LEIDOS NETWORK MANAGEMENT SOLUTION

Our MOSAIC open architecture network management solution connects your operations to the screening devices, transforming historically disparate operational data into security information. This link of security system data unlocks a new paradigm in operational functionality with enhanced data access, cybersecurity protection, central image processing, remote access, user management integration, life cycle management, system configuration, maintenance support, and rapid response in the race against emerging threats. Leidos is bringing forth a new era of totally integrated security solutions.

Opening the system architecture, using web based services, enterprise solutions, modern containerization management, and API integration, provides a flexible service model to integrate not only the Leidos portfolio, but also any sensor or third-party product allowing the desirability of choice by our clients. MOSAIC allows turnkey solutions across the entire customer campus and remote locations with enterprise level scalable and purposeful security efficient management services. This concept of open system connectivity, elasticity, and resilience forms the core of our network solution. Each cohesive device performs its critical functionality without reliance on the network services making security screening a highly available operation. The result is an efficient, modern, and totally integrated system that translates directly to a secure, positive, passenger experience.

FOR MORE INFORMATION
Leidos.com/Security-Detection
Intuitive Visualization
- Business Intelligence Dashboards
- Common Data Services and Formats
- Real-Time Monitoring
- Modular Component Streams
- Open Access to System Data
- Combined Device Reporting

Vital Core Services
- Resilient Design of Critical Screening Functionality
- Elastic Scalability to System Demand
- Loosely Coupled Event/Action Engine
- Cohesive Component Operation
- Cyber Secure

Operational Efficiency
- Open Architecture Design
- Extensible Integration of New Devices
- Integrated User Management
- Single Management Information System Access
- Standards Based and Vendor Agnostic Formats

OPEN. SEAMLESS. CONNECTED.

SIMPLIFY THE USER EXPERIENCE
- Reduce number of data stores and provide easier, more reliable access to data
- Access to real-time data
- Provide a common user interface for all OEM systems
- Integrate all decision making data
- Increased interoperation between systems
- Improve user management functions

IMPROVE OPERATIONAL CAPABILITY
- More efficient resource distribution
- Improve information sharing & leverage domain experts
- Improve leadership situational awareness
- Decrease operational costs
- Increase resiliency of critical infrastructure
- Interfaces to external systems
- Improve operational availability
- Improve life cycle management practices

INTEGRATE CYBER SECURITY
- Compliance to Cybersecurity standards
- Zero trust based design
- Adheres to cybersecurity standards
- Strict audit and information integrity monitoring
- Secure hardware protections
- Secure access controls
- Secure network communications