



**HONEYWELL
FORGE**
Cybersecurity⁺

HONEYWELL CYBERSECURITY MSS NEXT GENERATION SRA



OTD BİLİŞİM

GLOBAL VAD

AGENDA

MSS NEXT GENERATION SRA

01. MANAGED SECURITY SERVICES GLOBAL PRESENCE

02. MANAGED SECURITY SERVICES PORTOFOLIO

03. SECURE REMOTE ACCESS (SRA)

04. SRA NEW TECHNOLOGY

05. SRA ARCHITECTURE

06. SRA COMPONENTS SUMMARY



07. SRA RESOURCE REQUIREMENTS

08. PLATFORM HARDWARE



HONEYWELL MSS “**FOLLOW THE SUN**” GLOBAL SECURITY OPERATION CENTERS

24/7 Proficiency

to Reduce Operational Downtime and Lower Cyber Risk

-  Active Managed Security Service Centers
-  Future Managed Security Service Centers



-  Cybersecurity Innovation Centers & Research Labs
-  Support Centers (Atlanta, GA | Dublin, IR | Tel Aviv, IL | Dubai, UAE | Singapore, SG)



CYBERSECURITY CENTERS OF EXCELLENCE AROUND THE WORLD

HONEYWELL OT **M**ANAGED **S**ECURITY **S**ERVICES - NEXT GENERATION SOLUTION

Secure Remote Access

Designed to provide:

- Zero Trust architecture
- Multi Factor Authentication (MFA)
- Native key vault support
- Data stored at the plant level
- Availability without internet, on premise solution
- Resilient with component redundancy
- Auditing and Reporting

Patch and AV Automation

Designed to provide:

- Tested and qualified updates for Windows servers and stations
- Tested and qualified anti-malware signature file updates
- 3rd party patch delivery and automation

Cyber Care

Cyber Care for:

- PCN Hardening
- Cyber App Control
- Air-gapped AV/Patching Management
- Antivirus
- Security Devices (Firewall)

Managed Detection & Response (AMIR)

Designed to provide:

- Threat Detection and Incident Response 24x7x365
- Fully staffed Global OT-SOC
- SIEM/SOAR Platform for OT playbook orchestration
- Real-time monitoring and threat identification and notification
- Response and Remediation support
- Tabletop exercise (w/service and standalone)

Next Generation OT Services Platform (MSS)

HONEYWELL **MSS** NEXT GENERATION SRA

PROVIDED SERVICES:

Software Support

- **Asset support** – on-going support for asset management, keeping the asset configuration up to date with customer requirements
- **On-going maintenance and software support** for all MSS system components
- **Monitoring of software** (e.g., Edges and service center software to ensure it is all working correctly)

Software Installation for New Projects

- **Install, configure and test the solution** to ensure it works properly
- **User configuration** – setting up proper user access and connection restrictions to various sites/assets
- **Asset configuration** – making sure all assets/nodes are configured in system properly
- **Technical training** for system users and administrator

DELIVERED BY CYBER TEAM: MSS & CYBER PROFESSIONAL SERVICES TEAMS

MSS NEXT GENERATION SRA WHY DO WE NEED IT?

Communicated through HINTS newsletters in October:

The Honeywell Cybersecurity suite of products are entering the sunset stage. These products include:

- Forge Cyber Enterprise Core
- Forge Cyber Enterprise Premium
- Forge Cyber Site
- ICS Shield, and any other products branded as “NextNine”
- Risk Manager

The end of lifecycle dates for Forge Suite are:

- End of Sale = **December 31st, 2023,**
- End of Renewal = **December 31st, 2024,**
- End of Renewal for Performance Monitoring = **December 31st, 2024** (provided that all such subscription contracts expire/terminate –without the ability for renewal **on or before the end of 2025**)
- End of Life/Technical Support = **December 31st, 2026.**

MSS NG SRA PROVIDED SERVICES FOR NEW PROJECTS

SOFTWARE INSTALLATION

- | **Install, configure and test the solution** to ensure it works properly
- | **User configuration** – setting up proper user access and connection restrictions to various sites/assets
- | **Asset configuration** – making sure all assets/nodes are configured in system properly
- | **Technical training** for system users and administrator

SOFTWARE SUPPORT

- | **Asset support** – on-going support for asset management, keeping the asset configuration up to date with customer requirements
- | **On-going maintenance and software support** for all MSS system components
- | **Monitoring of software** (e.g., Edges and service center software to ensure it is all working correctly)

DELIVERED BY MSS & CYBER PROFESSIONAL SERVICES TEAMS

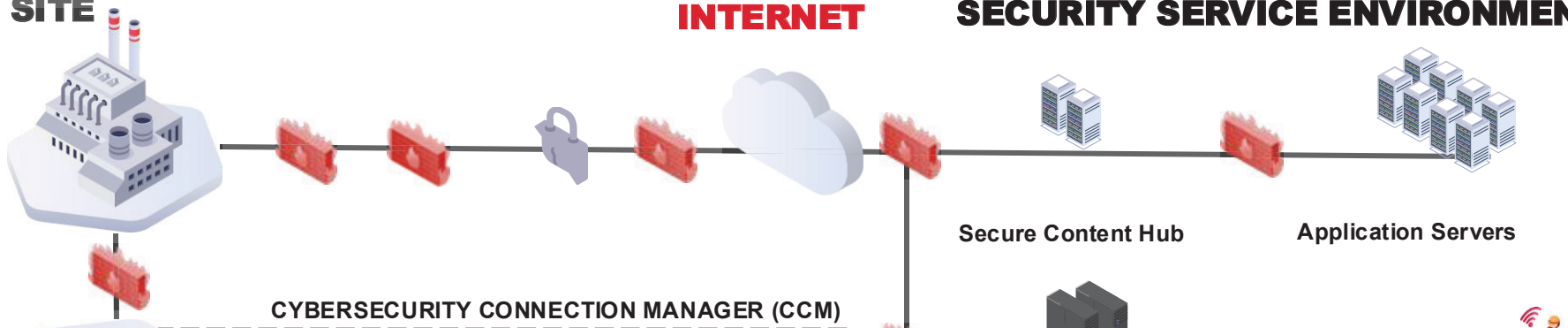
MSS NG SRA ARCHITECTURE

INDUSTRIAL SITE

INTERNET

SECURITY SERVICE ENVIRONMENT

Level 4

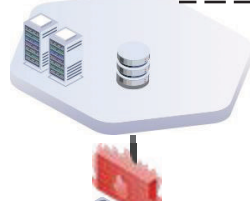


Level 3.5

eServer
Terminal Server

CYBERSECURITY CONNECTION MANAGER (CCM)

- Local Service EDGE VM
- Content Gateway VM

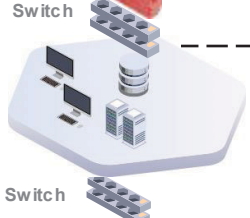


Level 3

Historian
Domain Controllers
EST / ESF
3rd Party

CYBERSECURITY APPLICATION MANAGER (CAM)

- SRA Controller VM
- AV VM
- WSUS VM



Level 2

Experion Servers
Domain Controllers
ACE
EST / ESF



Level 1

Controllers



Secure Content Hub

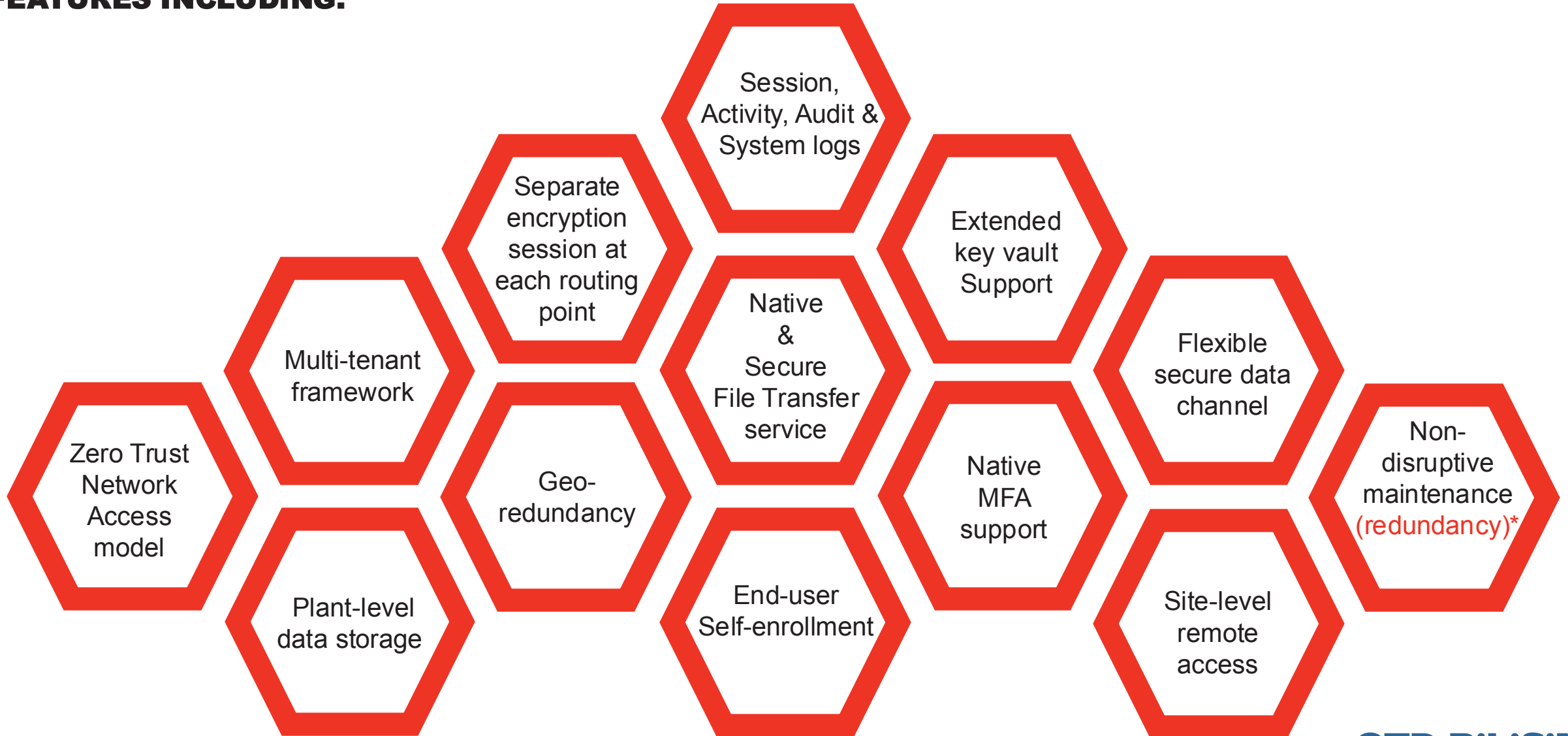
Application Servers

Geo-redundant
Global Service EDGES



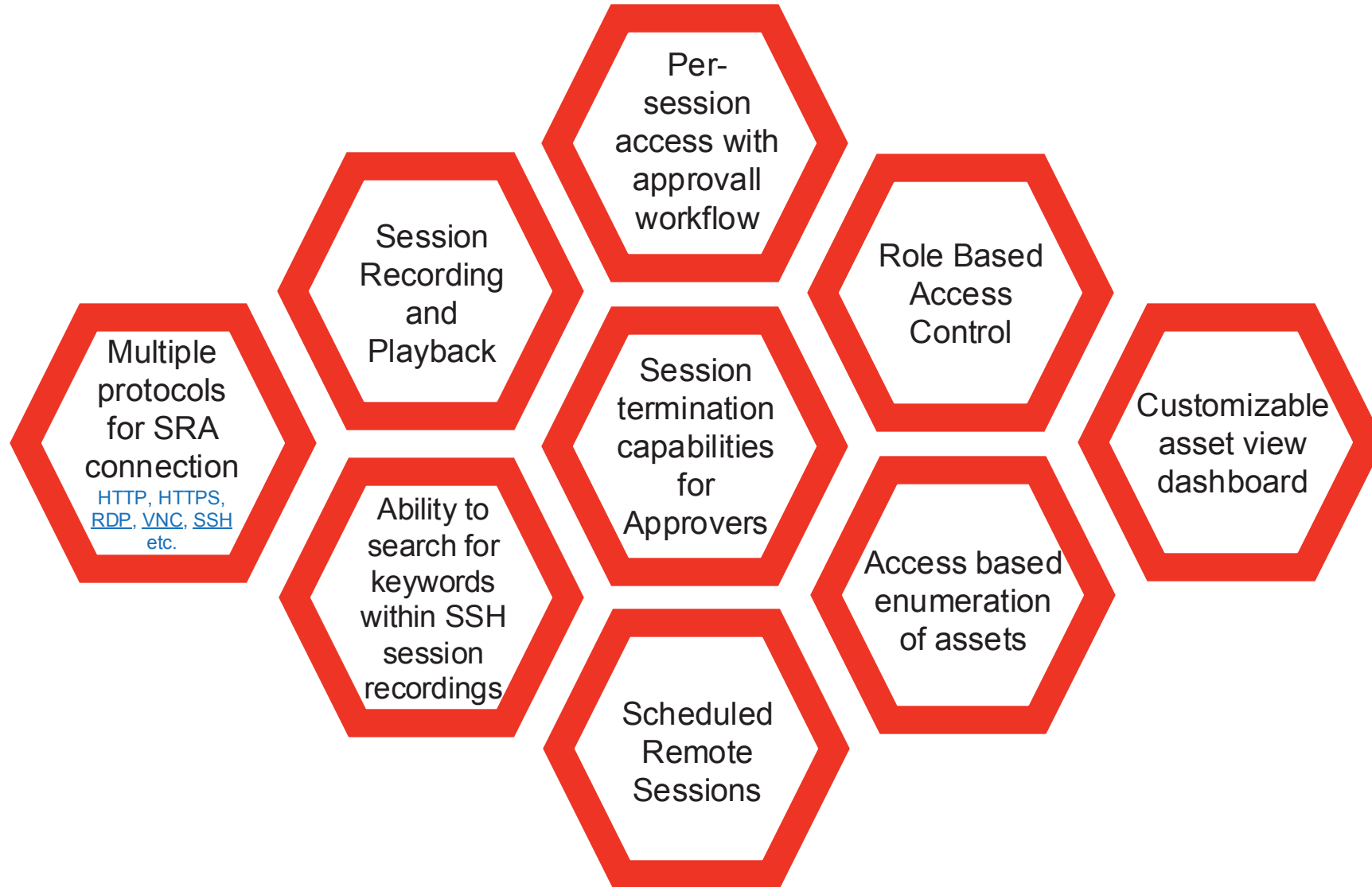
MSS NG SRA TECHNOLOGY

FEATURES INCLUDING:

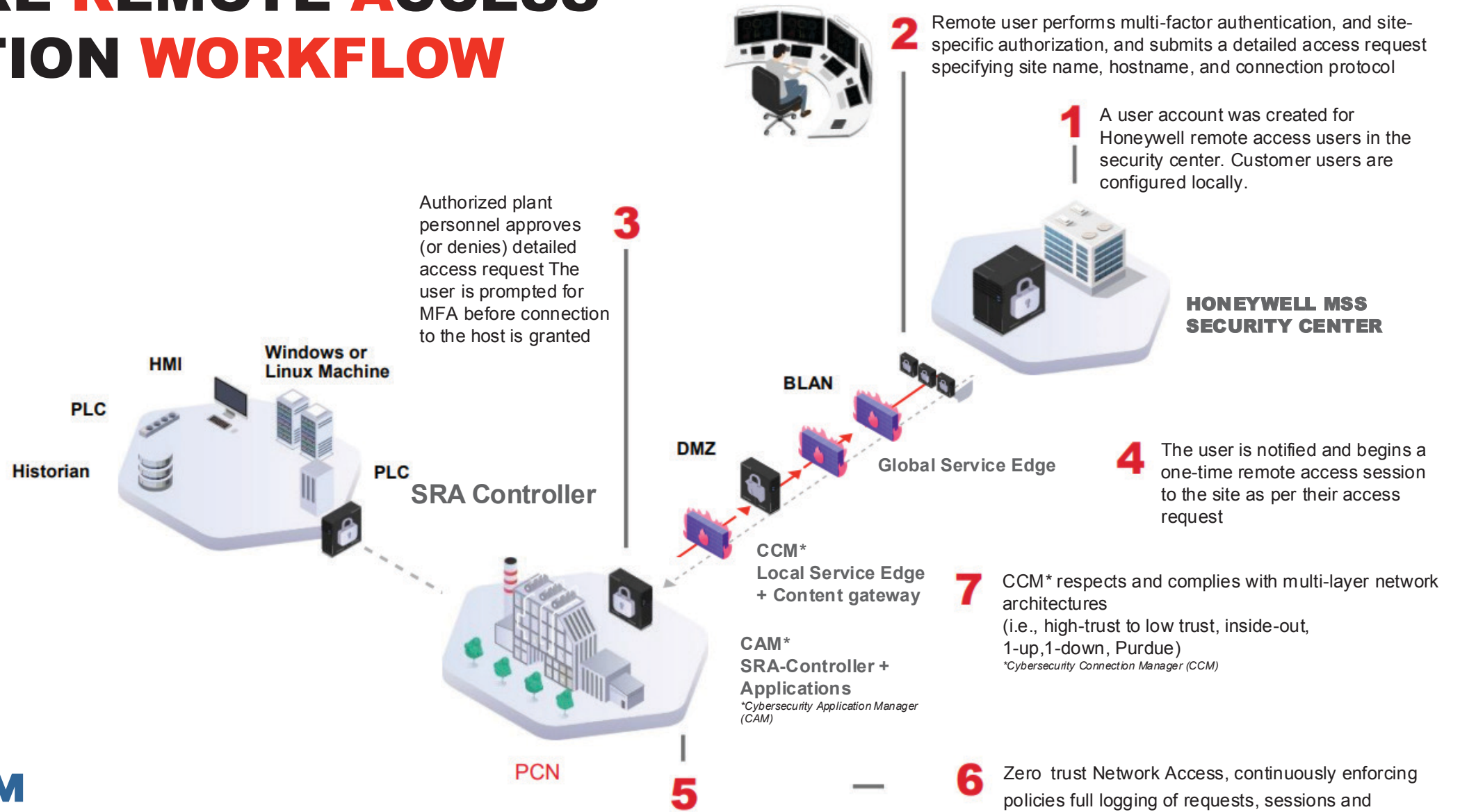


MSS NG SRA TECHNOLOGY

FEATURES INCLUDING:



HONEYWELL SECURE REMOTE ACCESS SOLUTION WORKFLOW



MSS NEXT GENERATION

SRA Controller

- Encrypted outbound channel to the Edges (TLS 1.3)
- Identity access control - MFA
- Policy enforcement
- ZTNA model
- Asset list with multiple supported RA protocols (RDP/VNC/SSH)
- Session recording, approval, supervision and termination
- Session File Transfer brokering
- Certificates are specific for each deployment (Public & Private keys)

Private EDGE

- Connects to the service EDGE network with outbound connectivity (TLS1.3)
- Does not store or decrypt data
- Intermediate connections between end-users and the Controllers
- Site-level remote access brokering allows local LAN users to stay local when connecting to the Controller

Service EDGE

- Routes traffic from the users to the SRA controllers
- Does not store or decrypt data
- Intermediate connections between end-users and the Controllers

Content Gateway

- Builds a secure TLS outbound channel to the Honeywell Security Center
- Data channel can be used for:
 - Security updates
 - Patches
 - Hotfixes
 - File reputation information
 - Vulnerability information
 - AMIR data

MSS NEXT GENERATION SRA RESOURCE REQUIREMENTS

Server	Level	vCPU	Mem (GB)	Disk (GB)	ESXi
Private Edge VM	3.5	4	6	128 (Thin Provisioning)	7.x
Content Gateway VM	3.5	4	4	40 (Thin Provisioning)	7.x
SRA Controller VM	3	4	6	128 (Thin Provisioning)	7.x
ePO VM	3	4	12	Drive C: 100 GB - OS Drive D: 200 GB - data/applications (Thin Provisioning)	7.x
WSUS VM	3	6	16	Drive C: 100 GB – OS (Thin Provisioning) Drive D: 200 GB - data/applications (Thin Provisioning) <i>Drive D: 600 GB – MSS + AMIR</i>	7.x

MSS NG SRA PLATFORM HARDWARE

Cybersecurity Application Manager L3

Model Number:	MZ-PCVMM24 - Essentials Platform Management Host
Chassis:	Dell PowerEdge R660XL 1U Chassis
Microprocessor:	Single Intel Xeon 2.6GHz
Processor Cores:	8 cores (16 vCPU)
Memory:	64GB RAM (4x16GB)
Storage:	2x960GB SSD RAID1



Cybersecurity Connection Manager L3.5

Model Number:	MZ-PCVM24 Essentials Platform Standard Production Host
Chassis:	Dell PowerEdge R660xs XL 1U Chassis
Microprocessor:	Single Intel Xeon 2.9GHz
Processor Cores:	8 cores (16 vCPU)
Memory:	64GB RAM
Storage:	2x960GB SSD RAID1



**THANK
YOU!**

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates, or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release, or timing of any such products, updates, features or functions is at our sole discretion.