L3HARRIS®

XL Virtual™ Security

Cybersecurity for Critical Communications Systems

L3Harris Technologies, Inc.

TABLE OF CONTENTS

XL Virtual™ Security 3
Summary 3
Essential Security Requirements 3
Client and Application Security 4
Authentication Schemas 4
End-to-End Encryption 4
Over-the-Air Rekeying (OTAR) 4
Data Security (Data At Rest) 4
Airlink Encryption 4
Personally Identifiable Information (PII) Protection 5
Event History Retention Controls 5
Network Security 6

LIST OF FIGURES

Figure 1: XL Virtual Network Infrastructure 3
Figure 2: Scalable Hosted/Integrated Solution 6
Table 1: Cybersecurity Controls 7

XL Virtual™ Security

Cybersecurity for Critical Communications Systems

SUMMARY

IP-based technologies are prevalent in wireless communications systems now more than ever. This offers flexibility, broader practical use case scenarios and greater economies of scale. Other benefits include a common backbone and infrastructure, commercially available standardized products, common support and maintenance and adaptability to emerging technologies.

As critical communications systems connect with enterprise environments, evaluating the agency's needs is crucial. Interoperability can increase exposure and risk, so stringent cybersecurity controls are implemented through a Defense-in-Depth strategy in designing the XL Virtual™ system.

L3Harris recognizes the importance of cybersecurity for wireless and enterprise IP-based systems. The following sections outline the key requirements and cost-effective solutions to meet these security needs.

ESSENTIAL SECURITY REQUIREMENTS

The XL Virtual network infrastructure and client applications fully integrate with L3Harris Land Mobile Radios (LMR) and leverage the enhanced data capability of LTE to provide Push-to-Talk (PTT) services to users on both commercial and private broadband networks, including Long-Term Evolution (LTE) networks.

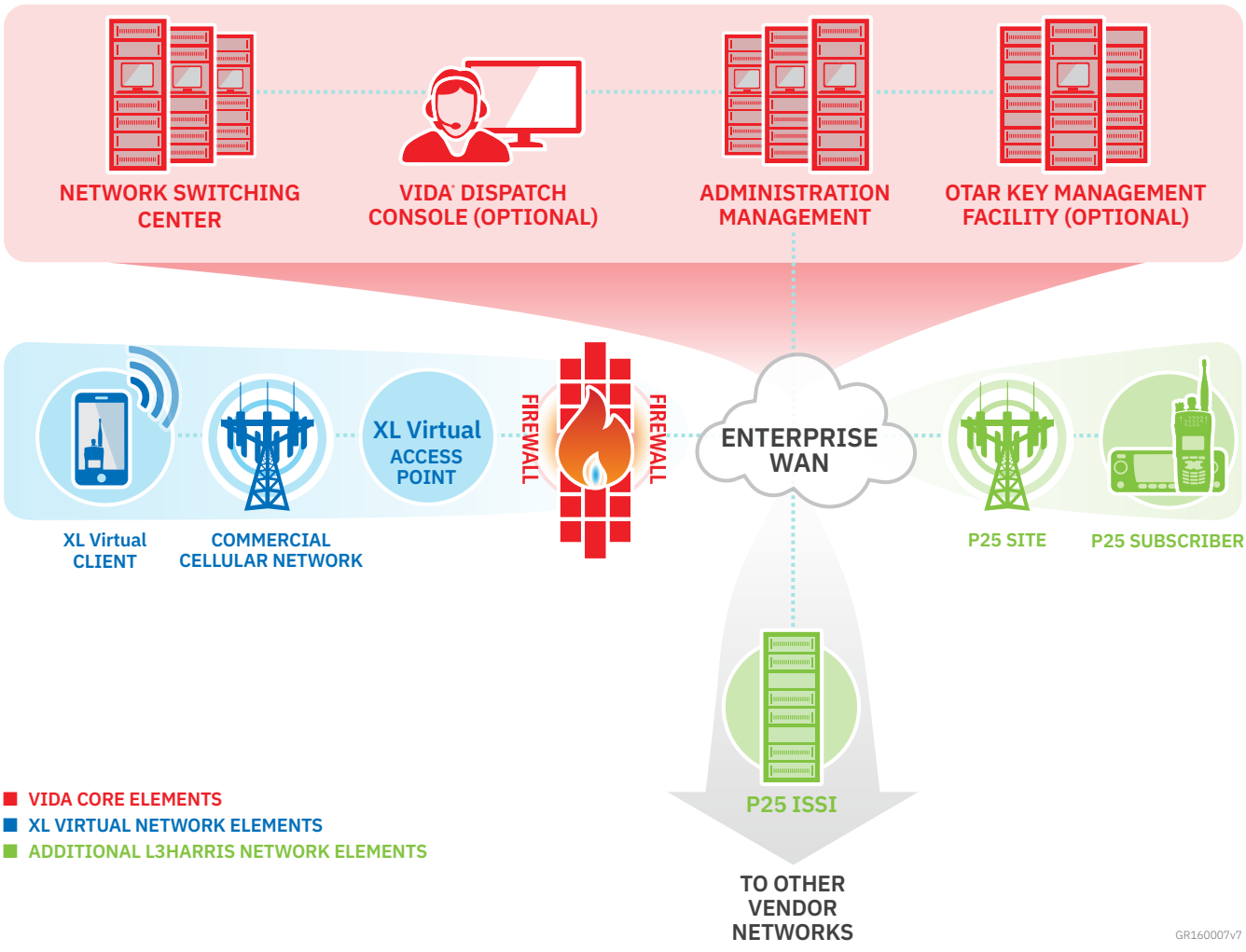

Figure 1: XL Virtual Network Infrastructure

CLIENT AND APPLICATION SECURITY

AUTHENTICATION SCHEMAS

The XL Virtual Push-to-Talk (PTT) communications app offers password protection at both the system and application levels. It utilizes a discretionary access control model, ensuring that these two types of protection are mutually exclusive. The application password is distinct from the administrator-issued Voice, Interoperability, Data and Access (VIDA®) password, as well as from the device password. A system administrator can define password storage options for the entire system on the device.

User authentication by the system may optionally use credentials generated by a Key Management Function (KMF) using the same mechanisms as TIA-102 Link Layer Authentication.

End-to-End Encryption

XL Virtual supports TIA TR8.8 P25-compatible Advanced Encryption Standard (AES) end-to-end voice encryption. XL Virtual clients can make encrypted calls to individuals or talkgroups that include standard Project 25 (P25) radios, consoles or other XL Virtual clients in the same crypto net (two or more end users who share an encryption key that they use to communicate with each other). Voice payload is encrypted end-to-end (Phone-Phone/Phone-Radio) using the same module as the P25 radio.

The universal encryption key is manually loaded initially; encryption keys can be subsequently changed over-the-air using a Key Management Facility.

Over-the-Air Rekeying (OTAR)

XL Virtual supports TIA TR8.8 P25-compatible rekeying. This feature enables a crypto officer to remotely rekey devices over the air.

Data Security (Data At Rest)

On devices that support application partitions, all personally identifiable data is stored in the application partition. This includes contact lists, group lists, settings and so on.

Airlink Encryption

The Airlink encryption feature encrypts all data and signaling between the XL Virtual client and the XL Virtual access point in the network using the Datagram Transport Layer Security (DTLS) protocol. XL Virtual contacts are retrieved using Transport Layer Security (TLS). The same cipher suites are used for both DTLS and TLS: LS_RSA_WITH_AES_256_GCM_SHA384 for Android and the XL Virtual Windows® Client and TLS_RSA_WITH_AES_256_CBC_SHA for iOS.

The feature supports either an authority-issued, customer-installed certificate or a customer-generated certificate.

A customer-generated certificate requires installing the public key on each XL Virtual client device using standard client device operating system mechanisms, such as email, device management push, HTTP key file download or side-load. The Airlink encryption feature can be enabled or disabled on a system-wide basis.

Personally Identifiable Information (PII) protection

Contact list information will not be stored in permanent storage outside the VIDA core and will be transferred securely via TLS or equivalent protocol to the client. Once on the client, data is stored in a separate user-storage area where supported.

Event History Retention Controls

A system-wide administrator option controls retention of on-client event history, including voice recordings.

NETWORK SECURITY

A comprehensive Defense-in-Depth security strategy is employed throughout XL Virtual's security architecture to include the U.S. Department of Defense Unified Capabilities Approved Products List (DoD UC APL) and/or Common Criteria (CC) tested security controls (i.e., firewalls, Intrusion Detection System (IDS), whitelisting, system hardening, auditing, virtualization, change management, fault tolerance and backup).

NAT (Network Address Translation) is implemented for XL Virtual to reduce network transparency and is implemented on external connections facing the customer premise or the internet. NAT is permitted and enforced only on specific ports relative to XL Virtual.

Implicit permit ingress/egress Access Control Lists (ACLs) are applied on the premise firewall for all traffic on the outside interface.

Additionally, implicit access rules are defined in a Demilitarized Zone (DMZ) to only permit required traffic between XL Virtual and VIDA applications. The XL Virtual solution is hosted in a DMZ of the VIDA Network with a robust security protection profile. Computing and network components have DoD Security Technical Implementation Guides (STIG) applied at Mission Assurance Category (MAC-2)/ sensitive levels.

The following diagram is a high-level proposed concept design for a scalable, hosted/integrated solution.

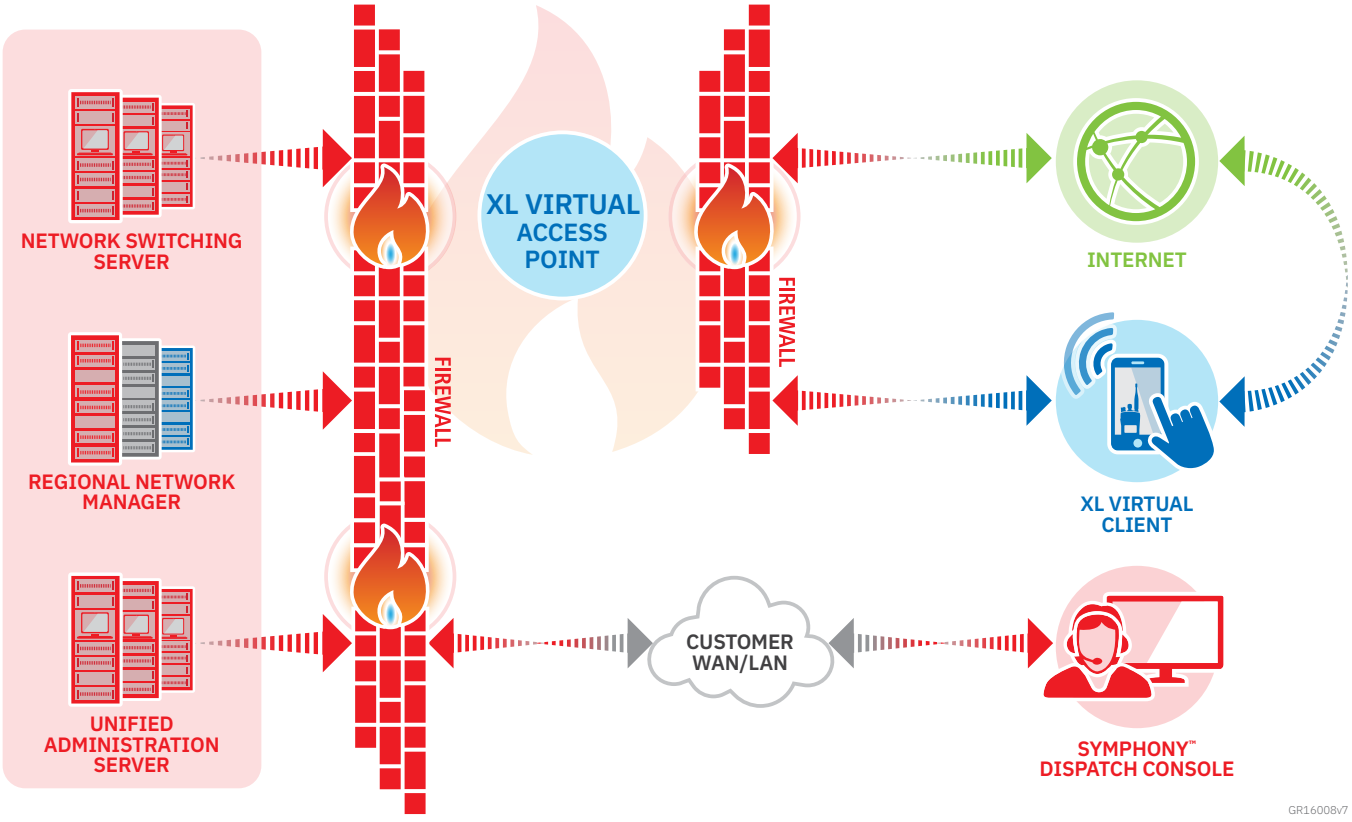

Figure 2: Scalable Hosted/Integrated Solution

INHERITED CYBERSECURITY FRAMEWORK

XL Virtual operates within the same secure framework as the hosting APCO P25 LMR system. The following cybersecurity controls are inherited directly from the LMR environment, ensuring consistent protection across both platforms.

SECURITY CAPABILITIES	DESCRIPTIONS
Access Control	› Active directory services › Certificate authority › Centralized logging of system level and security events › Two-factor authentication (Quest Defender)
System Hardening	› Apply baseline security controls on network and system components, including servers, workstations and network routers › Remove unused services, daemons, unnecessary rights from user and service logins › Configure secured web browsers › Utilize secured remote administration tools › Apply the latest third-party security patches
Software Update Management Server (SUMS)	› Automated patch management platform
Host-based Intrusion Protection System (HIPS)	› Threat detection at server and workstation levels › Industry-leading defense against targeted attacks, spyware, rootkits › Zero-day attack security via Trellix Endpoint Security Threat Prevention › Signature, anomaly and heuristic analysis available for the installed hosts
Network Intrusion Detection (NIDS)	› Monitors traffic and alerts the system administrator of signature-based violations › Collects network traffic using various network sensors › Network sensors aggregate network traffic across multiple hosts (to which the network is attached)
Disaster Recovery	› Disaster recovery with centralized backup recovery platform › Disaster recovery redundancy with cross-vaulting
Encrypted Communication Links	› Voice-traffic encryption between user devices and dispatch consoles › Application-level encryption

Table 1: Cybersecurity Controls

L3HARRIS
FAST. FORWARD.