ALERTENTERPRISE

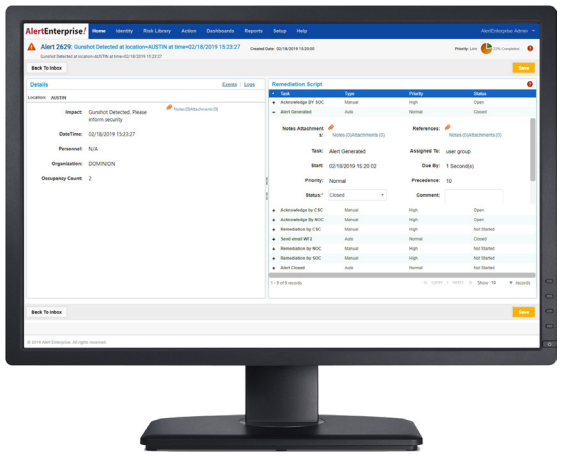
DATA SHEET

Enterprise Sentry™

Unified Security Awareness and AI-Powered Situational Intelligence

Centralized Monitoring of Complex Threats - Cyber, Physical and Airport Operations

Enterprise Sentry delivers a unified security awareness and situational intelligence suite that provides security intelligence across the domains of cybersecurity, physical access to facilities and assets, and Operational Technology like baggage handling systems, aircraft tugs, de-icing systems, and fuel pumps. Consolidated cyber, human and asset intelligence delivers unmatched abilities to correlate threats and empowering Security Operation Center (SOC) personnel to make informed decisions and take appropriate action.



Unified Security Intelligence

- Centralized view of complex threats, events and incidents across cyber, physical and operational domains
- Automated decision support - prioritizes response based on risk and criticality
- Built-in response scripts guide responders on policy-based procedures to follow
- Leverages existing physical security investments like access control and video surveillance

An Intelligent Cyber-Physical Security Solution

- Aggregate Information from vulnerability scanners, firewalls, log management and intrusion detection systems
- Turn data into insights and action with AI-Powered Identity Intelligence, rule-based engine and powerful dashboards
- Include non-cyber clues such as human identity, physical location, critical assets, and time of entry to eliminate false positives and validates alerts and events

Situational Intelligence to Monitor Insider Threat

Traditional PSIM (Physical Security Information Management) solutions lack the intelligence and richness that comes from contextual awareness of correlating events, alerts, and risks across multiple domains like IT Systems, Physical Entry events, and Operational Systems. Being able to associate a risk score with a person's identity, role and what critical assets they have access to, empowers security managers and SOC personnel to make informed decisions specific to each situation. This enhanced situational awareness makes the difference between a delayed response and an immediate response followed by optimal risk aligned action.

AI-Powered Identity Intelligence Technology

AlertEnterprise Identity Intelligence technology dramatically reduces the time and cost for detecting and resolving risk by automating threat protection. Its enhanced machine learning capabilities automatically baseline identity profiles, allowing it to quickly sort through millions of events to identify behavior anomalies and trends for an effective response to potential malicious behavior and policy violations.

When evaluating potential threats the system considers changes in identity behavior such as extended stays in secured areas, increased access attempts outside of regular shift hours, expired badge use, multiple incorrect PIN attempts, and unauthorized remote disconnections. False positives are kept low through powerful AI and the ability to train the system to learn from exception scenarios, helping to reduce the noise and move SOC teams from distraction to action and focus on what matters most.

Enterprise Sentry's patented active policy enforcement rules-based engine automatically identifies policy violations and unauthorized access, allowing security managers to monitor proactively, and respond to suspicious behavior, criminal activity, security violations, as well as operational and procedural issues.

Cyber-Physical Security Solution to Protect The Airport

- Analyzes logs and events collected from SIEM and log management tools
- Correlates with vulnerability scanner information and matches the vulnerability to threat intelligence sources
- Review physical and system access to headend systems and manage identities of employees and contractors with access rights
- Tracks privileged user activity and monitors configuration changes
- Rule-based solution automatically checks to see if meter disconnect threshold numbers are surpassed
- Based on a correlation of IT Security, Physical Access, Identity and Role information, an unauthorized remote disconnect alert is generated and halts further disconnects.