NOWELL
DEVELOPMENT

Application software &
Services

SHALOM ESX 5 – APPLICATION SECURITY SOFTWARE - QUICK SHEET

Collaborate & integrate hosted applications security & risk as a team

- Reduces risks of internal[1] security breach by privileged users, identity fraud
- Loss prevention, security and risk management integrated software solution (integrity assurance)
- Hosted authentication software platform for online financial transactions
- Java J2EE API to expose multifactor authentication services to your web based application software services, via IBS Openwave SDK
- Collaborative, team-based risk software is recommended for high-security business environments
- Enhances risk monitoring and authentication services for LDAP directory services such as Oracle Directory server and IBM Security Directory Server, and SailPoint IIQ IAM

## Multifactor authentication, behavior & trend patterns

- First Shalom ESX learns specifics about each user by collecting authentication data. This brief question-answer interview occurs only once
- This information is later used to authenticate users by questioning for identity verification if suspicious activity is identified.
- Secures application users by authenticating behavior over time, applications used, time of use, and from where (hosts), including their cloud network behavior (accessed networks, databases, and ports).

---

[1] Internal security refers to when an unauthorized outsider illegally gains access to business systems via stolen credentials and logon data

Software identifies high risk behavior, provides multifactor authentication

- Software monitors suspicious activity, an indicator of a possible internal security breach
- If suspicious activity is detected, Shalom ESX reports, then optionally authenticates the user by asking few questions. Optionally, can be configured to only report suspicious actions
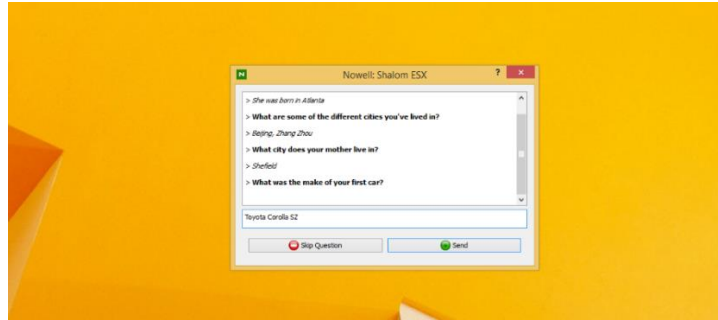
Prevent unauthorized system access, reporting capabilities

- After authentication the incident is reported to administrators to decide on next course of action; Identification and authentication reduces identity fraud;
- Shalom ESX contains security breaches by identifying, authenticating, and reporting in real time.
- It reports what/where/when it happened, and who did it, associated accounts and applications.
- Helps detect hidden viruses or implanted application introduced via email, network or perhaps web surfing
- All reports are stored in an SQL database where they can be sorted, search, compared and analyzed; Administrators can use the Shalom ESX Studio Admin Tool to look up reports, release users, and further review reports for malicious insider activity.

Setup, supported platforms and system components

- Shalom ESX Server is installed on an RHAT Enterprise Linux* cloud server for every network domain of unique user accounts in the cloud, client software on end-points; Oracle MySQL Database is required, and is installed in the cloud
- Microsoft Windows 7/8/10, Windows Server
- Open SSL cryptography support for data security
- Java JDK/JRE 1.8 or greater for IBS Openwave Java J2EE service
  *Windows networks require provisioned cloud server (hosted on premise or private cloud)
- Oracle MySQL DB 5.7, CentOS/RHAT EL 6.7 x86_64 (Stable QA/Approved)

"Give thanks to the LORD, for he is good; his love endures forever" Psalm 118
INTEGRITY ABOVE PROFITS