DEVELOPMENT
Application software
& services

The Problem: What Is the Insider Risk & Identity Fraud?

The Insider Risk refers to when internal associates of an organization use their access to information for the wrong reasons. It also refers to identity fraud, when someone's identity or account is stolen. Insider risks are very damaging because the internal user has detailed insider knowledge about their organization, and they are many times trusted by their employers. Since the internal employee is granted such liberty to carry out their jobs, financial theft by fraudulent internals often results in financial losses that are very great.

For example, in financial sectors, we've seen in some cases internals try to steal money or transfer funds from finance accounts using methods specific to their organization. Other times, internals steal sensitive customer information and later use it for fraudulent purposes like Identity Theft. Internals may also choose to steal and divulge sensitive intellectual property, classified information or trade secrets to unauthorized 3rd parties for profit. In other cases outside hackers crack into a system and gain access

Retail Industry statistics suggest that financial loss from internal theft and fraud is majority: 43% of losses from retailers are caused by theft from fraudulent insiders[1]. External financial theft by outsiders results in 35%. This shows that losses from insider risks in many organizations are very significant[2].

Javelin Strategies estimates identity theft losses at $54 billion per year. The Association of Certified Fraud Examiners estimates fraud losses average at about USD $175,000 per fraud incident. Total occupational fraud stands at $994 billion per year.

Identity Theft or Identity Fraud is another big security problem facing organizations. Often thieves or computer hackers steal user logon information in order to gain access to computer systems. Hacker thieves steal user ID's, user names, smart card PIN#'S, and computer passwords in order to log into computer systems using stolen computer identities. Once logged in, the thief is under disguise, impersonating a legitimate user.

Shalom ESX Platform helps to enhance the internal security posture of organizations. It helps to detect fraudulent insiders and intruders using stolen identities. Shalom detects suspicious or fraudulent user behavior inside computer systems. Security services like Shalom help organizations reduce theft, fraud, and misuse of information systems by internals. When security is enhanced, trust develops among business partners allowing seamless collaboration, teamwork and the assumption of shared risk and accountability. Also with the explosion of internet social media, identity fraud is becoming a personal issue, because ID thieves "hijack" identities of real people for exploitation, misrepresentation or wrongful gain

[1] Source: National Retail Security Survey 2009; Note that total 2009 retail shrinkage losses are at $33.5 billion which is 1.44% of total retail sales for 2009;Of this amount lost, $14.4 billion is lost from internal theft and fraud in the retail sector like grocery stores, warehouses, and multi-department retail stores

[2] CSI security survey revealed that over 70% of network abuse is caused by insiders

NOWELL
DEVELOPMENT
Application software
& services

Dr. Peter Stephenson, Chief Technology Editor, SC Magazine Review: “"it can be a significant arrow in the insider threat protection quiver"

CRN Test Center – “the product does accomplish its primary goal—containing the insider threat. Also, those driven by compliance needs will find both the security capabilities and reporting information key elements to building compliant information services—that alone may be worth the price of entry.”

Mr. Earl Greer, Federal Computer Week Review “"… adds significant protection against insider threats, and it aids in complying with security regulations"

Containing Insider Risks, and Identity Fraud

Suspicious behavior by authorized users is an indicator of internal security breaches. Malicious internals within an organization tend to exhibit very suspicious, unusual behavior on computer systems that. raises red flags Also, identity fraudster behavior differs very much from the real, authentic user. For example, if a user is accessing information that he does not need to know about, that is an example of suspicious or anomalous behavior. Shalom has the ability to detect such unusual anomalies in user and host behavior and sees such deviations as *suspicious.* The software uses multifactor authentication and risk analytics to track suspicious behavior.

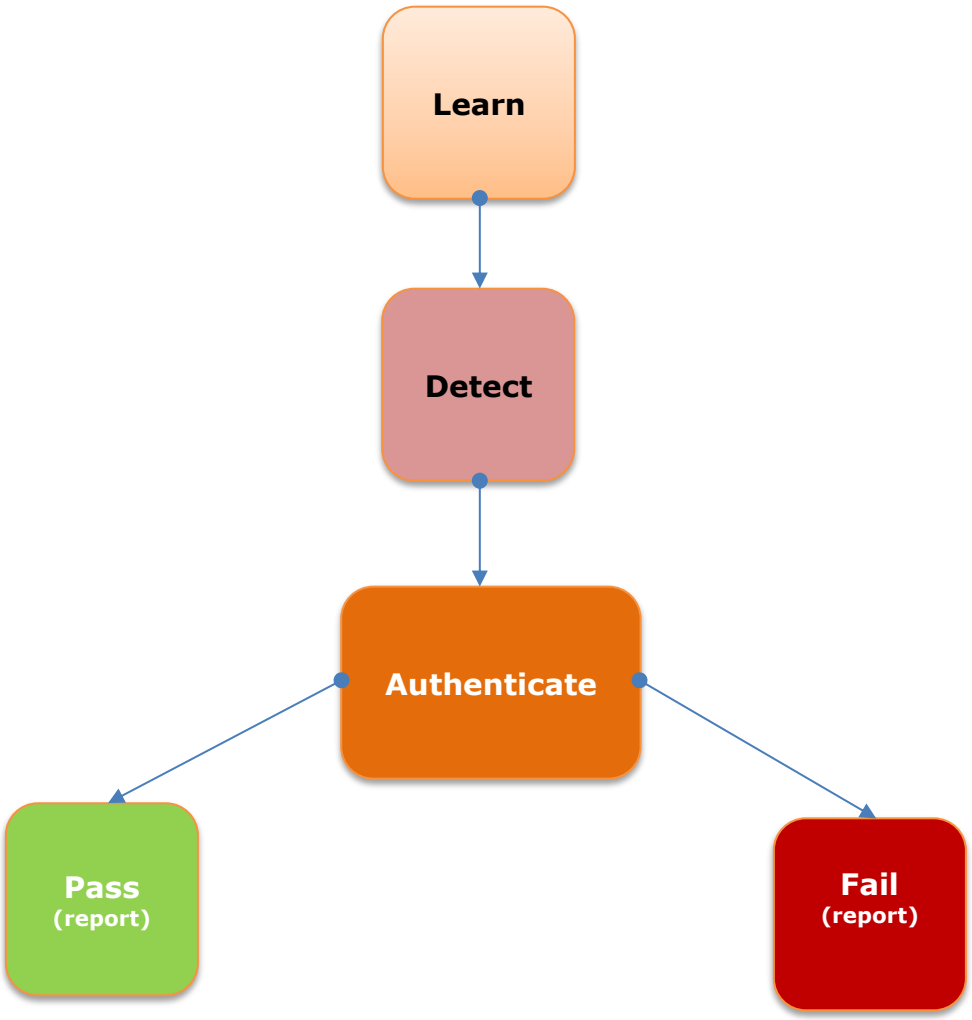
Shalom ESX risk software is installed on each host on the network, with a hosted server that resides in the cloud[3] that helps manage the software. The security platform is offered as a secure service over the internet for ease of deployment, reduced costs, less complexity, security, and in support of globally interconnected and distributed information systems.

Shalom ESX briefly interviews each user once, collecting personal information for later authentication. Next, it continuously learns computer behavior patterns for each user in the network. After a time period[4], each time a user logs on, Shalom looks out for suspicious behavior— behavior that is very different from how the user normally behaves[5]. If the Shalom service detects very suspicious behavior by a user, it reports and authenticates the user by presenting challenge questions. The user will be asked to answer the questions in order to authenticate successfully[6]. All events of interest are reported to the cloud server and accessible via the Shalom Administrator's management interface. Optionally, the system can be configured to only report suspicious insider activity without any question authentication

[3]Cloud here refers to the general internet – it could be a private, hybrid or public cloud. Nowell offers a comprehensive service in which Nowell can host the server and server software at a partners site. Other customers may choose to host the server component within their own infrastructure.
[4] Initial monitoring lasts for about a week (40 hrs.), but never stops.
[5] Risk monitoring and authentication has been used for several years internally by banks and credit institutions to identify potentially fraudulent transactions, credit applications, and wire transfers. This concept is not really new, it is slowly making its way into the general cloud computing domain
[6] If the person passes the authentication, everything is okay, however if the person fails, this could mean a compromised situation. In any case the administrators are notified of the pass or fail. Optionally, for stronger prevention, the user could be prevented access if they fail to successfully authenticate, although this is not the default behavior. The default behavior is to detect and report only - in order to minimize disruption of normal system activities

NOWELL
DEVELOPMENT
Application software
& services

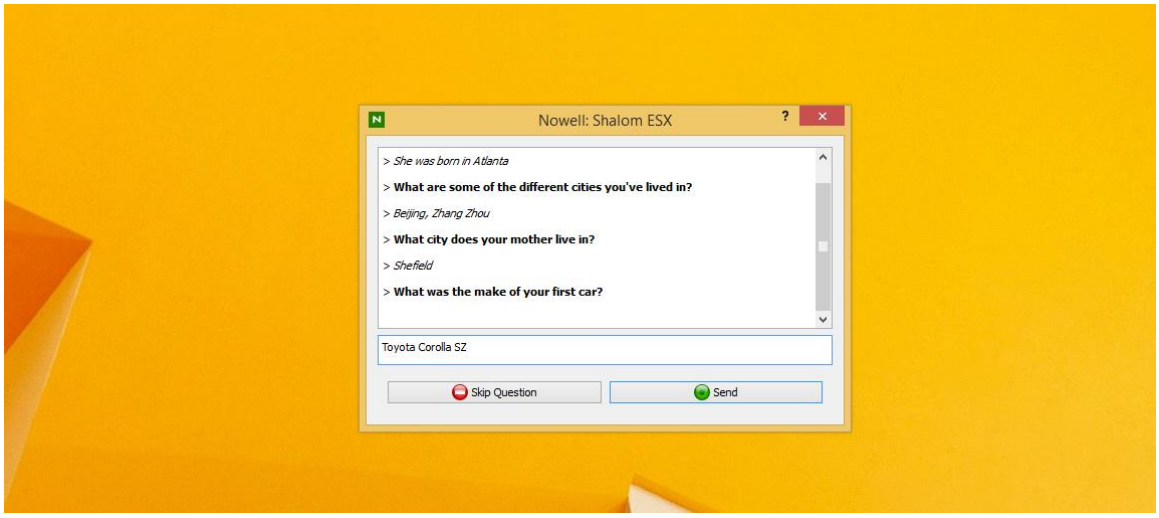
Risk Security Flow Chart



NOWELL
DEVELOPMENT
Application software
& services

First Shalom ESX Interviews Each User – Authentication Enrollment

- First, Shalom ESX interviews each user, collecting personal information (e.g. "year of birth", etc.). This information is later used to authenticate users by questioning for identity verification if they behave suspiciously. When Shalom encounters each user, it prompts them to complete this one time interview



Shalom ESX Looks Out For Highly Suspicious Activity (Anomaly Detection)

Shalom ESX monitors how users behave and constantly looks out for suspicious user activity. Shalom can detect when a user is behaving suspiciously or is logged in with someone else's account by observing differences in their behavior. Shalom ESX detects user anomalies with respect to what they do (desktop/cloud applications launched, commands executed, user network activity, etc), where they do it from (host, geo-location), and when (day-type, time) they do it.[7]

For example, consider Mark, an office associate. Between 9 a.m. and 5.p.m., as part of his daily routine, he typically uses PowerPoint and Word to proof read financial reports for his boss. Now, if all of a sudden, Mark logs in at 1 a.m., runs an "ftp" command to transfer files (which he has access to), such an unusual activity will be seen as suspicious and would trigger Shalom to report the action.

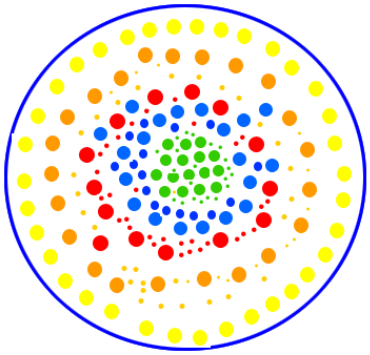
Here's another example. Let's assume Pete a traveling salesman, always works with his notebook 5 days a week, excluding weekends. If all of a sudden, Pete appears to be working on Amy's desktop, on a weekend, and at 3 a.m., such a drastic change in behavior would also trigger Shalom to report.

Shalom also tracks anomalous network resource behavior by users. Let's assume another user, Jason prints documents using his local office networked printer on a regular basis. If Jason is found to be printing documents using a printer located in another part of the office network, Shalom will be able to track that suspicious anomaly because he is sending data to a part of the network that he typically does not access on a regular basis.

Finally, Shalom profiles cloud applications' remote network behavior of each user and looks out for highly suspicious remote network[8] activity. For example, consider John, who typically accesses remote network shares A & B, on an outsourced cloud vendor's web application for his data entry work during normal business hours. If all of a sudden, John now accesses remote network share Z SQL database, which holds credit card numbers, such an activity would trigger a report.

Regardless of who logs into any Shalom secured endpoint, whether an impostor, an intruder, or an insider with possible malicious intent, Shalom software is constantly on the lookout for suspicious user activity, taking into account all possible behavior variables. After the software finishes learning about a user's behavior, it then begins to look out for unusual behavior anomalies and it authenticates suspicious activity

Shalom "Moving Window" Anomaly Detection: Circle of Normal Events (as time progresses to eternity)



Anomaly detection for each identity in real time - behavior towards the outside circle (yellow, orange, red) is often suspicious and of higher risk. Green & blue represents lesser risk. Graphical illustration of statistical adaptive algorithm

Shalom ESX emulates this Anomaly Detection method for each user and each host in real time – any behavior that's outside the circle is often "suspicious" because it is highly unusual and might indicate a potential internal security breach

8 *Software monitors remote hosts and remote application connections*

Authenticates Users for Identity Verification If They Behave Suspiciously (Multi-Factor Authentication)

Optionally, if Shalom observes a user behaving suspiciously— in a highly unusual manner— it authenticates the user to verify their identity. In the authentication, random questions are asked based on what was learned earlier in the initial interview. The questions asked are few, specific and therefore require specific answers. These questions are structured in such a way that only the real, actual account owner can give correct answers since only they know what was said in the interview

Identifies Suspicious Insiders and Reports In Real Time

Software reports the users' exact anomaly, including their suspicious activity (triggered application, command, or script), date and time of breach, location of the attack, and suspiciously accessed network shares, databases, and ports. These reports can then be reviewed to investigate for unauthorized insider activity. Questioning and reporting suspicious users at the very moment they behave suspiciously *disrupts, deters, and discourages* possible malicious insiders, as they'll know they've been caught and reported.

After authentication, a detailed security report is sent to information security administrators notifying them about the incident. Administrators are able to further investigate passed authentications for possible unauthorized actions by insiders. If a user fails the authentication, they will be reported to administrators for further action[9] and the account is in a high-risk state.

Shalom ESX Also Finds and Reports Phony Backdoor Computer Accounts

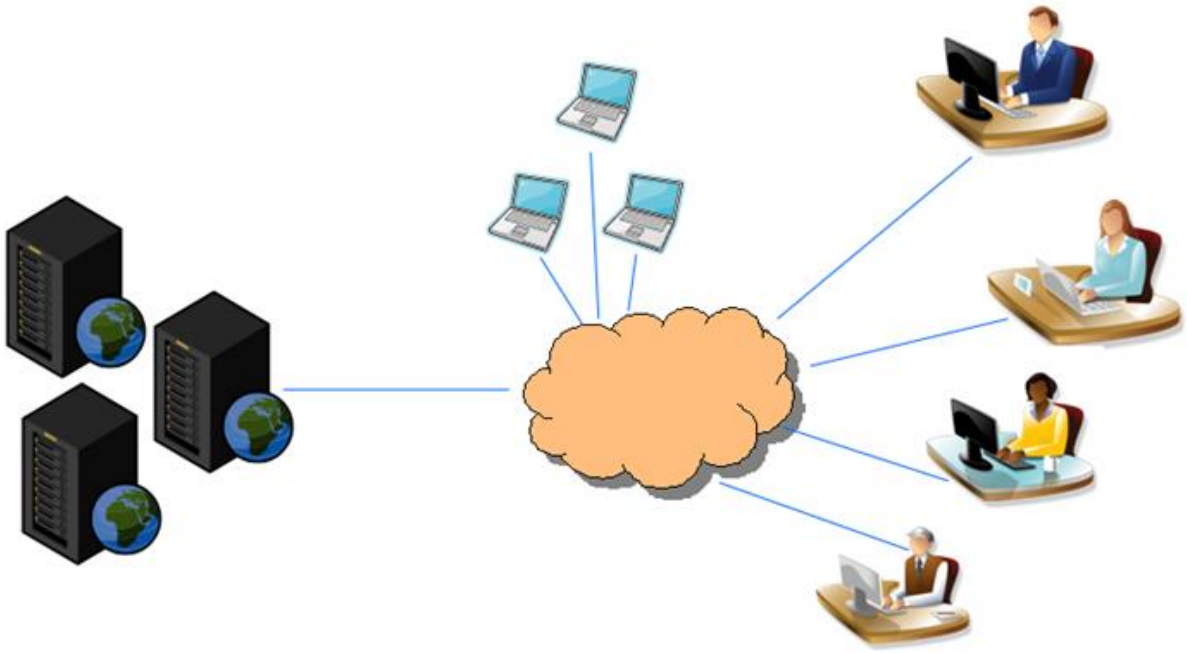
In some cases, the malicious insider aware of audited systems does not perform attack using their own accounts. Sometimes, they go as far as creating and using phony backdoor accounts that have admin level privileges. If the software encounters any new user (legitimate or illegitimate), it prompts them to complete the interview. At this point, perpetrators using newly created backdoor accounts are detected and immediately reported. Without reaching any conclusions, Shalom reports the name of the backdoor account, how they entered the network, from where and at exactly what time. IT administrators can then investigate and destroy backdoor accounts using Active Directory, LDAP, or whatever user identity management tool is used.

9 *It is possible to only detect anomalies—unusual behavior— without authenticating users. We recommend however, that secure computing environments should authenticate suspicious users to deter security breaches.*

NOWELL DEVELOPMENT
Application software & services

Shalom ESX Securing Multiple Users at the Same Time over the Cloud

Cloud SaaS Security Model



1. Shalom software is able to secure multiple users simultaneously logged into different parts of an enterprise network using different vector entry points
2. Delivered securely over the cloud, all data is encrypted, and packet authenticated using Dynamic AES 256 bit Strong Cryptography Implementation
3. Scale upwards or downwards, on-demand , on-the go
4. No additional hardware required
5. Advanced security cloud protections to prevent insider threats, internal fraud and identity theft
6. Hosted server in the cloud manages Shalom agents on desktops, laptops, and servers.
7. Integrates well with existing JNDI LDAP-based identity management & directory services
8. Reduces risk exposure of enterprise IT applications as they gradually migrate to the cloud
9. Validated Support for Windows XP, Windows Vista, Windows Server and Windows 7 (32 & 64 bit)
10. Customized-build support for POSIX based operating systems such as Linux and Sun Solaris *(Contact Nowell to see what variants of Linux /UNIX are available)*

Microsoft Partner Silver Cloud Platform redhat. Business Partner IBM Ready for Security Intelligence ORACLE Silver Partner

Software data is encrypted using OpenSSL NIST Certified AES 256 Bit Cryptography and kept private. Identification and proper authentication are necessary for detecting security breaches across various channels

Provides Enterprise Class Risk Analytics Reporting Using Industry Reporting Standards

Shalom reports via email, cell-phone SMS, and also logs all security events on the hosted cloud server accessible using the security admin tool GUI. These reports can be sorted, saved and archived for later use. The reports can also be converted into industry standard reporting file formats such as CSV for better integration, compatibility and exchange between disparate reporting and business risk intelligence applications. These incident reports state the suspicious event (what), the offending computer account (who), date, time (when) and corrective actions taken (authentication: pass, fail). The security tool also provides information on exactly who's logged in at any given location at any given time in the network.

Uses A "Moving Window" Method to Detect When Users Change Behavior

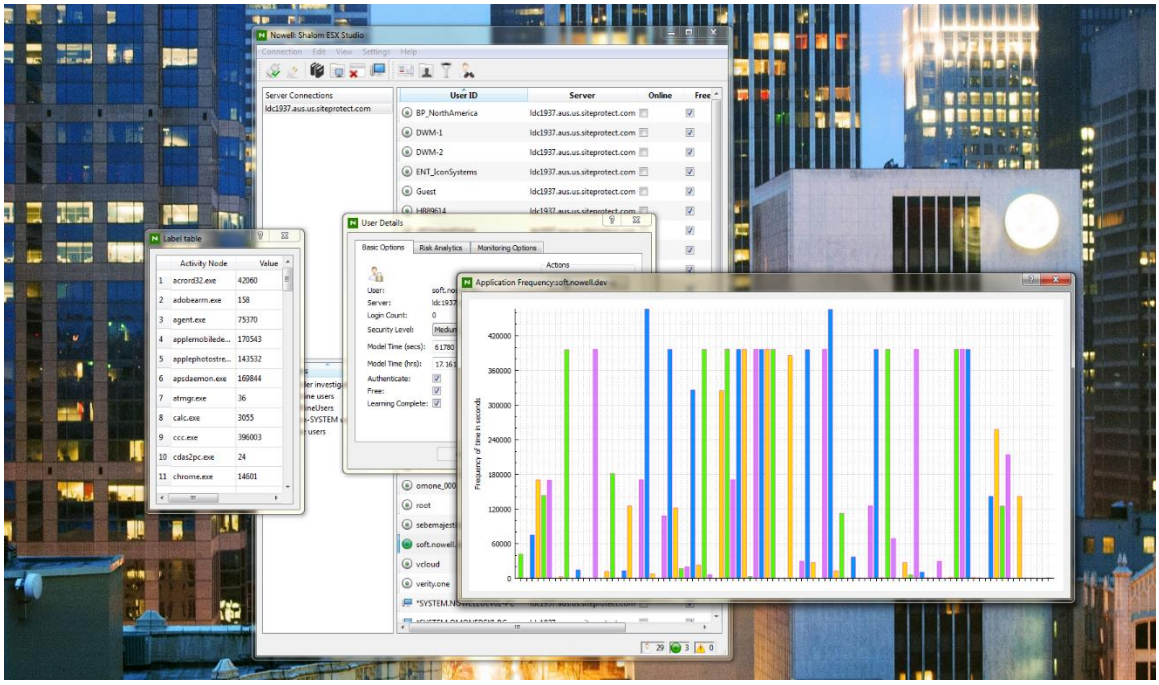
Shalom addresses changes in user behavior like a moving window that captures normal user behavior over time. Older behavior is eventually removed and only the more current, normal user behavior is retained for anomaly detection. For example, let's assume an accountant, Martha, uses Excel and a legacy application for her accounting work. Now Martha receives a promotion, becomes an auditor and now uses a Web based auditing tool, so her computer behavior changes. Shalom detects this change, adapts automatically so that her old behavior as an accountant is eventually dropped from her base profile. This moving window concept applies to all variables (application use, time, network, etc.) profiled. This adjusting capability ensures that Shalom always detects suspicious activity even when legitimate users change job functions.

Easy To Deploy and Manage Across Large Networks Using Administration Tool

- Shalom software is configurable. Optionally, Shalom can be configured to only report suspicious insider activity and profile bits can be set per site.
- Shalom software is managed centrally by a secure, very easy-to-use intuitive graphical user interface

NOWELL DEVELOPMENT
Application software & services

Shalom ESX Security Platform Administration Interface – features LDAP Integration with Directory Services



All Data and Communications Encrypted Using OpenSSL AES 256 Bit (Rijndael) Encryption

All relevant security information gathered from users being secured is completely hidden and stored away in a central location tightly encrypted using OpenSSL AES 256 bit dynamic strong encryption. The Advanced Encryption Standard (Rijndael) is the encryption standard adopted by several governments and businesses. In addition, all network data communications, data-in-transit, and security data-at-rest in Shalom ESX Platform are strongly encrypted and packet-authenticated. Also, all actions taken on the security tool are always logged for auditing administrator actions.

Internal Risk Management Controls Help Prevent Internal Fraud

The Shalom ESX Administration tool helps to prevent fraud caused by insiders. The administration tool offers a display dash board for the disclosure of risk patterns that may be indicators of potential fraudulent internal activity. Loss prevention specialists can correlate this information with financial systems to detect fraud and assess internal risk posture. Graphs and charts are also available for summarized reporting.

NOWELL DEVELOPMENT
Application software & services

Enterprise Regulations: SOX, GLBA, Visa-CISP,PCI Security Standards, FISMA, FFIEC, and HIPAA That All Call for Internal Security Controls

ID thieves or Insiders are sometimes the root-cause of stolen company information. Such sensitive information could be customer personal information, banking data, credit cardholder data, intellectual property, patient health records, or even classified information.

By authenticating intruders, you reduce the risk of impostors accessing your sensitive data from inside the network. However, in the case of passed interrogations, suspicious and possible unauthorized insider activity is always reported so malicious insiders are contained in real time.

Safeguards must be implemented to fully protect the confidentiality, integrity, and privacy of corporate data, supporting enterprise regulations that all call for proactive internal controls.

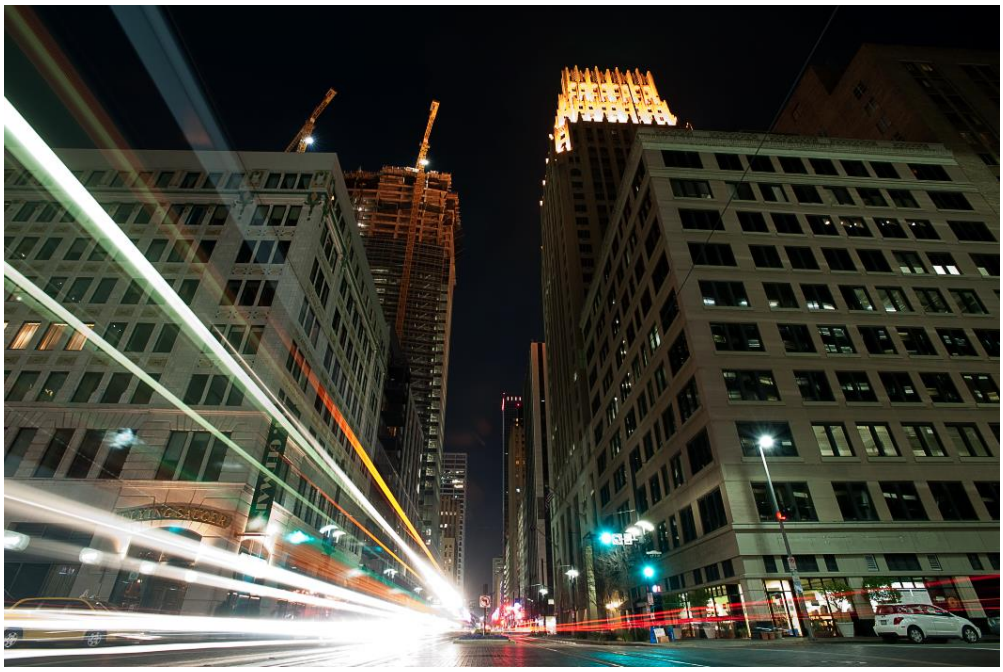
Summary

1. Detect and Deter Insider Risks and Identity Fraud in Real Time.
2. Provide Intelligent Multifactor Authentication— prevent infiltrators & assures authorized access.
3. Reduces the overall risk exposure of enterprise IT applications as they gradually migrate to the cloud
4. Support risk regulations: FFIEC, SOX, GLB, VISA-CISP, PCI Compliance, FISMA, BASEL II, NIST SP's and HIPAA.

5. Invest in a reliable, mature cloud security services framework as you move your IT into the cloud

Contact us for more information support@nowellgroup.com

NOWELL
DEVELOPMENT
Application software
& services



Contact Us Today:

Nowell Development, Inc
11152 Westheimer Road # 956
Houston, Texas 77042
United States of America
Web: http://www.nowellgroup.com
E-mail: support@nowellgroup.com
Phone: +1-(713)-496-2366
http://linkedin.com/company/nowell-inc

NOWELL
Integrity Above Profits

"Et cognoscetis veritatem, et veritas liberabit vos"
"And you shall know the truth, and the truth shall make you free" John 8:32

المسيح هو السلام

" ويجب أن تعرف الحقيقة ، والحقيقة سوف تمنحك الحرية "