



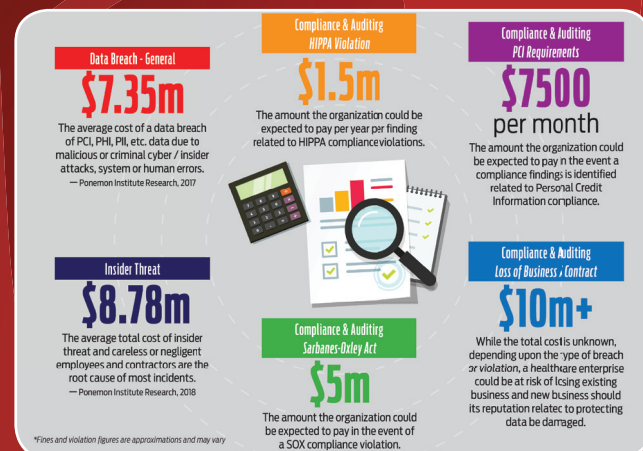
Physical and IT Security Convergence

Beyond compliance - managing risk for the healthcare enterprise

Delivering quality healthcare is a combined effort requiring close cooperation between provider networks, hospitals, medical specialties as well as lab and testing services. Add to this the dimension of prescription management, pharmaceutical supply chain and retail pharmacy. The claims and delivery management systems for health insurance carriers, HMOs and PMOs all need access to medical records. Patient information has to flow seamlessly across all delivery organizations and health insurers. Regulations like HIPAA and industry best practice frameworks like HITRUST require that primary healthcare providers not only vigorously protect patient privacy, but also take responsibility for enforcing the same standards of security due diligence for their partner providers. New provisions allow for potential fines for privacy violations to range from \$25,000 to \$1.5 Million per occurrence.

REGULATIONS AND STANDARDS

- HIPAA
- Sarbanes-Oxley
- NIST SP800-xx
- ISO 27001/ 27002
- HITRUST



ALERT ENTERPRISE SOLUTIONS

- Enterprise Guardian
- Enterprise Sentry
- Identity intelligence Technology
- Enterprise Visitor Identity Management

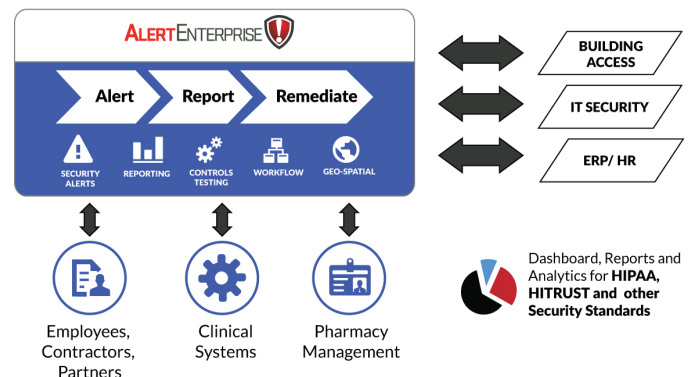
ACTIVE POLICY ENFORCEMENT FOR IT AND BUILDING ACCESS

Hundreds of access points, thousands of employees and scores of service provider organizations make up the extended healthcare enterprise. Determining risk to this broad enterprise involves managing roles and critical access for each of those roles. Do employees or contractors have the right training and certification to access personal health information? Safeguarding confidential personal health and financial information also means monitoring who has physical access to the records. Did the badge access and system access for terminated employees get turned off at the right time?

AlertEnterprise software delivers real-time integration of Identity Access Governance with Physical Access Control and Human Resource applications. The converged security approach automates policy enforcement and compliance, helping you automatically validate employee background checks, training and certification, authorization to view patient information and other vendor services.

YOU'VE IDENTIFIED THE RISK. NOW WHAT? - ALERTENTERPRISE DELIVERS THE NEXT STEPS

Identifying the risks alone is not enough. Organizations need to make sure that immediate steps are being taken to mitigate risks. AlertEnterprise automates remediation and helps you to analyze risks, and visualize remediation paths before taking action. Business analysts, IT security and physical security teams can collaborate visually and implement the next steps – which may include reviewing correlated risk recommendations for selected employees and removing physical access to certain parts of the facility or system access to certain applications that contain sensitive data.



AlertEnterprise delivers blended risk management capabilities to the extended healthcare enterprise. Auto-remediation helps organizations avoid fines while staying in compliance with HIPAA and HITRUST.

AlertEnterprise integrates IT and physical security across diverse systems, applications, databases and geographically distributed assets. It provides rules-driven risk prevention for cross-enterprise access security and transaction authorization. AlertEnterprise also provides real-time monitoring and correlation of IT and physical access events for timely detection, alerting and remedial action in response to security, regulatory or policy violations. AlertEnterprise integrates with multiple PACS systems, ERP Systems, HR systems, Patient Records Management, Clinical Systems, Pharmacy Management Systems and other critical applications found in hospital and other healthcare environments.

Improve Compliance & Enforce Policies

- Training, PRA Compliance
- Certification Requirements
- Content Packs: SOX, GDPR, HIPAA, HITRUST, Health Level 7 (HL7) Integration
- Full Audits Controls/ Chain of Custody
- Access Review & Recertification
 - Area Owner Access Areas
 - Manages Reports
- Immediate Access Revocation upon Termination
- Access rights and approvals to secure areas
- Visitor Screen and Approvals

Reduce Costs of Breach, Risk & Damages

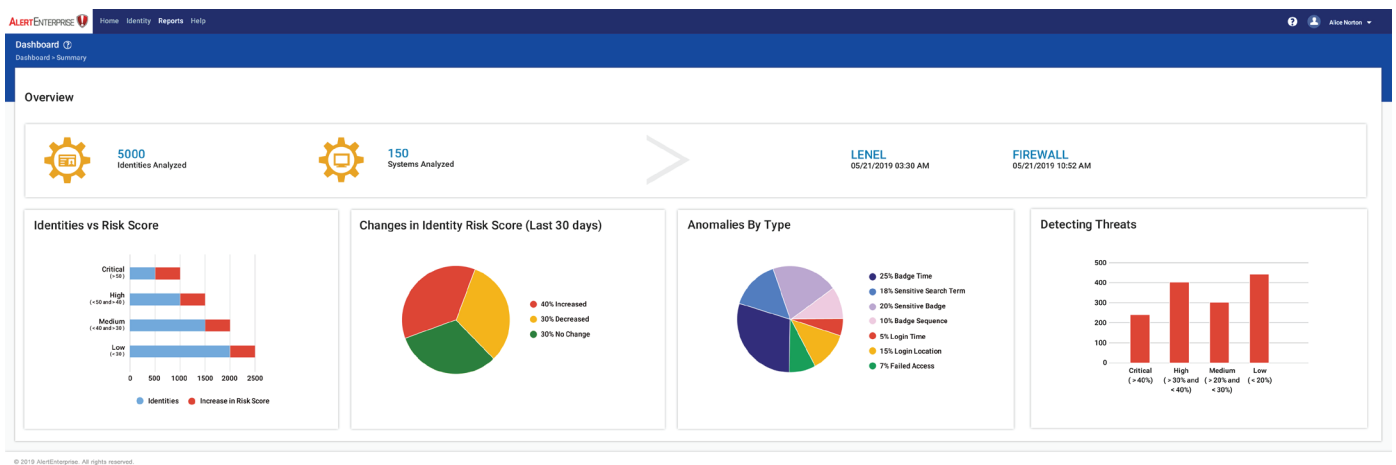
- Risk-Based Security Controls
- Unique Identity/ Recon.IT&PS
- Segregation of Duties
 - Privilege Users
 - Secondary Approvals
- Segregation of Data
 - Privacy/ Encryption
 - Secondary Approvals
- Eliminate Access Creeps
- Eliminate Orphan Accounts

Streamline Security Administration & Support Costs

- Automate manual data entry
- Automate manual paper process
 - HR Driven
 - Access Requests
- Eliminate duplicates, errors
- Streamline badge operation
- Improve security investigation
- Automate manual audit, reports
- Leverage existing investments
- Partner Channel Access Management with Self-Service Portal

ALERTENTERPRISE SOFTWARE FEATURES

- Real-time validation of certification and credentials during access provisioning
- Manage deprovisioning process and cross-linkage of access termination from multiple systems simultaneously – physical, logical and operational.
- Identify compliance gaps in real-time and suggest remedial actions to remain in compliance with HIPAA, Sarbanes-Oxley, NIST SP800-xx, PCI and ISO-2700x standards.
- Identification of risks based on validating employee and contractor access to critical applications and healthcare facilities
- Enforcement of security policies and procedures across vendor and partner ecosystems following HITRUST provisions
- Visual risk and remediation modeling with ability to display key assets on geo-spatial maps with drill-down details on event and asset criticality. Ability to integrate physical security alerts and surveillance video.



Customer Benefits

Delivers most comprehensive view of risk combining logical and physical security
 Improve security - recognize previously undetectable events by analyzing blended threats
 Reduces cost of compliance by eliminating silos and redundant investments
 Verifiable compliance with regulations, standards and best practice frameworks – eliminate fines
 Incident response and management including enforcement of restricted zones
 Previously undetectable events can be displayed as system alerts with location-based context
 Segregation of access, screening and testing following medical emergencies or pandemic outbreaks