BlastWave

Foundational Technologies

for OT Zero Trust Protection

DISA TEMS

Goals + Agenda Topics

- Mission Value & Alignment with DISA/DOD
- BlastWave Zero Trust for OT – US AF
- DOD Zero Trust example + work with DOD CIO PFMO
- OT Considerations: OT for Base and Mission Operations
- Solution Architecture 100% offline air gapped
- BlastWave Solution Briefing & Demonstration
- Meeting DISA/DOD OT Zero Trust Technology Needs
- BlastWave Contacts & Recorded Presentation

BlastWave Hits Ot Zero Trust Out of the Park

Resnick, Randy J SES OSD DOD CIO (USA) Sun, Mar 31, 5:39 PM (2 days ago)

to Thomas, me, Joe, Daryl, Kelly, Andrew, James, Thomas, Danita, Bill, Danielle, Chris, Ryan, Jeff, Marcus, Van, Michael, Thomas, Hugo, Cam, L, William

Tom,

The OT ZT Alliance Members hit the ball out of the park with this OT draft ZT guidance submission. WOW! This is a serious contribution to the ZT PfMO and thought leadership in the OT field as I've ever seen, bar none, and aligns perfectly with exactly what we were seeking if DoD is going to frustrate and mitigate adversarial exploitation on OT systems, as we desire to do during our ZT implementation and follow-on phases.

Let us study your document deeply, and as we have questions, we will ask them. With a desire to not SPAM everyone on this email, would there be an optimal point of contact for our OT Technical questions and specifically questions on content from this report (clarification, corrections, etc.) that could triage our inquiries?

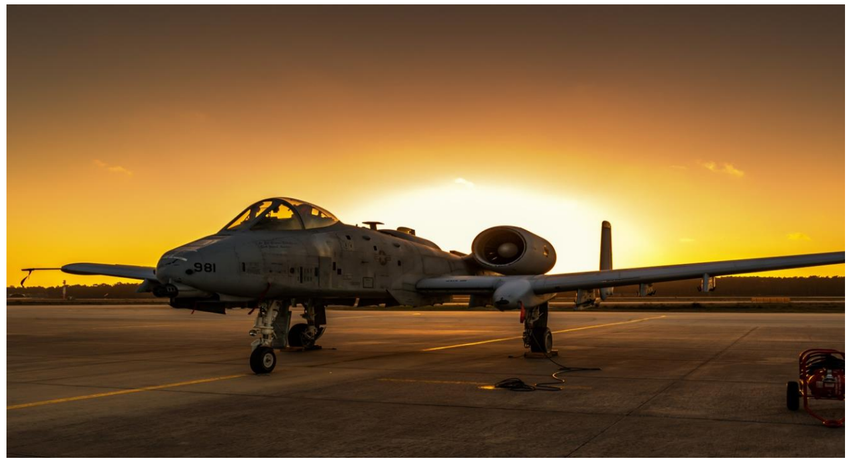
Thanks again, Tom! We are thrilled that the Spangdahlem pilot was the catalyst which led to this report, and that the ZT PfMO was its instigator. We know that progress on Zero Trust means nothing unless Companies which demonstrate leadership in their fields are willing to team together and partner where necessary. And for that, I deeply thank all of you personally in your willingness to have your companies partner together on this task, to not only deliver a showcase OT ZT example in Spangdahlem (the 1st and only one on the planet that I am aware as of this date), but to also work together to deliver such a well thought out, comprehensive ZT guidance report for OT cybersecurity. This work you all produced will become foundational, I believe, and help propel us forward much faster than we ever expected.

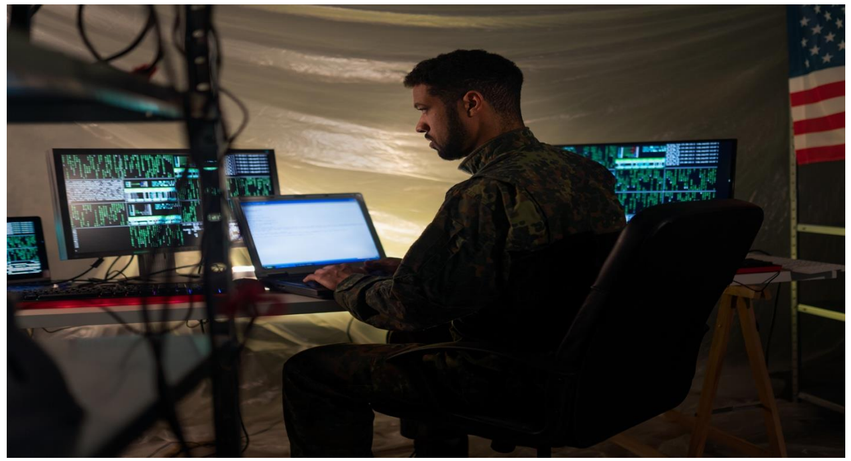
Thank you all, again.
Randy

Randy J. Resnick, SES, CISSP
Director, DoD Zero Trust Portfolio Management Office
DoD CIO/CS
The Pentagon, Room 3D1048

Easy to Install

BlastWave was the first
OT Zero Trust Deployment in the
Department of Defense at a
US Air Force Base in Germany





BlastShield Case Study: Spangdahlem Air Base

DoD/USAF

Proven DoD OT Zero Trust Solution

- DoD-Mandated Zero Trust by 2027
  - OTZTA formed to deliver comprehensive solutions for all OT (and IT) requirements

- Zero Trust Deployment Details:
  - 95 devices with 97 microsegments in 4 hours
  - 20 users with passwordless authentication

- Awarded initial pilot and follow-on permanent deployment
  - Funded by the DoD CIO
  - Air Force Water Treatment facility
  - Completed pilot Jan 8th
  - Installed and active within 4 hours
  - DoD CIO: “Miracle that you completed the entire project in 60 days”

BlastShield OT Zero Trust DOD ZT PFMO

BlastWave

OT Zero Trust Alliance

BlastWave + OT Zero Trust Alliance

	1.1.1 Inventory User		**2.1.1** Manual Device Inventory		**5.1.1** Granular Access Control Definition Pt. 1		7.1.1 (OT) Infrastructure Risk Modeling
	1.2.1 App-Based Permissions		2.1.3 Enterprise IdP Pt. 1		**5.1.2 (OT)** Granular Access Control Definition Pt. 2		**7.1.2** Log Correlation and Parsing
	1.2.2 Rule-Based Dynamic Access		**2.2.1 (OT)** Transitory Asset Connection		**5.2.1** Plan SDN API's		**7.1.3** Log Event Analysis
	1.3.1 Org MFA/IdP		2.3.4 (OT) Endpoint Anti-malware Control		**5.2.2** SDN Implementation		**7.2.1** Threat Alerting Pt. 1
	1.4.1 PAM implementation Pt. 1		**2.4.1** Deny Device by Default		**5.2.3** Segment Control/Management/Data Planes		**7.2.2** Threat Alerting Pt. 2
	1.4.2 PAM implementation Pt. 2		**2.5.1(OT)** Vulnerability Compensating Controls		**5.2.4 (OT)** Unidirectional Traffic Flow Controls		**7.2.4** Asset ID and Correlation Alerting
	1.5.1 Org ID Life Cycle Management		2.6.1 (OT) UEDM Tools and MDM		**5.3.1** Datacenter Macro-Segmentation		**7.2.5** User/Device Baselining
	1.5.2 Enterprise Life Cycle Pt. 1		4.2.3 Software Defined Storage Policy		**5.3.2** B/C/P/S Macro-Segmentation		**7.3.1** Analytics Tool Implementation
	1.6.1 (OT) Establish User Behavior Baseline		4.4.2 (OT) Process Variable Integrated Analysis		**5.4.1** Network Microsegmentation		**7.3.2** User and Device Baseline Analysis
	1.7.1 Deny User by Default		**4.4.4 (OT)** Process Data Trend Analysis		**5.4.2** Role-Based Dynamic Microsegmentation		**7.4.1** User and Device Profile Definition Pt. 1
	1.8.1 Single Authentication		**4.8.1 (OT)** Data Timeliness Functions Pt. 1		**5.4.4** Data Protection in Transit		**7.5.1** Cyber Threat Intelligence Pt. 1
	1.8.2 Periodic Authentication		**4.8.2 (OT)** Data Timeliness Functions Pt. 2		**5.4.5 (OT)** Network Incident Response Isolation		**7.5.2** Cyber Threat Intelligence Pt. 2
	1.9.1 Enterprise PKI/IdP Pt. 1				6.1.1 Policy Inventory and Development		

On-Premise Air Gap Deployment: Can be deployed without internet access – **100% Offline**

BlastWave

OT Considerations: OT for Base & Mission Operations

OT Networks on Military Bases:

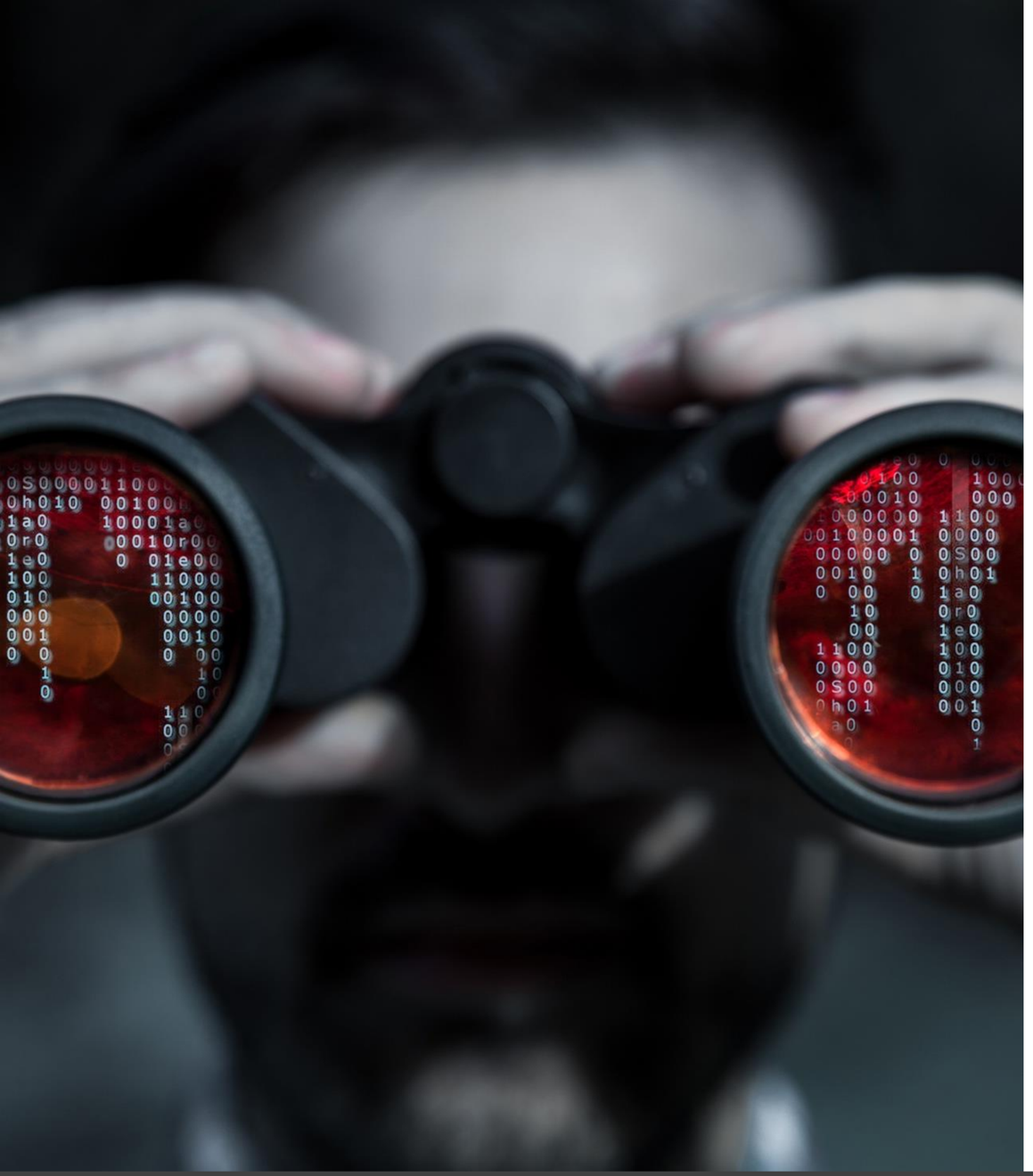
- Base Power Generation & Distribution
- Back up Power
- Base Water/Wastewater
- Fuel Storage & Distribution

OT Facilities Related Control Systems: FRCS

- Building Controls – Power, HVAC, Security, Camera
- Manufacturing

Mission Systems:

- Automated Material Handling
- Logistics & Transportation
- Remote Communications
- Propulsion systems
- Signaling systems
- Munition systems
- Mission Water
- Health - MRI, IV, XRAY
- Weather
- Satellite



1.Network Cloaking Blocks Reconnaissance

Cloaking renders standard & AI-enhanced reconnaissance tools ineffective by only responding to valid authentication requests & dropping all other packets, eliminating many Initial Access vectors from MITRE ATT&CK

Prevents Reconnaissance:

Only responds to PKI authentication

Virtual Air Gap:

No Public IP Access for OT Devices, preventing C&C & vulnerability exploitation

Device Cloaking:

Private-to-Private IP NAT to hide OT devices from internal lateral movement and insider threats

2. Segmentation Blocks Lateral Movement

Device-level microsegmentation blocks the privilege escalation, defense evasion, credential access, discovery, & lateral movement vectors in the MITRE ATT&CK model. Internal users are blocked from exceeding their authority & accessing restricted systems.

Granular Device/Protocol Policies:

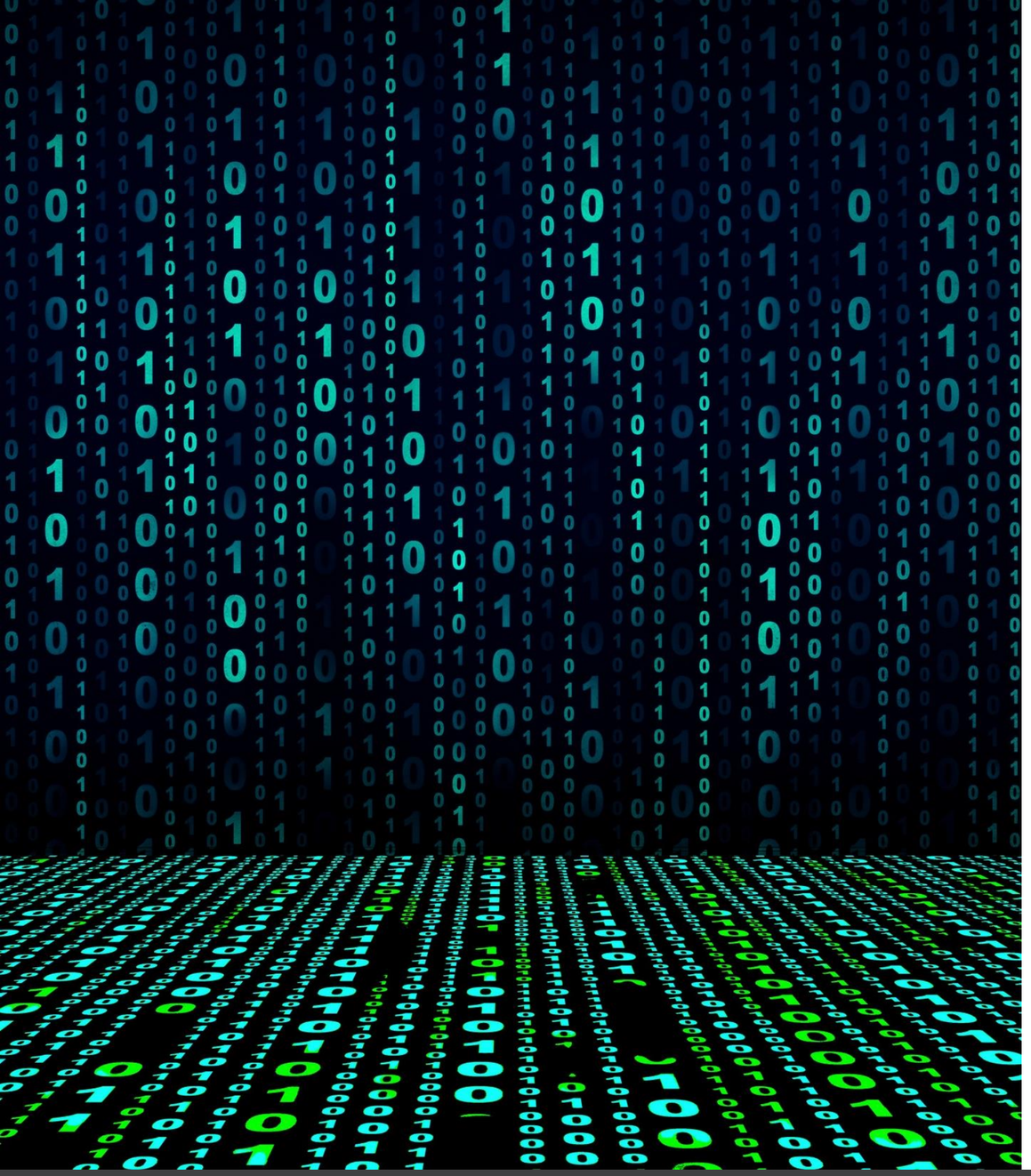
Policies can restrict down to a single device & protocol, or entire groups of device types

Layer 2 Lateral Movement Prevention:

Layer 2 isolation even for devices deployed on same L2 network or switch

Optional Secure Agent:

Critical Servers can install agent to further segment & protect access to the OT Network



3. Secure Remote Access

Deployment flexibility: 100% Offline on premise (Air Gapped) with MFA FIDO Key or Private Secure Cloud

P2P Tunnel Mesh:

Full mesh Peer 2 Peer tunnels between user & devices/agents

Least Privilege Access and Revocation:

User Access & revocation in real-time

Fine-grained control to device or groups of devices

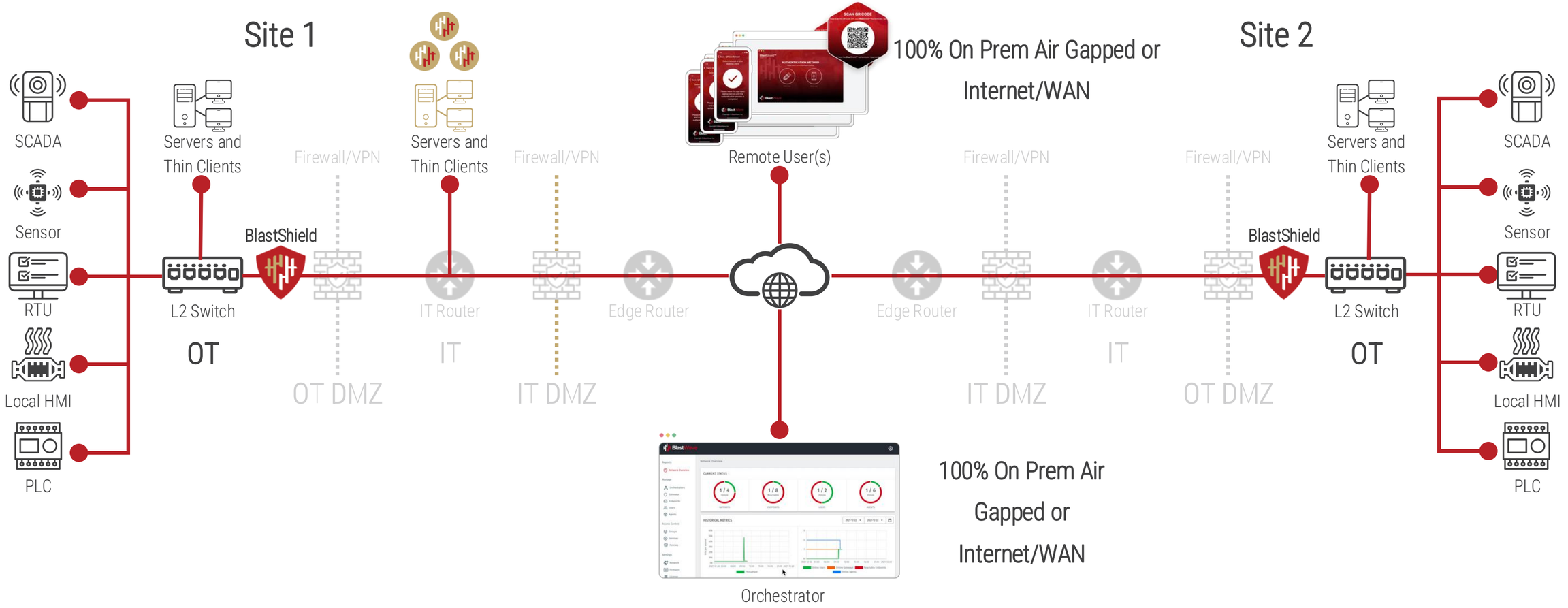
Phishing Resistant MFA:

no passwords required (no passwords to steal)

Apple Pay-style biometrics for user access

BlastShield Deployment

BlastShield creates a Secure OT Overlay onto your Infrastructure



BlastWave

Concept of Operations Architecture and Zones/Conduits (No Zones)

Level 4/5 Enterprise Network

IT Zone

IT Services | OT Remote Access | IT Firewall

Process Information Zone

Monitoring | DB Server

Level 3.5 DMZ

DMZ Zone/Main Site

PAM Server | Patch Server | Thin Clients | Jump Server | Historian

Level 0-3 OT Network

IEC 62443 recommends creating zones and conduits as a way to segment the OT network and reduce risk.

Main Site

- **Supervisory Zone**: SCADA | Thin Clients
- **Control Zone**: HMI | Controller | Operator Workstation | SCADA
- **Safety Zone**: IP Camera | Sensor
- **Process Zone**: Actuator | PLC

Remote Site(s)

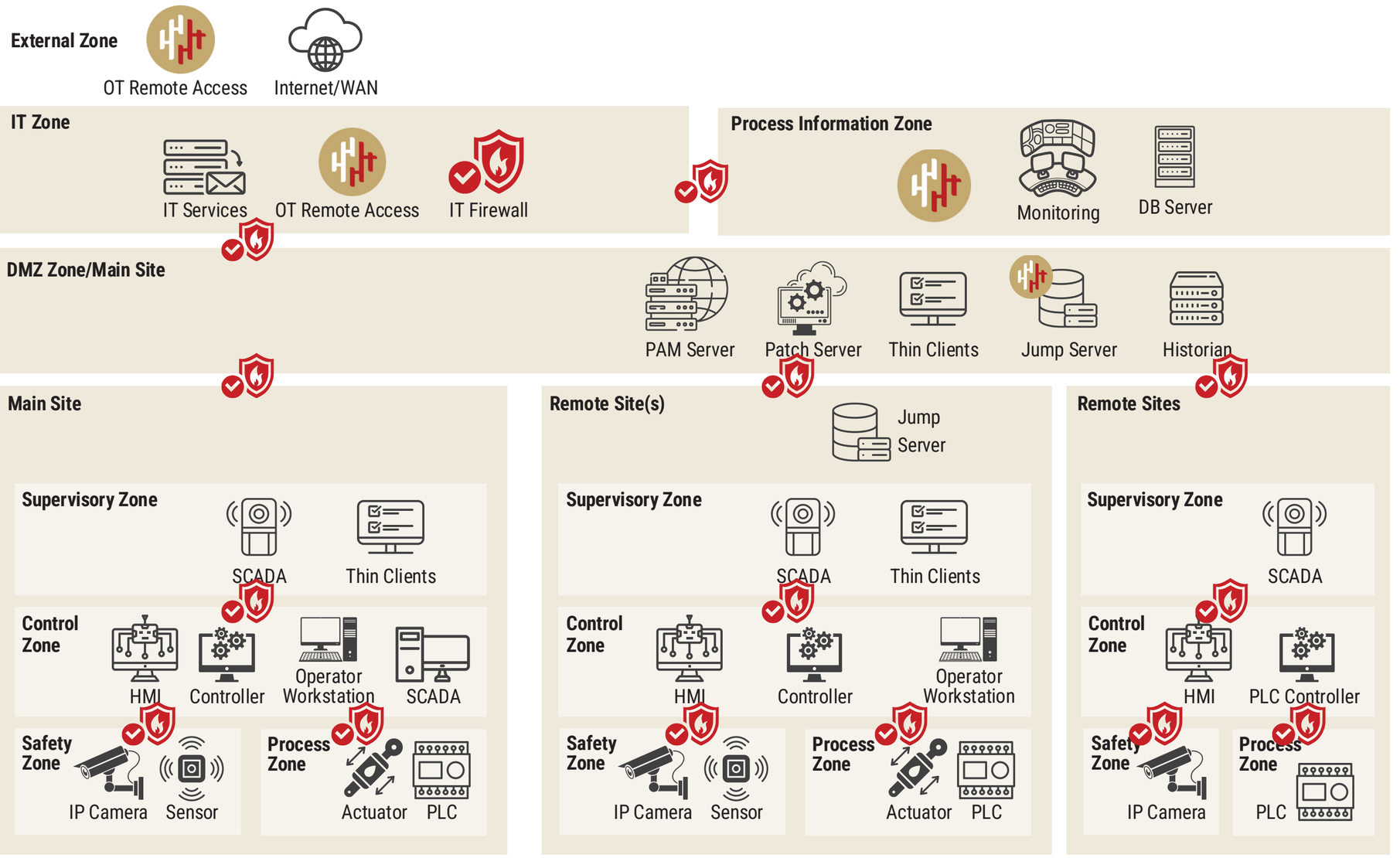
Jump Server

- **Supervisory Zone**: SCADA | Thin Clients
- **Control Zone**: HMI | Controller | Operator Workstation
- **Safety Zone**: IP Camera | Sensor
- **Process Zone**: Actuator | PLC

Remote Sites

- **Supervisory Zone**: SCADA
- **Control Zone**: HMI | PLC Controller
- **Safety Zone**: IP Camera
- **Process Zone**: PLC

Concept of Operations Architecture Zones/Conduits (Firewalls)



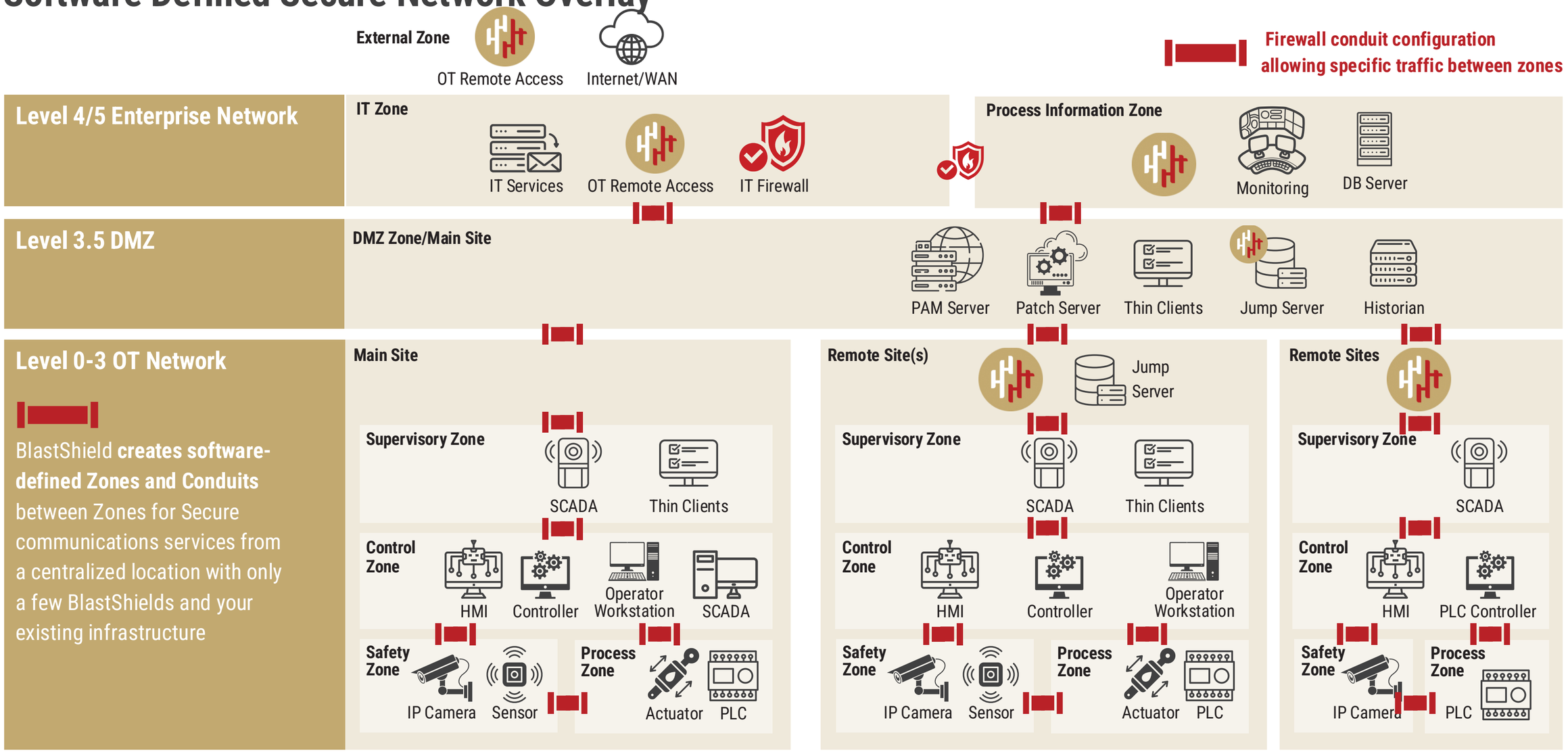
BlastWave

Concept of Operations Zones/Conduits (BlastWave)

Software Defined Secure Network Overlay

BlastShield OT Software Abstraction
Fine-Grained Protection

Firewall conduit configuration
allowing specific traffic between zones



BlastWave

BlastWave Demonstration

OT Cybersecurity Protection

Meeting DISA/DOD OT Zero Trust Technology Needs:

Network Cloaking:

Prevents Reconnaissance and prevents vulnerability exploits for OT systems

Microsegmentation:

Software-defined segmentation, including Layer 2 Lateral movement prevention

OT Secure Remote Access:

Phishing-Resistant passwordless Least Privilege Access for users

BlastWave

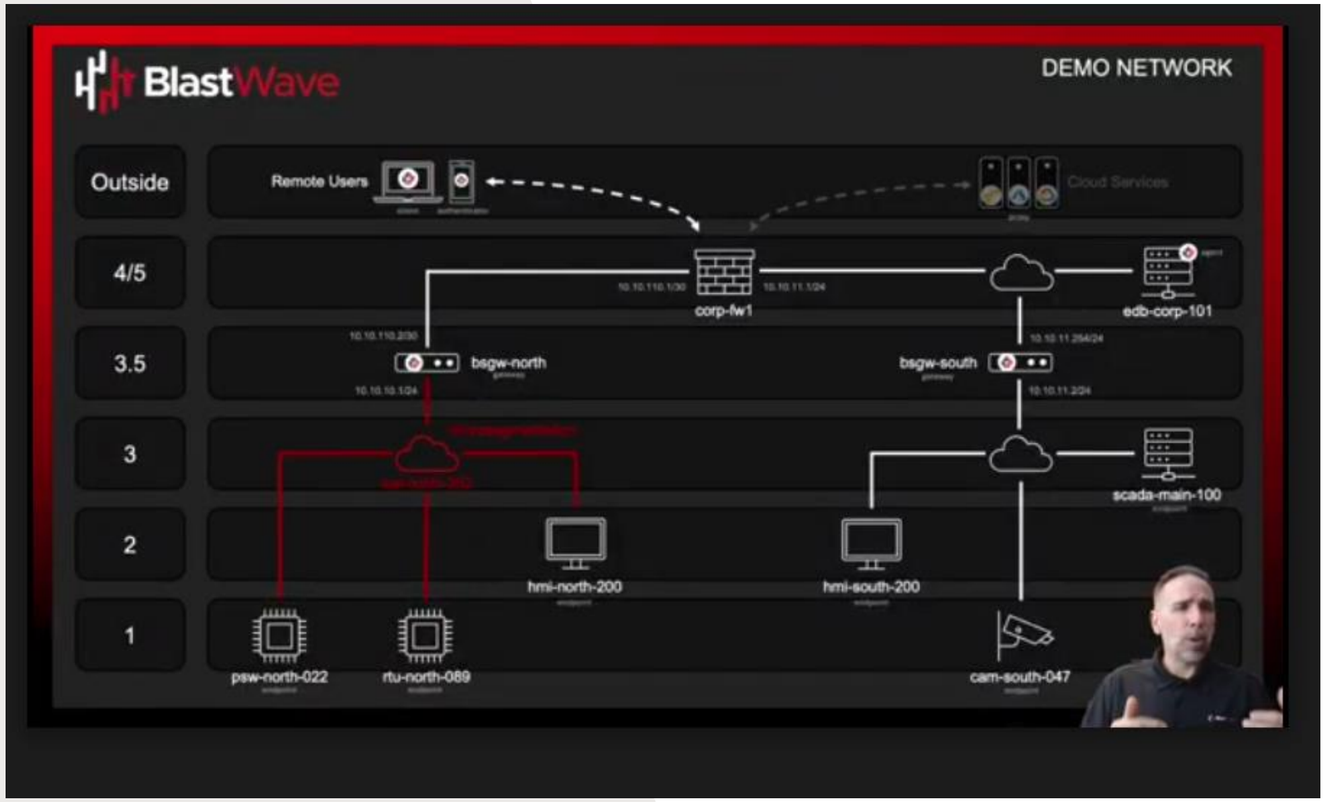
Contact Information for a briefing + trial:

Cam Cullen, CMO: cam@blastwave.com

Stephen Gallagher, Sales: stephen@blastwave.com

Joe Baxter, Architect: joe@blastwave.com

Demo Recording



https://drive.google.com/file/d/1G6lpBR7idZDs6l2ura8RFf5dMNnoRUt2/view?usp=sharing