

AlertEnterprise!

True Convergence of Physical and Logical Security



COMPANY
BACKGROUND

Quick Facts

Name:	AlertEnterprise, Inc.
Year Founded:	2007
Corp. Headquarters:	Silicon Valley, California
Office Locations:	Los Angeles, CA; New York, NY; London, UK; Hong Kong, PRC; Chandigarh, India
Products and Services:	Enterprise Security Software
Investors:	Startup Farms Inc., Opus Capital Ventures.
Background:	Founders of Virsa Systems, acquired by SAP in 2006 to form SAP GRC business unit

Company Overview

AlertEnterprise is an enterprise security software company that bridges the single most overlooked gap in enterprise security - the true prevention and detection of cross-enterprise threats by linking physical access and IT security to ensure compliance with regulations and standards. AlertEnterprise delivers unprecedented capabilities to visualize previously undetectable threats and assists managers in remediating security risk across the enterprise.

AlertEnterprise has created a unique solution that allows organizations to detect blended threats and delivers incident response and auto remediation based on

- By converging logical and physical access security, AlertEnterprise uniquely detects and prevents cross-enterprise risks that would otherwise go unnoticed.
- With automated risk analysis, detection and case management, AlertEnterprise automates compliance with corporate, policy, operating procedures and State and Federal regulations, including NERC-CIP, CFATS, SOX, and others.
- The AlertEnterprise customer base includes energy companies that are utilizing the solution for critical infrastructure protection

The company operates its business to fulfill the security and risk management needs of customers in three different security impact zones:

- Managing security risk for sensitive business applications in regulated industries
- Managing risk of cyber intrusion and physical access to critical infrastructure
- Security risk and incident management solutions for Federal, Homeland Security, DoD and Intelligence applications

Prevention Scenarios

AlertEnterprise is designed to prevent threat scenarios like the following:

- A relay setting in a utility control room is changed by a technician who never physically entered the building - blackouts follow.
- A technician at a major chemical company enters several labs to remove dangerous chemicals. He has all the components of a dirty bomb.
- Oil refinery technicians are over-exposed to hazardous chemicals and fall ill, triggering lawsuits. .
- A pharmaceutical executive steals drugs to sell on the Internet via rogue pharmacies.
- A mid-level manager at a major health provider accesses confidential patient information – in clear violation of several regulations, most notably HIPAA.
- An IT manager at a major financial institution is downloading customer social security numbers from the server room, a room he never physically entered. The information is sold to scam artists that ultimately create thousands of fraudulent bank accounts.
- A freight train is derailed into a nearby chemical plant as a result of unauthorized changes to SCADA control settings. An explosion results.

Products Overview

AlertEnterprise Solutions

AlertAccess

AlertAccess provides rules-driven and policy-compliant user access management and provisioning across the enterprise, analyzing risk across all IT applications, physical systems, and the network. AlertAccess is architected to take advantage of existing Segregation of Duties (SoD) engines for ERP applications and provide an enterprise view for access control exposure across the enterprise.

AlertInsight

AlertInsight completely automates risk remediation and fundamentally aligns IT and business users by providing actionable and visual analytics. It overlays and integrates data from multiple sources including ERP, IDM, Corporate Directories, HR, and GRC to provide the complete context required to perform on-the-fly remediation. The visual model converts the technical complexity into business-friendly relationships and descriptions.

AlertAction

AlertAction provides geo-spatial monitoring and remediation of cross-enterprise threats, serious acts of sabotage, terrorism, fraud and theft etc. The solution offers capabilities to co-relate seemingly innocent events and activities to detect real threats and risks, while boasting of powerful alerting and automated Remedial Action Strategies (RAS) for decisive action.

Business Solutions

Risk and Compliance Functions

- Multi-regulatory compliance
- Continuous visibility into cross-enterprise risk
- Dashboards and audit reports
- Powerful Visual Remediation

Cross Enterprise Multi-Modal Risk Analysis

- Risk analysis across IT Systems, Physical Access and Industrial Control Systems
- Remediating access violations and correlating with compliance gaps
- Completing risk analysis prior to granting access and user requests

Managing Access to Business Critical Assets and Systems

- Access and custody of corporate assets
- Policy-compliant On-boarding and Off-boarding

Managing Healthcare Privacy Data and Applications

- HIPAA Compliance
- Policy-compliant Records Retention and Management

Critical Infrastructure Protection Solutions

Protection against cyber attacks targeting:

- Bulk Electricity System in N.A. (NERC CIP)
- Chemical Storage and Transportation (CFATS)
- Mass Transportation and Port Security (MTSA, C-TPATS)
- Water Treatment and Distribution (ANSI/ISA99)
- Pharmaceutical (21 CFR Sub Part 15(J))

Benefits

Protection from sabotage, terrorism and insider attacks to prevent

- Drug and chemical diversion
- Denial of Service and Attacks on Reputation
- Misuse of weapons-grade or hazardous material

Federal, Military, DHS and Intelligence Solutions

Federal Government and Agencies

- Certification and Accreditation (C&A); FISMA and NIST SP800-53A
- Conducting risk assessments and creating audits reports

DHS, First Responder Support

- Incident Management
- BCP / DR
- Geo-Spatial Visualization
- Remedial Action Scripts

Military and Intelligence Applications

- Pre-access risk assessments
- Blended threat detection
- Contingent Provisioning

AlertEnterprise takes access security to the next level by integrating logical and physical security across diverse systems, applications, databases, and geographically distributed assets. Unlike any other solution provider in the industry, AlertEnterprise delivers a unique risk management capability following a three-step process that aggregates blended threats from IT systems, Physical Access Control Systems, and Critical Control Systems to uncover previously undetectable threats and risks.

AlertEnterprise next generation solutions deliver:

- Rules-driven risk prevention for cross-enterprise access security and transaction authorization.
- Real-time monitoring and correlation of logical and physical access events for timely detection, alerting, and response to security violations.

AlertEnterprise uniquely allow corporations the ability to:

- Automate, enforce, and audit policy-compliant user access to ERP systems, IT applications, physical locations, databases, network, and geographically distributed assets.
- Perform blended risk analysis to detect and prevent cross-enterprise threats.
- Align IT application security, physical access security, and auditors by deploying business-friendly visual analytics for auto-remediation of access violations.
- Automate testing of controls for industry regulations.
- Enforce policy-based employee on-boarding, off-boarding, and change processes, including automated provisioning and de-provisioning of access privileges and physical assets.
- Monitor and correlate user access events displayed on a geo-spatial map.
- Trigger remedial action schemes so personnel can follow best practices and corporate, policy-driven response guidelines for resolving threats.

Technical Capabilities

Multi-regulatory Compliance Management

- Built-in repository of common controls across multiple regulations
- Controls mapped to risks and vulnerabilities
- Common rule sets

Integration with Multiple ERP systems and business process automation

- Pre-integrated with Oracle and SAP
- Business rule sets can be defined

Integration with IT Security Automation

- Identity and Access Management
- Configuration and Change Management
- Vulnerability Scan Systems
- Security Incident Management and Event Management
- Data Loss Prevention and Content Filtering

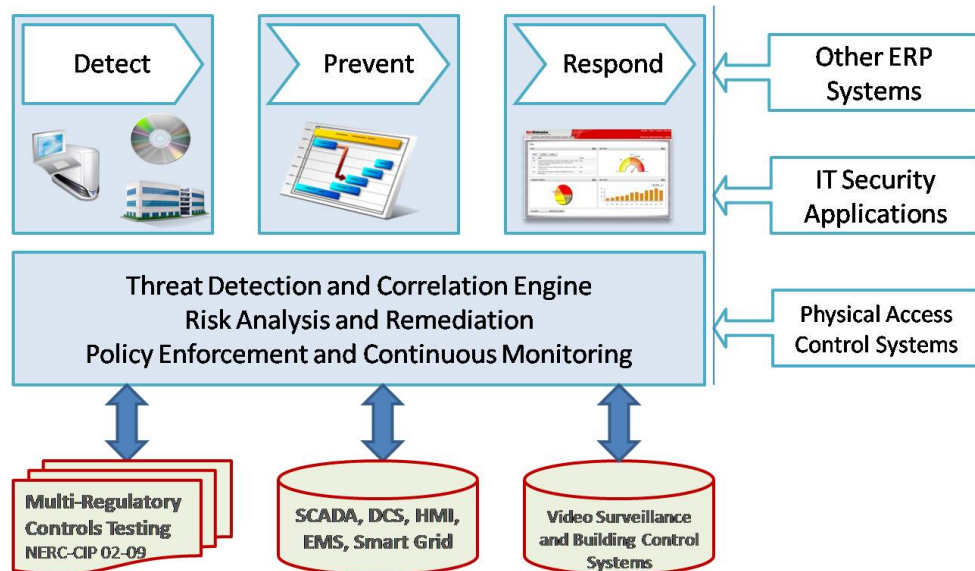
Integration with Physical Security and Physical Access Control Systems

- Integration with building control and card access systems
- Access Card provisioning
- Integration with video surveillance and biometrics

Correlation engine to render risk following detection of blended threats

- Aggregate threats from IT Security, Physical Access and Control Systems
- Accept external feeds like iDefense, NVD, and other threat sources
- Accept access and control violations from a variety of sources

Technical Architecture



AlertEnterprise Architecture supports the convergence of IT Security, Physical Access Controls and Industrial Control Systems to uncover blended threats.

About AlertEnterprise

AlertEnterprise provides the only complete solution for role-based, rules-driven access enforcement. AlertEnterprise addresses blended risk assessment and security across all logical systems, IT applications, databases, and physical systems from a single analytic dashboard, complete with auto-remediation capabilities. Additionally, AlertEnterprise delivers visual risk and event monitoring, alerting, mitigation, and analytics displayed on a geospatial map. AlertEnterprise is headquartered in Fremont, CA and on the web at www.alertenterprise.com

Contact

AlertEnterprise Inc.
45680 Northport Loop E.
Fremont, CA 94538
USA

Tel: 510-440-0840
Fax: 510-440-0841
Email: info@alertenterprise.com