L3HARRIS™
FAST. FORWARD.

# CYBERSECURITY SOLUTIONS

Comprehensive VIDA System Protection

# SECURE YOUR CRITICAL COMMUNICATIONS

No organization is safe from cyber attacks. At the turn of this decade, the FBI reported approximately 1,500 ransomware cases*, with threat frequency and methods growing each year. This results in billions of dollars lost due to network downtime, work disruption and recovery of critical data. Vulnerabilities will increase as organizations turn to cloud-based services to improve efficiency and inter-agency interoperability. Yet, even so-called closed networks are not safe from insider attacks or inadvertent system user actions.

For decades, L3Harris has leveraged industry-leading expertise to help protect network communications for some of the world's most security-conscious customers. Our technologies are engineered to evolve with threats and meet the industry's most stringent standards including NIST 800-53, DHS-4300, CNSS 1253 from the U.S. federal government and DoD, along with North American Energy Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) for energy generation and transmission, and International Organization for Standardization (ISO) 27001 – Information Technology – Security Techniques for international organizations.

L3Harris Cybersecurity Solutions provide the system updates you need to increase peace of mind against the constantly evolving landscape of security threats.

* https://pdf.ic3.gov/2018_IC3Report.pdf

> **Cybersecurity Assessment**
System evaluation by cybersecurity engineers to identify vulnerabilities, follow industry best practices and develop a plan for ongoing security enhancements

> **Security Update Management Services (SUMS+)**
Efficient operating system security patch deployment and management

> **VIDA® Secure Sentry**
Maintains compliance with government-adopted STIGs

# END-TO-END PROTECTION

**L3Harris Cybersecurity Solutions deliver the latest technologies, maintenance and processes to keep organizations effective and vigilant against cyber threats.**

### CYBERSECURITY ASSESSMENT

Connectivity to other communications systems and cloud-based solutions improves interoperability but adds security attack vectors. L3Harris cybersecurity engineers will evaluate your system and make recommendations to minimize risk and help maintain the integrity, confidentiality and availability of networks. This includes an assessment of system vulnerabilities, compliance with the latest industry best-practices, an analysis of system logs and alerts and a comprehensive evaluation report, which provides a roadmap for ongoing security enhancements.

### SUMS+

Updating multiple operating systems can be risky with constantly evolving software vulnerabilities. SUMS+ delivers peace of mind and added security with an automated software patch process. This includes simultaneous acquisition, testing and distribution of multiple patch policies to eliminate significant management overhead.

The SUMS+ automation agent continuously monitors and reports endpoint states, including patch levels, to a management server. The agent also compares endpoint compliance against defined policies, such as mandatory patch levels. This allows organizations to quickly identify and distribute needed updates to Windows®, Linux® and VMWare® operating systems without the need for domain-specific expertise. SUMS+ will confirm successful installations and update servers in real time.

## METHODS OF ATTACK

**Probing and Scanning for Network Vulnerabilities**

- Scanning to detect open ports
- Enumerating to access network contents including user accounts and files
- Exploiting publicly-known vulnerabilities and exposures in system software

**Sniffing and Eavesdropping**

- Intercepting network traffic during transmission

**Malicious Coding and Malware**

- Ransomware and other code designed to cause damage to a computer, server, client or network

**Denial of Service**

- Flooding of internet traffic from a variety of sources to deny service to a targeted server

**Spoofing**

- Gaining system access by disguising a communication from an unknown source as being from a known, trusted source

**Password Cracking**

- Gaining access to accounts and resources by guessing or recovering a password from stored locations or from data transmissions

**Man-in-the-Middle**

- Attacker secretly inserts itself between client and server to relay and possibly alter communications between two parties who believe they are directly communicating with one another

# HARDEN CYBERSECURITY DEFENSES

**Organizations can lower network risks with L3Harris VIDA® Core security solutions.**

## VIDA® Secure Sentry

VIDA® Secure Sentry adds another level of protection through quarterly releases of publicly-available, government-adopted Security Technical Implementation Guides (STIG) and vendor-released patches addressing Common Vulnerabilities and Exposures (CVEs). STIGs are a collection of recommended setting and controls.

L3Harris applies this guidance to test updates on the VIDA® system, providing compatibility with applications prior to making VIDA Secure Sentry releases, with the highest priority CVEs addressed as necessary in interim releases.

L3Harris Cyber Security Assessment, SUMS+ and VIDA® Secure Sentry are available as part of our Infrastructure Managed Services Plan.

## Compare

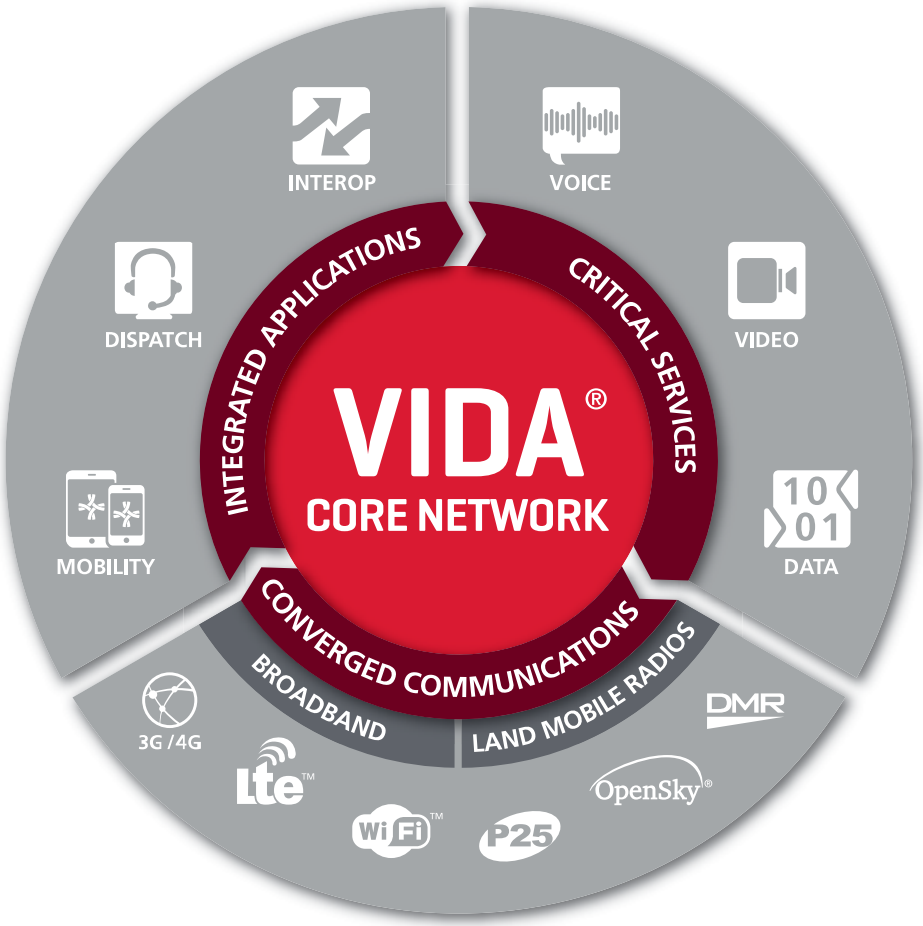
Select the plan that works best for your organization, your budget and your resource strategy. We're here to fully discuss the options or create a custom plan that meets your needs.

| | Service Assist | Service Partner | Service Managed |
|---|---|---|---|
| **Premium Technical Support (PTS)** | ✔ | ✔ | ✔ |
| **Security Update Management Services+ (SUMS+)** | ✔ | ✔ | ✔ |
| **Software Managed Services (SMS)** | | ✔ | ✔ |
| **SMS Installation** | | ✔ | ✔ |
| **Standard Repair Services** | Available option | Available option | ✔ |
| **Annual Preventive Maintenance** | | Available option | ✔ |
| **SUMS+ Installation** | | Available option | ✔ |
| **Planned Network Upgrades** | | Available option | ✔ |
| **On-Site Corrective Maintenance** | | Available option | ✔ |
| **Obsolescence Protection** | | | ✔ |
| **Enhanced Annual Preventive Maintenance** | | | ✔ |
| **Network Operations Center (NOC) Monitoring*** | | | ✔ |
| **Rapid Response Service Level Agreement (SLA)** | | | ✔ |
| **Cybersecurity Assessments** | | | ✔ |
| **System Administration** | | | ✔ |
| **VIDA® Secure Sentry** | | Available option | ✔ |
| **VIDA® Secure Sentry Installation** | | Available option | Available option |
| **On Demand Services** | Available option | Available option | Available option |

*Enhanced and custom services available

# ADD MORE LAYERS TO YOUR SYSTEM'S SECURITY

**These L3Harris VIDA Core solutions can be customized to each organization's needs.**




> **Disaster Recovery**
Unitrends NCM delivers instant recovery and automated system failover

> **RPM2 with Advanced Access Control (AAC)**
The AAC administers authorization policies for users programming radios with RPM2 to help keep unauthorized radios from being programmed to access your system

> **Session Auditing**
VIDA uses Centrify to detect and report suspicious user activity in real time. It also monitors and controls privileged sessions to leverage shared and individual accounts with full metadata logging

> **Network Security**
A Cisco® ASA Firewall with FirePOWER™provides intrusion detection and prevention. Link encryption, Layer 3 switching and network monitoring support additional controls on the VIDA network

> **Link Layer Authentication**
Restricts unlicensed users from accessing data systems by requiring networks to authenticate each user and users to authenticate the systems when it registers

> **Host Security – McAfee ePO/Host Intrusion Detection System**
Detects and rejects known attacks and malware and reports back to the ePolicy Orchestrator for policy enforcement

> **Centralized Log Management**
Splunk® Enterprise collects event data within the VIDA® network and allows searching the log's information from a single dashboard

> **Access Control**
Prevents disclosure of information to unauthorized parties and provides mutual authentication for web services employing the VIDA Windows® Active Directory and Certificate Authority

> **Key Management Facility**
P25 standard AES and DES encryption secures voice and data and includes support of the P25 standard Inter-Key-Interface to securely share keys between systems

> **eData Gateway**
Application secures User Location data with no additional VIDA hardware required

# FAST. FORWARD.

**Cybersecurity Solutions**



**Non-Export Controlled Information**

L3Harris Technologies is an agile global aerospace and defense technology innovator, delivering end-to-end solutions that meet customers' mission-critical needs. The company provides advanced defense and commercial technologies across air, land, sea, space and cyber domains.

L3HARRIS™