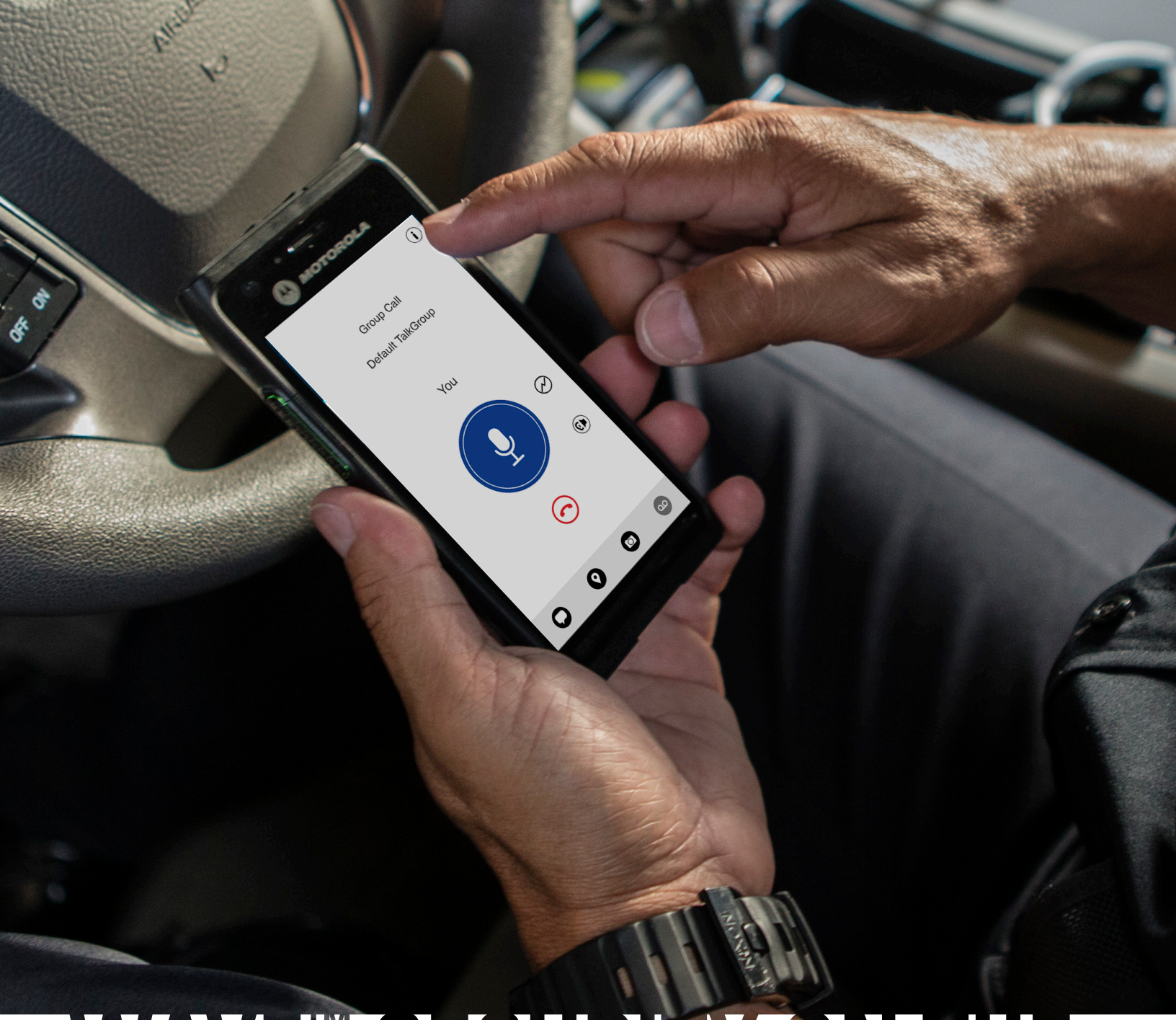


WAVE™ SECURITY ON THE MICROSOFT AZURE CLOUD

ADVANCED SECURITY FEATURES FOR WAVE BROADBAND PUSH-TO-TALK WHEN DEPLOYED ON THE AZURE CLOUD

MOTOROLA SOLUTIONS

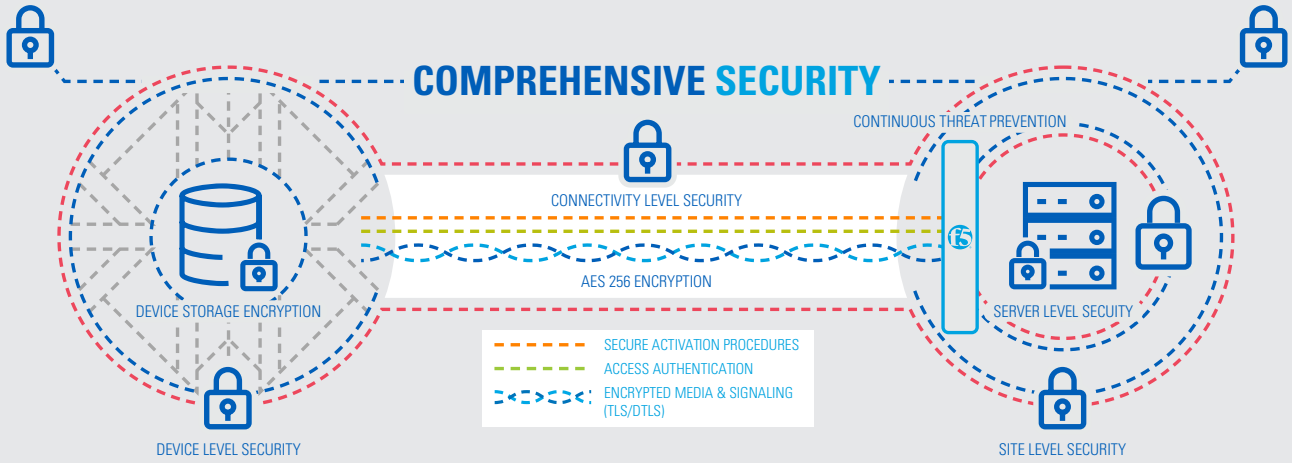
WAVE ON THE MICROSOFT AZURE CLOUD OVERVIEW

WAVE™ is Motorola Solutions' carrier-independent broadband push-to-talk service that uses the cloud to extend instantaneous private and group communication to phones, tablets and PCs. WAVE delivers the push-to-anything (PTX) communications needed to share videos, images, documents and text messages at the push of a button. WAVE also provides access to features based on the 3GPP (3rd Generation Partnership Project) Mission Critical PTT (MCPTT) standard that enhance safety, situational awareness, and operational efficiency.

WAVE provides the following key features to allow team members to stay connected at the push of a button, wherever they may be, whatever network they are using.

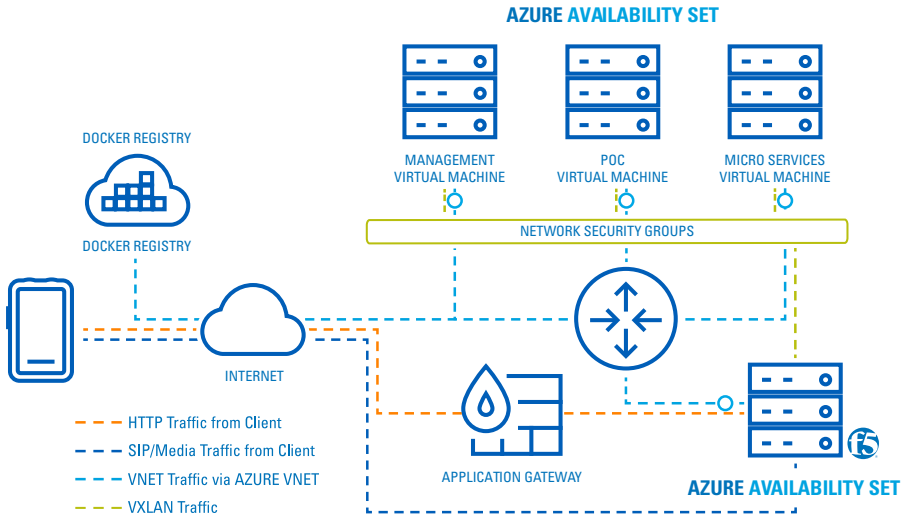
- **PTT Communications** - Fast, secure and reliable PTT voice communication at the touch of a button. Collaborate with an individual, predefined group, or ad-hoc group created on the fly.
- **Integrated Secure Messaging** – Push text, video, audio, photos and files to individuals or groups, and access the threaded history for communication details. Store and forward communication is also supported for offline users.
- **Mapping and Location** – Share your location with an individual or a group, view and track other users' locations on a map, find an address, or drop a pin on a map and share.
- **Voice Messaging** – Leave a message when a contact or group members are unavailable. WAVE will automatically deliver the message when users become available.
- **Real-Time Presence** – Set your status and see who is available with real-time presence information (Available, Do Not Disturb or Offline).

As shown in the figure below, the Wave platform security focuses on protecting data end-to-end: on the client, in-transit, and on the server.

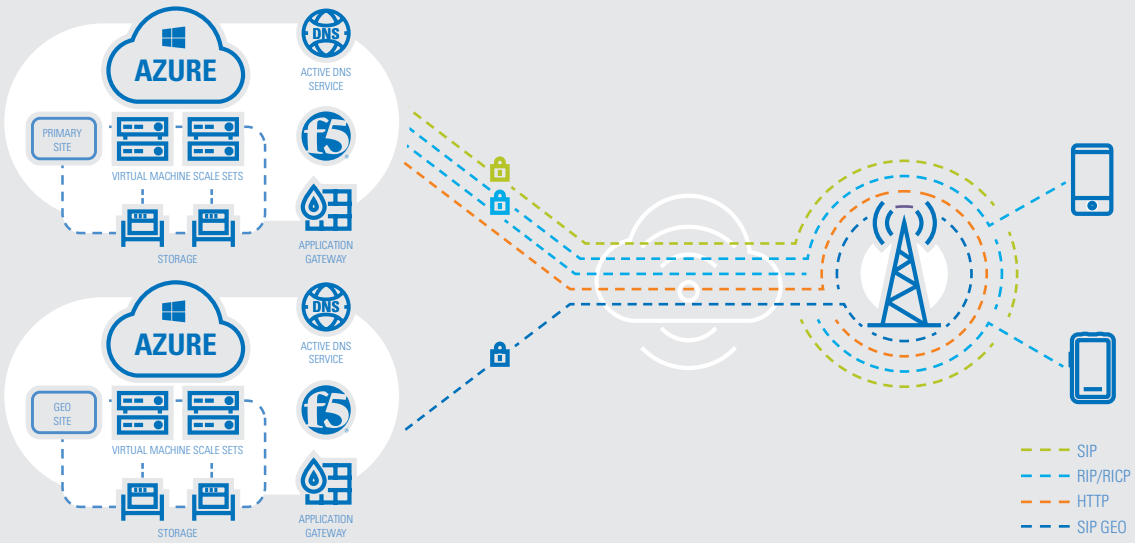


HIGH-LEVEL ARCHITECTURE

The Motorola Solutions' broadband PTT platform is built upon 3GPP standards utilizing SIP signaling, RTP/RTCP for media streaming and XML/XCAP for subscriber contact and group management. The WAVE application servers managing these sessions are housed in containers running on Virtual Machine(s) (VM) hosted in Microsoft Azure data centers as depicted in diagram below.



When communicating with the system, domain name resolution to FQDN(s) for various services is resolved through Azure's DNS Service. All session communication is encrypted and terminated on either the Web Application Firewall or an F5 acting as a Session Border Controller for SIP and media processing as shown in the image below.



IDENTITY AND ACCESS MANAGEMENT

Role-based Access Management

The WAVE broadband PTT solution on the Azure cloud has multiple types of account access: Operational VM users, Operational CMS users, Customer Care Web users (WCSR), WAVE Administration Portal users to manage customers, contacts & groups, and WAVE Web Dispatch users.

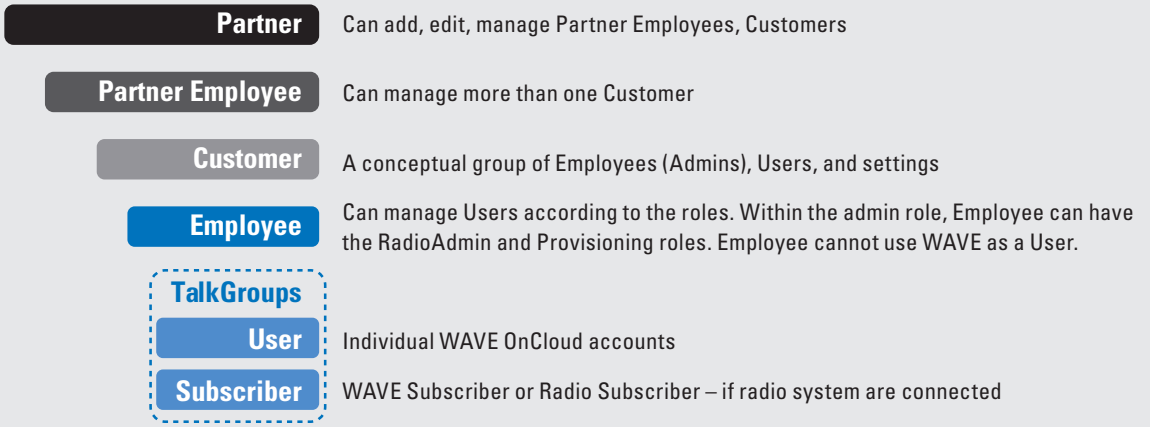
- Operational VM user accounts rely on the policies put in place through Azure's Active Directory (AD) with conditional access based on a group, location, and application sensitivity.
- CMS GUI and WCSR User Accounts have Administrator Type accounts identified for managing them. The Administrator for each account type has the capability to suspend or delete user accounts, create new user accounts, and reset user passwords. These accounts are managed/maintained by MSI operations management.
- WAVE Administration Portal user accounts to manage end customers, contacts and groups are created by MSI operations.

Subscriber Onboarding

Mobile subscribers for PTT service are provided one time activation codes from WAVE during the on-boarding and provisioning process. Activation codes are time sensitive and are sent securely over email to PTT recipients.

Multi-factor Authentication

Azure Portal administration and back-end OAM PTT application server access is protected through Azure's Multi-Factor Authorization (MFA) service and through MSI's 2-Factor and AD authentication for operational users accessing OAM VLAN ports respectively.

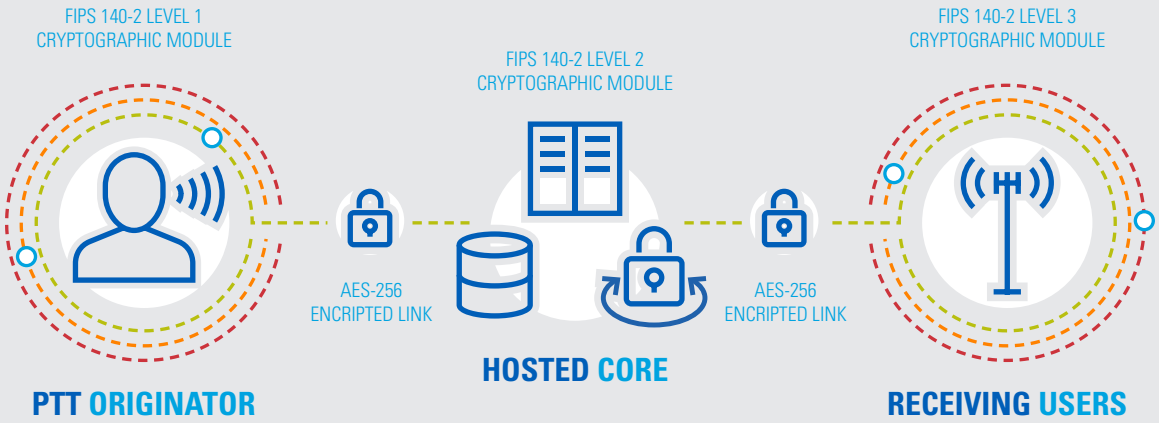


SECURING DATA IN TRANSIT

Motorola Solutions' WAVE PTT Mobile Application utilizes FIPS 140-2 Level 1 compliant cryptographic algorithms to protect users from unauthorized call interception and monitoring, as well as providing secure alerting and contact management. The WAVE application running on the device and the server negotiate the level of security supported during both signaling and media sessions.

The following security functions are supported in the cryptographic libraries of the WAVE broadband PTT application:

- All signaling, media and administration data sessions negotiate with servers using the highest level of encryption, the 256-bit Advanced Encryption Standard (AES):
  - Signaling (SIP)
  - Media (RTP/RTCP)
  - HTTPS admin data
- Authenticated Ciphers Supported:
  - AES_128_CBC_SHA
  - AES_256_CBC_SHA



PROTECTING DATA AT REST

Server Disk Encryption

Server side protection of data at rest is performed through both inherent Azure storage as well as RHEL Linux volumetric encryption. Azure Storage Service Encryption (SSE) automatically encrypts data before it is stored, and it automatically decrypts the data when you retrieve it. The process is completely transparent to users. Storage Service Encryption uses 256-bit AES encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently. WAVE takes advantage of SSE to secure configuration and operational application logs.

Disk volume encryption for OS and VM are performed using Network-Bound Disk Encryption (NBDE) which allows the user to encrypt root volumes of hard drives on physical and virtual machines without requiring to manually enter a password when systems are restarted. Server based encryption keys are stored off-cloud in a Hardware Security Module (HSM) for added protection.

Client Storage Encryption

On the device, the WAVE application uses AES-256 to encrypt all locally stored data, including secure messaging files, authentication credentials, configuration, and settings. The locally stored data can be decrypted by the application only on the specific device on which it was encrypted, and the WAVE application will not log sensitive data such as username, password, configuration values received from the server, or application configuration values.

Key Management

Coming in a future release, the keys used to authenticate sessions such as certificates and tokens or to encrypt data at rest will be centrally stored in a key management system.

PERIMETER DEFENSES

Advanced Next Generation Firewall

Check Point CloudGuard IaaS delivers advanced, multi-layered threat prevention and, in a future release, will protect WAVE PTT assets in Azure from malware and sophisticated threats. Through integration with Azure Security Center, CloudGuard will provide consistent security policy management, enforcement, and reporting.

Web Application Firewall

The Azure Application Gateway is deployed to service and secure web based connections into the PTT platform. Acting as a Web Application Firewall, the AG securely terminates HTTPS connections from mobile subscribers and protects web applications from common exploits and vulnerabilities. The WAF implementation is based on rules from the OWASP (Open Web Application Security Project).

SIP and Media Session Border Control

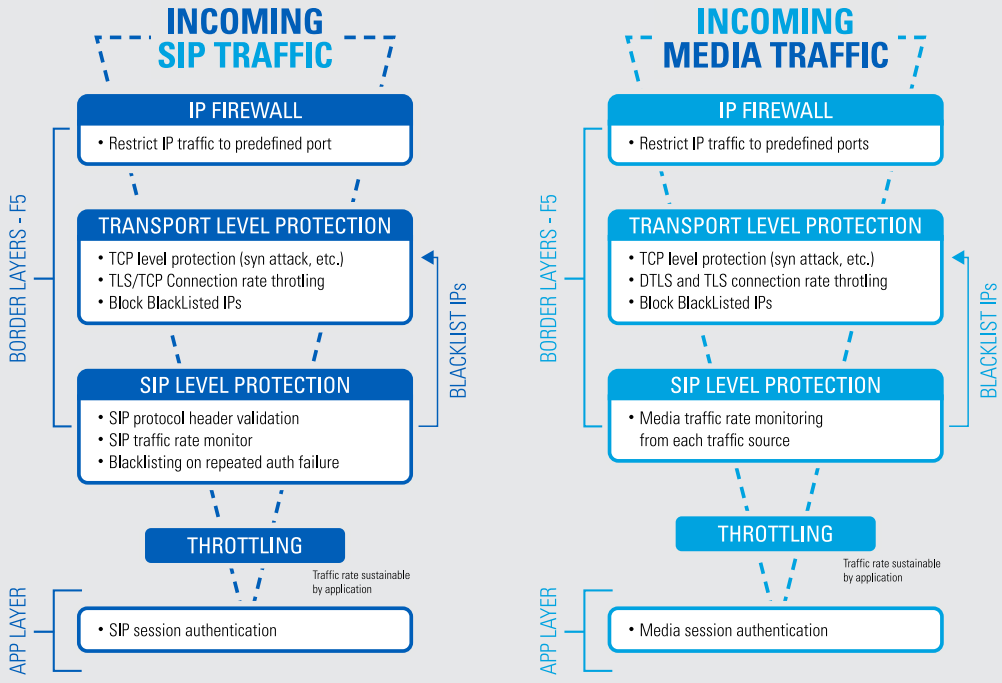
The F5 Virtual Edition acts as a session border controller (SBC) providing SSL offloading and load balancing for both SIP and media connections to the PTT backend pool member servers. In addition to terminating encrypted sessions, the F5 is configured to provide media and SIP connection throttling protection against any DOS attack.

Azure DDOS Protection

Azure basic DDoS protection, combined with application design best practices, provide defense against DDoS attacks. Automatically enabled as part of the Azure platform, the always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses utilized by Microsoft's online services. The entire scale of Azure's global network can be used to distribute and mitigate attack traffic across regions, and protection is provided for IPv4 and IPv6 Azure public IP addresses.

Network Security Groups

All sessions that traverse between VMs and containers pass through a network security group (NSG) which contains a list of security rules that allow or deny inbound or outbound network traffic based on: source or destination IP addresses, Application Security Groups, ports, and protocols. WAVE implements NSGs between outward facing WAF/SBC and inward PTT application servers. Additionally, layer 3 access control lists further restrict the flow of communication between application containers.



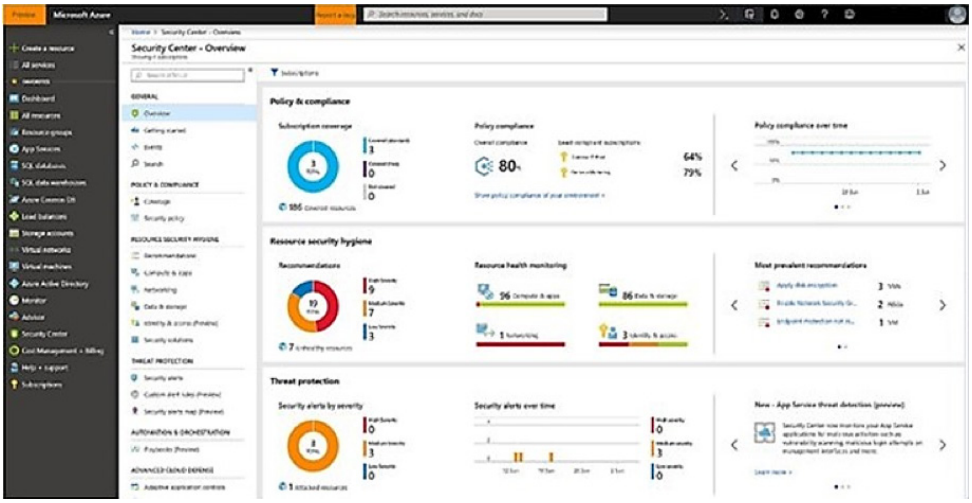
OPERATIONAL SECURITY

Security Center Overview

The WAVE broadband PTT service comes with Azure's Security Center monitoring agent installed and running on VMs providing unified security management and advanced threat protection for the PTT applications. Security Center strengthens the WAVE security posture through finding and fixing security vulnerabilities, applies access and application controls to block malicious activity, detect threats using analytics and intelligence, and respond quickly when under attack through proactively engaging MSI global operations support teams.

Incident Response

WAVE Operations processes real time alerts and notifications from Security Center and other SIEM platforms to detect, assess, diagnose and resolve security incidents which occur on the VMs, network, and PTT applications globally.



LIFE CYCLE MANAGEMENT

Software Release Cadence

The WAVE PTT server software follows two major releases per year, with minor maintenance releases in between to cover vulnerability patches, minor bug fixes, or feature enhancements.

Patching Policy

Motorola Solutions has implemented a multi-tier patching process to correct both industry vulnerabilities and vendor specific software bugs. The tiering is based on both patch criticality and specific vendor life cycle release cadence. Third-party software is further categorized as either foundational or supportive to the overall PTT solution.

For vulnerabilities, Motorola Solutions follows the 3rd party vendor's CVSS(3) mapping recommendations which are applicable to the broadband PTT system. Specifically, critical severity vulnerabilities are further reviewed by design for their applicability to the PTT applications. Those deemed not applicable are provided reasons or mitigation in a subsequent customer advisory. All other vulnerabilities are addressed through regular patching release cycles through the year based on specific vendor release cadence.

For more information, please visit us on the web at: www.motorolasolutions.com/product

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**