Alert Enterprise

Guardian™

Security Convergence Software for Physical Identity and Access Management (PIAM)

Guardian is the industry-leading Physical Identity and Access Management (PIAM) solution that integrates Physical Access Control Systems (PACS) and badging with enterprise applications, HR systems and IT directory services like Active Directory and LDAP.

As regulations and standards mandate monitoring of physical access to systems and critical assets, PIAM solutions must account for threats that extend beyond IT to include physical access, as well as operating systems that control large production plants and critical assets.

Guardian software delivers PIAM that operates across badging systems from multiple vendors to deliver a single interface that actively enforces uniform policies across all facilities, sites, and locations regardless of disparate badging systems from multiple vendors. Highly configurable, Guardian software enables you to create attributes, forms, workflows on the fly without the need of a code change.

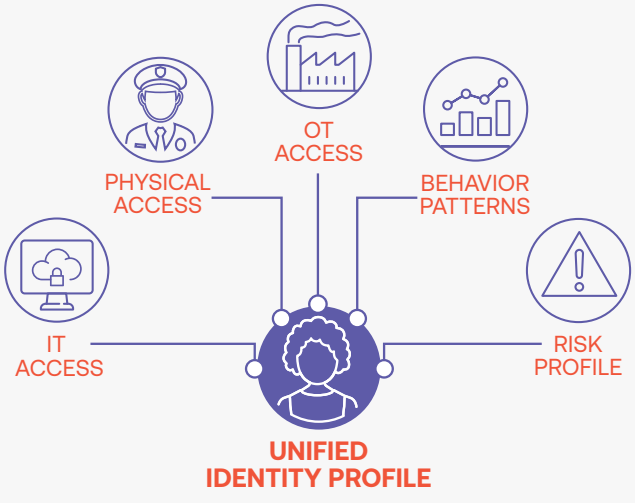
Automated PIAM from Hire to Retire.

Guardian simplifies onboarding/offboarding and termination processes through a single source for access requests and reviews from multiple systems as well as IT and non-IT assets.

Extend Converged Digital Capabilities across IT and Physical Environments.

Universal digital identities across logical and physical and SCADA systems reduce risk, close security gaps and actively enforce policies. Guardian tracks multiple roles and identities, including identities to access physical locations, logical systems, and even specific roles to access individual functions within critical systems and applications.

A Unified Identity Profile Enables Intelligent Decision Making.



CONTACT US | LEARN MORE

Key Functionality

Identity and Access Governance

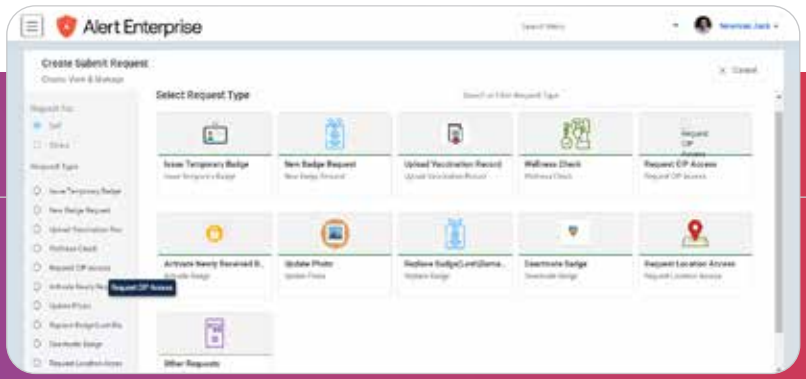
- Upfront analysis for risk and training prior to assigning critical access
- Access certification and role lifecycle management
- Compliance automation and active enforcement with configurable rules engine
- Expiring training
- Background checks
- Conflicting access
- Number of active badges
- Provisioning to on-premise, cloud applications and badging systems
- Centralized contractor management for non-HR cardholders

Physical Identity Management

- Common digital identity for logical and physical identities with active directory integration
- Single interface to provision across multiple badging systems
- Support for high security standards like PIV-I, PIV-C, FICAM, etc.
- Centralized contractor management to manage non-HR temporary badge holders

Manage Access to Operating Assets/SCADA Assets

- Monitor and restrict access to key roles for critical plant operating assets
- Integrate events and alerts from SCADA, DCS and plant applications into security and operational dashboards



Self-Service Portal for Independence and Autonomy.

Empower users, managers, and area owners in your organization and reduce the burden of your support staff through the Self-Service Portal. The Portal helps you promote independence and autonomy across your identity population. Employees can manage badge and access events such as reporting a lost or stolen badge, resetting a password or PIN, and requesting physical access to an area or location. Area owners or building administrators can manage their buildings and people who have access and perform automated and manual access review re-certifications. System administrators can disable badges or remove access in emergencies.

CONTACT US | LEARN MORE

Alert Enterprise

Integrated Visitor Identity Management Identity Intelligence.

Seamless integration with Visitor Identity Management enables you to centralize all aspects of the visitor identity lifecycle through a single interface.

When integrated with AI-powered Identity Intelligence technology, Guardian software provides you the ability to conduct risk analysis prior to provisioning access, helping you protect against insider threats.

Guardian Benefits

- Eliminate gaps between logical and physical identities
- Scale the operation of Access Control Systems to meet enterprise needs across time zones and geographies
- Deliver unified operation and enforce policies uniformly across Access Control Systems from multiple vendors without changing underlying systems
- Automate physical security controls and audit reporting required by various industry regulations
- Reduce cost and reduce risk by eliminating overlap of functions, extending the useful life of existing systems and enhancing overall security
- Provide a running migration path from existing Access Control Systems to newly selected systems when desired, without the risk of disruption or outage

CONTACT US | LEARN MORE