



Alert Enterprise

PIAM for the Food & Beverage Industry.

The Food and Beverage industry must meet high quality standards and adhere to rapid production cycles to preserve nutrition value and freshness.

Securing our most important critical resource - the food supply chain - means correlating threats across underlying HR, IT, Physical Security and Operational Technology used in production and processing.



Alert Enterprise Guardian delivers GEN AI-powered enterprise-wide security, governance, compliance, policy enforcement, automation and workforce management to the Food and Beverage industry in a single platform. This takes your global physical identity and access management program to the next level. Whether it's R&D, the production floor, QA/QC, clean rooms or beyond, Guardian has got you covered.



The Alert Enterprise Solution.

Alert Enterprise Guardian, an AI-powered platform for physical identity and access management, is used by numerous Fortune 500 companies worldwide. Here's why customers select Guardian:

- Highly flexible platform to digitally transform the entire hire-to-terminate lifecycle for employees, contractors and visitors deeply integrated with your existing physical access control systems and extended ecosystem relating to workplace access
- Automate governance, risk and compliance relating to your physical identity & access management program
- Powerful insights driven on AI and Machine Learning
- Tools to aid compliance and automation of controls for **GMP, FDA, CFR, EMA, ISO, GDPR, NIST, UK GOV DCA**
- Elevated critical business processes around identity and access management/governance in an integrated solution
- Implement a single solution for cross-platform provisioning of access with converged physical and logical systems

DOWNLOAD THE SOC
INSIGHTS DATASHEET

[CONTACT US](#) | [LEARN MORE](#)

Challenges.

The following are the most common challenges faced by Food and Beverage organizations:

- Lacking an automated and dynamic process for hire-to-terminate identity lifecycle management for physical access
- Minimal automation and integration with physical access control systems like Genetec, C-Cure 9000, LenelS2, Honeywell, PACOM, etc.
- Slow access auditing & recertification processes
- Initial onboarding processes, time to be productive
- The area access request process is manual and siloed
- Lacking dynamic workflows, tooling and approval processes
- Lacking in native web app, mobile apps and plugins for other platforms like ServiceNow to maximize user adoption
- Lacking ability to apply policy in real-time for physical access
- Lacking ability to automatically detect nonconformities with SOPs, policies, regulations, SOD violations, etc.
- Lacking real-time threat profile for active identities/users to perform insider threat detection
- Lacking a dynamic visitor identity & access management process seamlessly integrated with physical identity & access management program
- Failing to achieve a frictionless workplace access experience, looking to go mobile NFC-based access



Case Study

Revolutionizing PIAM in Food Manufacturing

Food and beverage manufacturing is a high-stakes game of juggling supply chains, ensuring safety and navigating complex workforce dynamics. Imagine coordinating a massive network of suppliers and distributors while keeping a tight grip on quality and compliance at every stage of production. Now add the need to stay nimble amid market changes and workforce challenges.

For one of the biggest players in the industry, these hurdles were make-or-break for success and sustainability. Their systems needed a high-tech upgrade—one that would unify their operations, boost security and streamline compliance across multiple locations and jurisdictions.

In search of a way to optimize their operations and secure their assets, the global leader turned to Alert Enterprise. We will seamlessly integrate a tailored, advanced solution with their existing systems, setting them up with an automated, future-ready infrastructure.



A Comprehensive Approach to Identity and Access Management.

The Guardian PIAM platform goes beyond traditional access control, integrating multiple facets of security, asset management and compliance to create a holistic approach that's both robust and flexible. Integrated with SAP SuccessFactors, the Guardian system ensures only authorized personnel have access to critical areas within their facilities.



Enhancing Access Control with Nedap and Genetec.

By integrating with Nedap's access control system and leveraging license plate recognition (LPR) technology, our client can ensure only authorized personnel and vehicles gain entry to secure areas. The project also includes integration with Genetec Security Center, a leading security platform. This introduces even greater levels of automation and control, ensuring our client's security infrastructure is not only effective today but also ready for the challenges of tomorrow.



Asset Management and Truck Enrollment: A Game Changer for Logistics.

Having to manage over 1,000 trucks in Mexico alone, our client needed a solution that could handle the scale and complexity of their logistics operations. Alert Enterprise's asset management & intelligence solution simplifies asset tracking - and improves security - by seamlessly enrolling trucks as assets in the Guardian system, ensuring only authorized vehicles are granted access to specific areas.



Looking Ahead: The Future of Mobile Credentials.

Our client is exploring future-proofing workplace access with mobile credentials for authentication, a testament to their commitment to staying ahead of the curve. Mobile credentials provide a secure and convenient alternative to traditional badges. Access management becomes even more flexible, allowing for real-time updates and seamless integration with other systems.



Automating Badge Printing with Fargo Connect.

In a large-scale operation, managing employee and visitor badges can quickly become a logistical headache. To address this, Alert Enterprise incorporated Fargo Connect, an automated badge printing solution that integrates directly with Guardian PIAM. Badges are printed on demand, with the correct credentials and access rights already assigned, ensuring a smooth onboarding process.



Streamlining Compliance with LMS Training Solutions.

In an industry as heavily regulated as food manufacturing, compliance training is a critical component of daily operations. To streamline this process, we're implementing the integration of a Learning Management System (LMS), designed to ensure all employees and contractors are up to date with their training requirements before gaining access to critical areas. This integration simplifies training compliance and provides real-time visibility into who has completed the necessary courses.

Guardian Benefits



Visual, easy-to-use interface allows security and risk managers to make smarter business decisions



Automated policy enforcement for up-to-date training and certification



Data that goes beyond baseline documentation reduces compliance cost and active policy enforcement



Pre-built connectors provide easy integration with ERP, HR, PACS, video security and MES system

Automating Food & Beverage Security

Take the Risk Out of Your Automated Food & Beverage Production.



Advanced Threat Detection.

- AI-powered predictive analytics
- Supply chain application integration to receive transportation alerts
- Monitor warehouse access by employees and contractors to prevent material theft



Operational Risk Management.

- Monitors production processes for sabotage and malicious incidents
- Manages supply chain risks including changes to master data and transactions
- Manages the movement of goods and risks from spoilage and arrival notification requirements by FDA



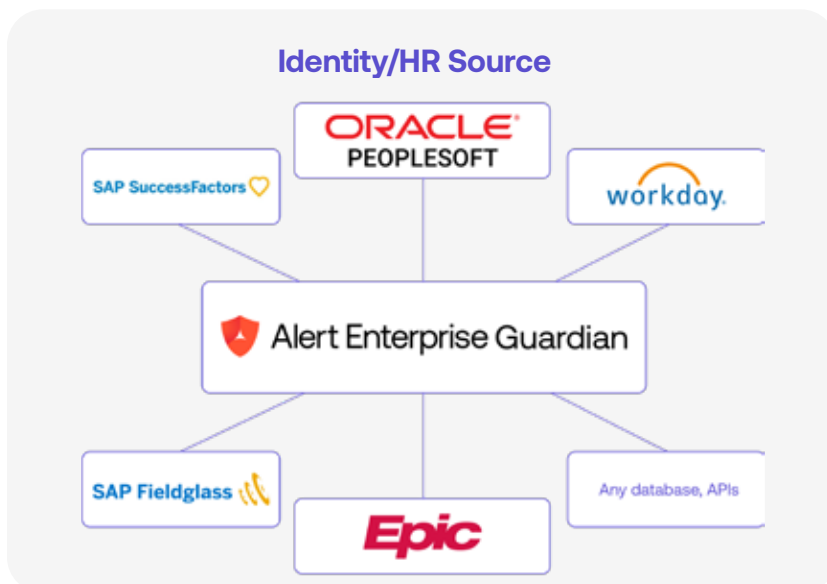
Operational Compliance Enforcement.

- Automate F&B-related regulatory compliance: Public Health Safety and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act 2002); Food Safety Modernization Act (FSMA); HSPD 9 Defense of Agriculture and Food; and other FDA requirements
- Enforcement of FDA Hazard Analysis & Critical Control Point (HACCP) Standards
- Yields streamlined conformance to ISO 22000 Food Safety Standards



End-to-Threat Visibility.


- Analyze blended threats across IT Systems, Physical Access Controls and Industrial Controls
- Rich-content situational awareness display – geospatial mapping to Google Maps, Virtual Earth
- Incident Management and Response system including pre-packaged remedial action strategies



We take care of your hire-to-retire process, too.

By integrating with HR Systems like SAP SuccessFactors, Workday, Oracle and more, Alert Enterprise software automates background checks, trainings and certifications, and risk analysis – from onboarding to offboarding. Insider risk: removed.

SEE OUR
INTEGRATIONS



Workforce Access Automation.

Alert Enterprise **Guardian** with GEN AI at its core provides a frictionless workplace access experience, that is **safe, secure and compliant**.

Here are sample use case scenarios that Guardian solves out-of-the-box:



Automated Hire-to-Retire Transformation.

Real-time integration of Guardian with leading HR systems and data lakes allows Supervisors/HR or Security Administrators to trigger a new Identity creation process (as part of onboarding) and auto-provisioning of access levels based on their role, location and access policies.

Similarly, the HR/Admins can initiate a "User Termination" workflow as part of the employee offboarding process. This triggers automated removal of identities and access levels across all connected systems.



Access Management.

Guardian integrates across various enterprise applications, physical facilities and critical assets including leading platforms like Genetec, Lenel, C-Cure 9000, Honeywell, AMAG, etc. This empowers the system users and managers to view/request access for themselves or others in the organization, and audit if the same access was granted via an established standard.

Admins/Users can create a new request (via a self-service portal) to add/remove specific access, either for themselves or others. These requests are sent for single or multi-step approval and auto-provisioning (once approved) based on the security needs. Contractor user access review is performed on a quarterly basis or as required by compliance. Guardian can be configured to deactivate a badge after a configurable number of days of inactivity.



Asset Governance.

The Guardian platform provides Asset Inventory Management for various asset types like metal keys, gate openers or other high valued assets, that can be assigned to individual employees.

The self-service portal (with SSO/AD) is fully capable of requesting assets, and the necessary approval process can be configured to record approvals and the chain-of-custody, end-to-end lifecycle of these assets.



Report Generation.

Multiple compliance standards require both physical and logical access to be reviewed every 90 days. Alert Enterprise Guardian is capable of generating reports required for periodic reviews (daily, weekly, monthly, etc.) and ad-hoc reviews consisting of identities that are active, inactive and pending for approval, training, etc.

Guardian integrates with other IT, HR, Cybersecurity, Learning Management and Ticket Management systems to generate reports that provide a unified view of threats across the enterprise, and deploy rules-based solutions to prevent malicious acts, sabotage, terrorism and cyber threats.



Anomaly & Insider Threat Detection with AI.

Guardian tracks employees' requests to access a new facility or area for themselves or another person, which enables the security personnel to correlate staff entry into sensitive locations with business reasons and prior access patterns.

AI-powered anomaly detection, like a badge swipe at off-shift hours, piggybacking and multiple access denied attempts, can be enabled for critical resources to reduce the risk from insiders. By enabling convergence between physical and logical security systems, the solution can gather and provide security intelligence from a number of sources and systems.

The AI policy engine also helps in detecting noise/duplicate alarms and provides only the qualified alarms for security teams to address. The alarm response dashboard can be an external application like ServiceNow, Splunk or others. The connector framework will help push these qualified alarms to any system.



Enforcement of Compliance Standards.

Alert Enterprise Guardian delivers GEN AI-powered enterprise-wide security, governance, compliance, policy enforcement, automation and workforce management to the Food and Beverage industry in a single platform, taking your global physical security identity and access management program to the next level. Whether its R&D, the production floor, QA/QC, cleanrooms and beyond, Guardian has got you covered.

Similar governance can be performed on a need basis for contractors or temporary employees, with automatic alerts sent when there is a change in status for individuals, the ability to track the approvals and revocations.

For access requests and approvals, Guardian automatically checks security policies and documents compliance with requirements that verify who approved access to which facilities and for what duration of time. It also enforces the Segregation of Duties (SOD) which avoids access requests being self-approved.



Syncing Across Multiple PACS.

Guardian connects with multiple Physical Access Control Systems (PACS) to manage physical access to critical facilities - from one place. It takes the guesswork out of approving access to physical locations or applications based on specific roles within the organization.

This enables the security staff to remove physical access to systems and facilities with a single click and invoke mitigating controls like additional video surveillance or proximity tracking.



Visitor Management System.

Alert Enterprise Visitor Management System provides Corporate Security with enhanced control of visitor access and enforces security standards. All of the platform features related to workflow, notification, compliance and PACS integration are available for visitor scenarios as well.

Following are the common use cases which are available out-of-the-box:



Streamline Visitor Registration Process.

The Visitor Management System can be deployed as a Kiosk (self-service) or Lobby (managed service) setup. The visitor registration process can be streamlined by providing a pre-registration workflow and enhanced by integrating with local or federal banned lists.

Access points are managed and locations are secured in a granular manner using a centralized management process. The solution provides front desk and security teams with streamlined, robust and secure processes for validating a visitor's identity.



Audit All Visitor Logs.

The Visitor Management System maintains logs that report on who visited a facility, who approved their visit, how long they stayed and which areas within the facility visitors were allowed to access. This provides the ability to conduct an audit and enhance search capabilities.



Establish Visitor Escort Compliance Requirements.

The system enforces strict compliance standards when the visitor is requesting access to critical facilities. The access request form lists the expected time to check out as a mandatory field.

The solution triggers escalation emails when the visitor is not checked out after a certain number of hours (configurable). If the visitor is not checked out after 24 hours (configurable), VMS triggers an email to ESOC.



Automate Background Checks.

Upon visitor registration, the Visitor Management System performs an automated background check, using the visitor's ID or driver's license information against a set of watch lists (BOLO, do-not-enter, etc.).



Identify and Notify All Visitors in the Facility.

The system solution provides a single interface for accurately identifying all the visitors in a facility and notifying them in case of an emergency. This offers a holistic view of building occupancy at any given time.

[DOWNLOAD THE VIM DATASHEET](#)

[CONTACT US](#) | [LEARN MORE](#)





Alert Enterprise

How Alert Enterprise Leverages Technology So Food & Beverage Organizations Can Maintain Continuous Compliance.

- Extends access management and risk analysis beyond IT applications to include physical access control systems
- Creates a unified access and reporting mechanism across applications in all domains (IT, Physical Access Control Systems, SCADA)
- Establishes an all-encompassing strategy for onboarding/offboarding related to access management, managing contractor access as well as validation of certification and background checks
- Offers holistic business alignment for security risk and compliance posture alignment

[READ ABOUT OUR CUSTOMER SUCCESS](#)

[CONTACT US](#) | [LEARN MORE](#)