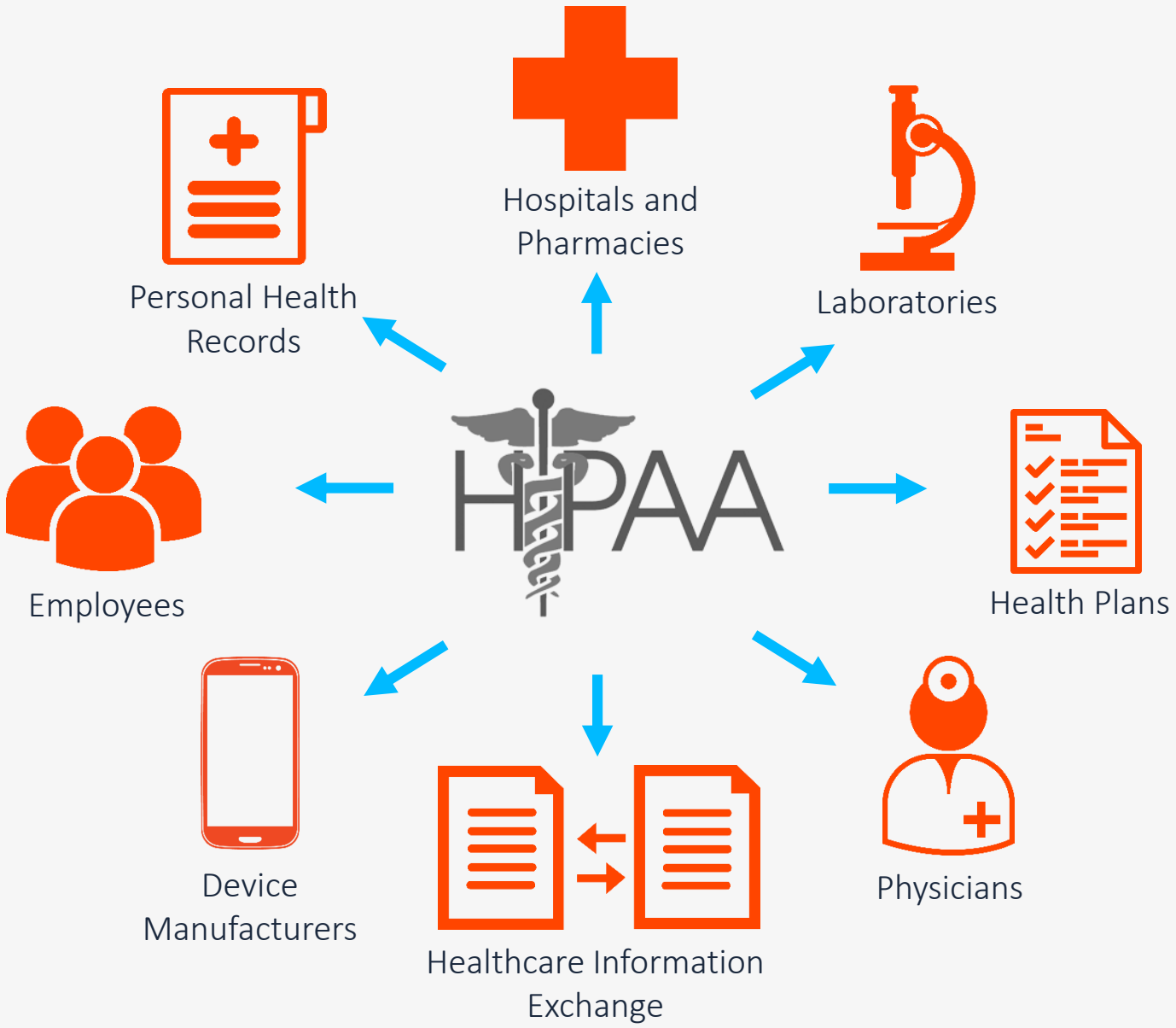
iSecurity & HIPAA Compliance

About HIPAA

- Health Insurance Portability and Accountability Act
- Enacted by the U.S. Congress in 1996
- A group of regulations that combat waste, fraud, and abuse in health care delivery and health insurance.
- Title II of HIPAA, - the Administrative Simplification (AS) provisions, addresses the security and privacy of health data.



HIPAA Requirements for Enterprises

- Institute a required level of security for health information, including limiting disclosures of information to the minimum required for the activity
- Designate a privacy officer and contact person
- Establish privacy and disclosure policies to comply with HIPAA
- Train employees on privacy policies
- Establish sanctions for employees who violate privacy policies
- Establish administrative systems in relation to the health information that can respond to complaints, respond to requests for corrections of health information by a patient, accept requests not to disclose for certain purposes, track disclosures of health information
- Issue a privacy notice to patients concerning the use and disclosure of their protected health information
- Establish a process through an IRB (or privacy board) for a HIPAA review of research protocols
- As a health care provider, include consent for disclosures for treatment, payment, and health care operations in treatment consent form (optional).

iSecurity Products Supporting HIPAA (1)

- Firewall – prevents criminals from accessing and stealing sensitive data. Covers all 53 System communications protocols. Logs all access attempts and reports breaches.
- Audit – monitors and reports on all activity in the System I, performs as real-time auditing and detailed server audit trails.
- Compliance Evaluator – provides at-a-glance compliance checks assessing security status, strengths and weaknesses, based on industry and corporate policies.
- Authority on Demand – Control of user authorities, and dynamic granting of additional authorities on an as-needed basis, accompanied by more scrutinized monitoring.
- AP-Journal (including READ logs) – Monitoring of all changes in business-critical data & alerting of relevant personnel upon significant changes.
- Visualizer - Business Intelligence System for display and analysis of data from the System i

iSecurity Products Supporting HIPAA (2)

- Password - Full password management capabilities, including enforcement of site-defined password policies. Provides detailed daily reports of unsecured passwords.
- Anti Virus - Protection from Windows-compatible viruses and programs used or stored on System i server. Performs automatic pre-scheduled periodic scans.
- Central Admin - Manages multiple systems from a single control point
- Action - includes real-time alarms and protective response mechanisms for the System i
- Capture – performs silent capturing, saving and playback of user sessions
- View - protects and controls the display of classified data in iSeries user workstations.
- Screen - Automatic protection for unattended workstations
- Encryption (future) - Prevents intruders from using stolen information even when they succeed in obtaining it.

iSecurity Compliance with HIPAA

HIPAA Technical Safeguards Requirement	Description: (R)=Required (A)=Addressable	Firewall	Audit	Visualizer	Compliance Evaluator	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
164.312(a)(1)	(R): Access Control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	√	√	√	√	√		√	√	√	√		√		√	
164.312(a)(2)(i)	(R): Unique User Identification. Implement procedures to assign a unique name and/or number for identifying and tracking user identity.		√	√	√	√			√	√	√		√	√	√	
164.312(a)(2)(ii)	(R): Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.		√	√	√	√		√		√			√	√		
164.312(a)(2)(iii)	(A): Automatic Logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.											√				
164.312(a)(2)(iv)	(A): Encryption and Decryption. Implement procedures to describe a mechanism to encrypt and decrypt electronic protected health information.		√	√	√	√		√	√	√	√					√

iSecurity Compliance with HIPAA

HIPAA Technical Safeguards Requirement	Description: (R)=Required (A)=Addressable	Firewall	Audit	Visualizer Evaluator	Compliance	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
164.312(b)	(R): Audit Controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	√	√	√	√	√		√	√	√	√		√	√	√	
164.312(c)(1)	(R): Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.		√	√	√	√		√	√	√						
164.312(c)(2)	(A): Mechanism to authenticate electronic protected health information. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.		√	√	√	√		√	√	√						
164.312(d)	(R): Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	√	√	√	√	√			√	√			√	√	√	

iSecurity Compliance with HIPAA

HIPAA Technical Safeguards Requirement	Description: (R)=Required (A)=Addressable	Firewall	Audit	Evaluator Visualizer	Compliance	Central Admin	Anti-Virus	AP-Journal	Action	Capture	View	Screen	AOD	Password	Assessment	Nubridges
164.312(e)(1)	(R): Transmission Security. Implement technical security policies and procedures measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	√		√	√	√			√	√					√	
164.312(e)(2)(i)	(A): Integrity Controls. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	√	√	√	√	√			√	√					√	
164.312(e)(2)(ii)	(A): Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.		√	√	√	√		√	√	√	√					√

HIPAA Links

- The official central governmental hub for all HIPAA issues
  - http://www.hhs.gov/ocr/privacy/index.html
- CMS (Center for Medicaid & Medicare):
  - http://www.cms.hhs.gov/SecurityStandard/
  - http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf
- HIPAA Security Guide
  - http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806rev.pdf
- HIPAA Security Standards Final Rule
  - http://www.hipaa.samhsa.gov/download2/HIPAASecurityStandardsFinalRule.ppt#271,16,Basic Changes from NPRM
- HIPAA Security Rule Standards and Implementation Specifications
  - http://www.nchica.org/HIPAAResources/Security/rule.htm#admin2

Raz-Lee Security – Mission & Product Lines

"Raz-Lee Security is committed to providing the best and most comprehensive IBM i compliance, auditing and security solutions"

- Founded in 1983
- 100% focused on IBM i (AS/400)
- Corporate offices in: US, Italy, Germany
- Installed in more than 40 countries, over 12,000 licenses
- IBM Business Partner
- Integration Partner with Tivoli and Qradar
- Partnerships with other major global SIEM & DAM solution providers:
  - Official partnerships with McAfee, RSA enVision, HP OpenView, GFI, NNT
  - OEM by Imperva SecureSphere
  - Proven integration with ArcSight, CA UniCenter, Splunk, Juniper
- Worldwide distribution network

Business Partners

Raz-Lee's Global Distribution Network

iSecurity: Selected Customers

- CHS (Community Health Systems, US)
  - ¬200+ systems and growing
  - Replaced Powertech
- Royal Bank of Scotland
  - Purchased iSecurity after POCs of nearly ALL competitors!
- Venetian Casinos (multi-national)
  - Purchased iSecurity following extensive compliance POC.
- Euronet Worldwide
  - Banking clearinghouse in Europe & Asia
  - Replaced competitor with iSecurity.
- Svenska Handelsbanken
  - One of the largest banks in Scandinavia
  - Used competitor for several years; replaced it with iSecurity.

Internationally renowned IBM i solutions provider

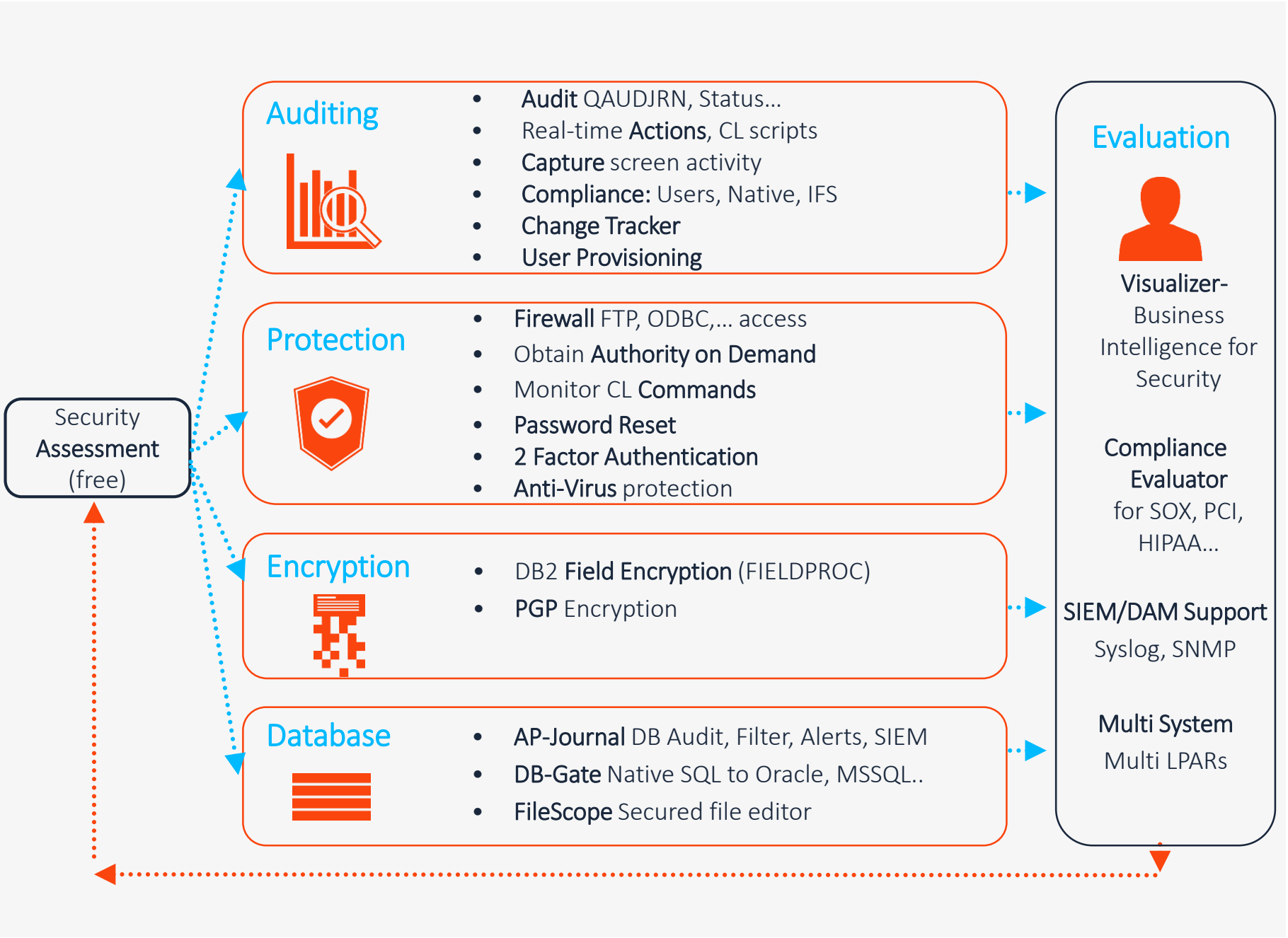
iSecurity Characteristics

The leader in IBM i security with on-going product development

- Full GUI and green screen - short learning curve, ease of use
- Visualizer Business Intelligence analysis
- Hundreds of built-in, customizable reports. Report/Query Generator and Scheduler produces print, screen, HTML, PDF, CSV e-mailed reports.
- Wizards, Real Time/Periodical, Alerts. All done on IBM i
- Supports SIEM with CEF, LEEF formats; Sends SYSLOG, SNMP, Twitter, e-mail, SMS, etc.
- Cross-enterprise reporting, definitions, logs
- Exceptional performance on all sizes of systems
- Unique products: Capture, Change Tracker, DB-Gate, Anti-Virus

iSecurity Suite of Products

- GDPR, PCI, HIPAA, SOX, JSOX, FDA
- Local Regulations
- Auditor's Requests
- Detect Security Breach
- Management Decision



Contact Us

marketing@razlee.com