WHITEPAPER

HARRIS®

TECHNOLOGY TO CONNECT,
INFORM AND PROTECT™

BeOn® Security

Cybersecurity for Critical Communications Systems

Peter Monnes
System Design Engineer
Harris Corporation

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

BeOn® 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 economy 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 interconnect with enterprise environments, overall agency needs must be evaluated. Interoperability typically increases an organization's exposure factor, attack surface and threat vectors that collectively increase risk. For this reason, stringent cybersecurity controls are implemented using a Defense-in-Depth strategy throughout the BeOn system design.

Harris recognizes the importance of cybersecurity to wireless communications systems and enterprise IP-based systems. The following sections identify the requirements and offerings to meet these important system design security requirements in a cost-effective manner.

ESSENTIAL SECURITY REQUIREMENTS

The BeOn network infrastructure and client applications fully integrate with Harris 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.

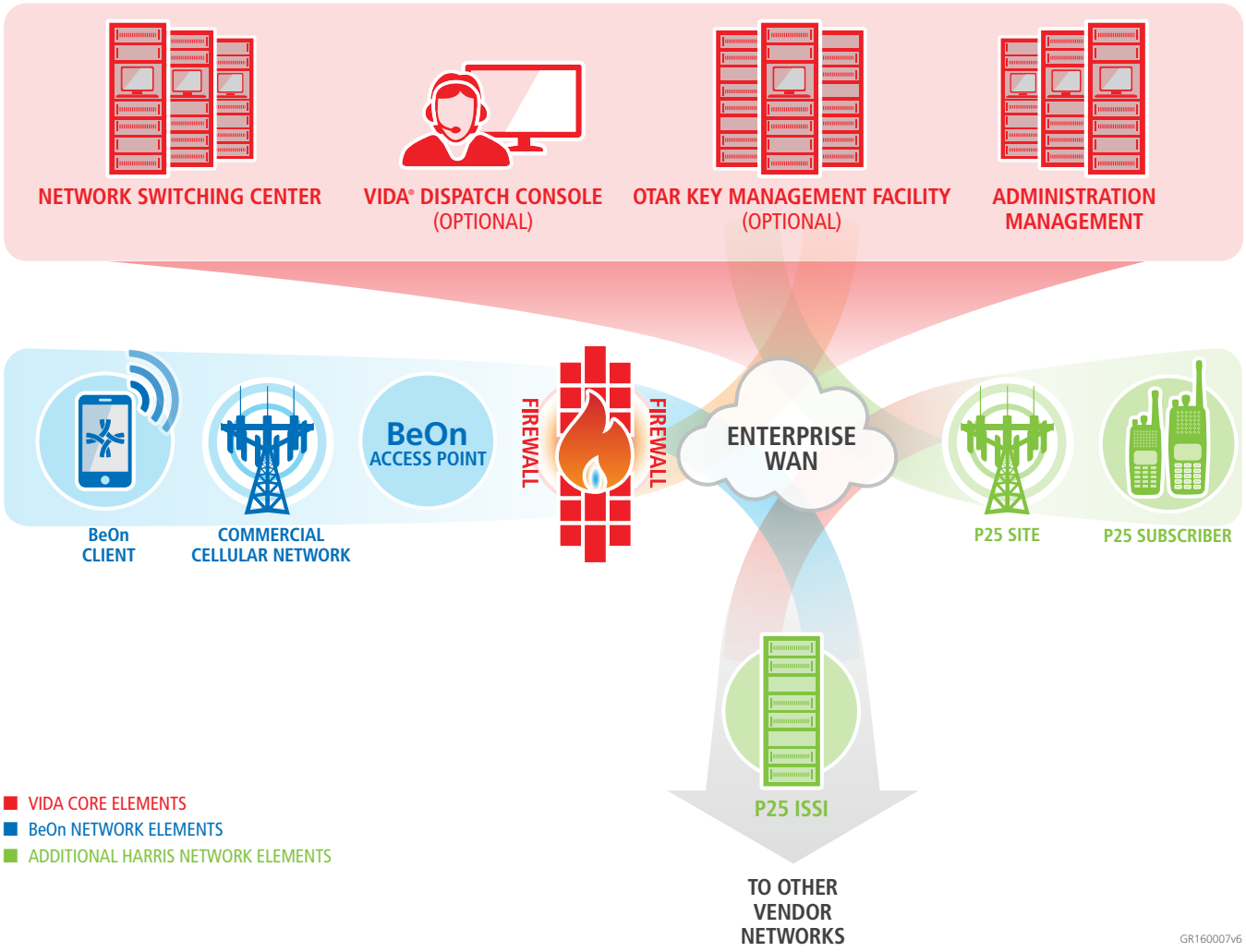

Figure 1: BeOn Network Infrastructure

CLIENT AND APPLICATION SECURITY

Authentication Schemas

BeOn® supports mutually exclusive system- and application-level password protection using a discretionary access control model. The application password is independent from the administrator-issued Voice, Interoperability, Data and Access (VIDA®) password and separate from the device password. A system administrator can specify system-wide, on-device password storage options.

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

End-to-End Encryption

BeOn supports TIA TR8.8 P25-compatible Advanced Encryption Standard (AES) end-to-end voice encryption. BeOn clients can make encrypted calls to individuals or talkgroups that include standard Project 25 (P25) radios, consoles or other BeOn 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 Federal Information Processing Standards (FIPS)-compliant module as the P25 radio.

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

Over-the-Air Rekeying (OTAR)

BeOn supports TIA TR8.8 P25-compatible rekeying. This allows a crypto-officer the ability to 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.

FIPS

The voice encryption infrastructure and algorithms used by BeOn for end-to end-voice encryption are FIPS-compliant. The VIDA encryption infrastructure and the BeOn application have achieved FIPS 140-2 Level 1 certification.

BeOn application source code has undergone independent, third-party white box security testing confirming strong coding principles and practices.

Airlink Encryption

The Airlink encryption feature encrypts all data and signaling between the BeOn® client and the BeOn access point in the network using the Datagram Transport Layer Security (DTLS) protocol. BeOn 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 BeOn 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 BeOn 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 via TLS or equivalent to the client. Once on the client, the data will be stored in separate user-storage 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 BeOn®'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 Prevention System (IPS), whitelisting, system hardening, FIPS 140-2 crypto, auditing, virtualization, change management, fault tolerance and backup).

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

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 interesting traffic between BeOn and VIDA applications. The BeOn 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.

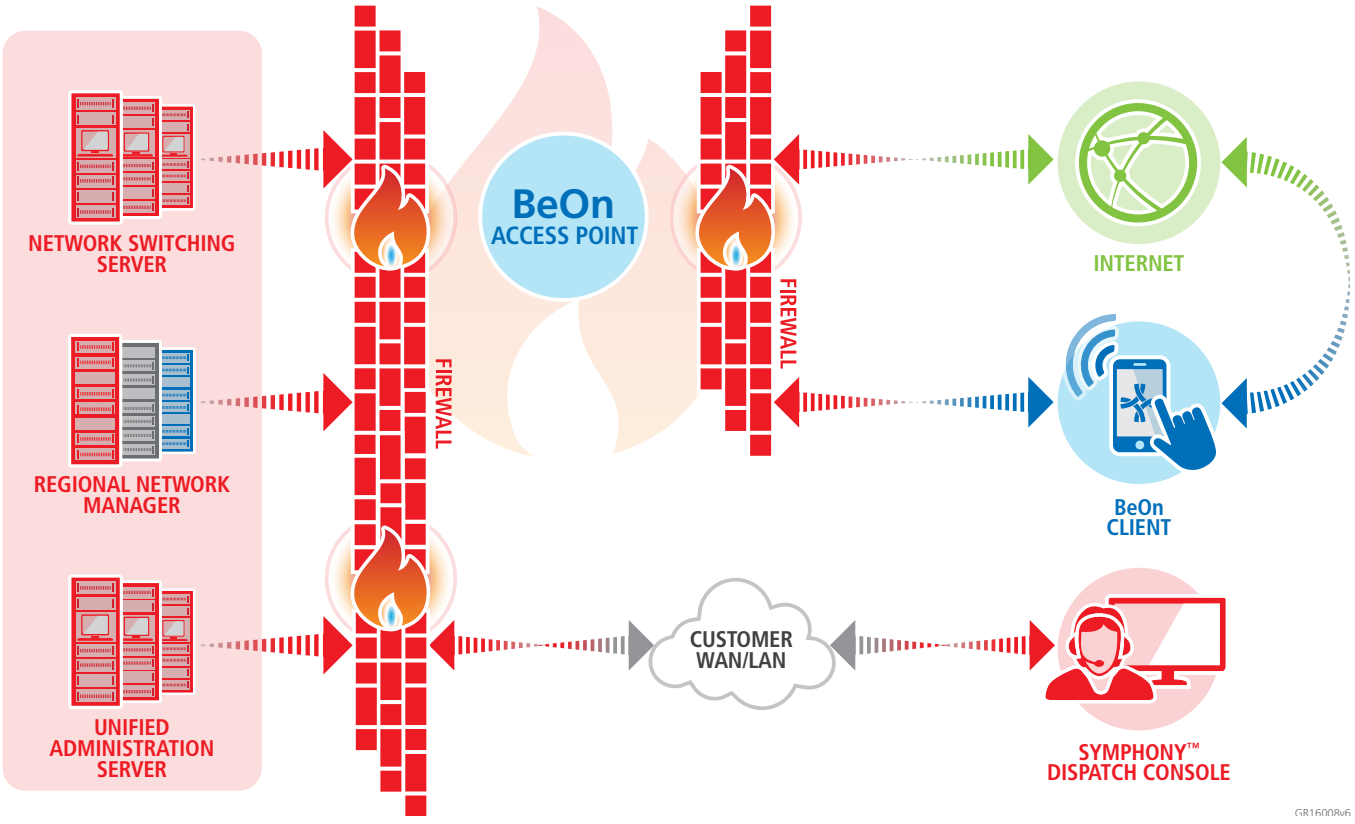

Figure 2: Scalable Hosted/Integrated Solution

Inherited cybersecurity controls implemented within the hosting LMR environments for BeOn:

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 McAfee Complete Endpoint Protection • 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

About Harris Corporation

Harris Corporation is a leading technology innovator, solving customers' toughest mission-critical challenges by providing solutions that connect, inform and protect. Harris supports government and commercial customers around the world.

Learn more at harris.com

FLORIDA | NEW YORK | VIRGINIA | BRAZIL | UNITED KINGDOM | UAE | SINGAPORE

Non-Export Controlled Information

HARRIS® TECHNOLOGY TO CONNECT, INFORM AND PROTECT™