OT Zero Trust Protection Use Cases

Secure Infrastructure for OT Networks

BlastWave

Secure Infrastructure for OT Networks

Protecting the critical infrastructure that powers nations worldwide is not just a big task; it's crucial. Too many people have given up on protecting their OT assets and are content to monitor them to see when something goes wrong. However, the potential risks are too high to be complacent. Zero Trust for OT is crucial and should be prioritized since the return on mitigation is so high.

OT Networks with BlastWave

BlastWave's OT Zero Trust Protection solution addresses critical security and operational challenges while driving cost efficiencies. BlastWave offers three key "never trust, always verify" technologies to protect critical infrastructure OT networks:

Network Cloaking:

Network Cloaking ensures that critical yet outdated legacy infrastructure becomes invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker.

With BlastShield, network operators ensure security and compliance with industry standards and guidance like NIST 800-53, 800-207 (Zero Trust), and IEC 62443. AI-enhanced reconnaissance tools cannot probe into the internal workings of a facility because they have no path to reach the internal OT networks.

OT Secure Remote Access:

BlastShield provides OT Secure Remote Access to critical OT systems, ensuring operators and 3rd party contractors can monitor and manage them without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. A full mesh of P2P encrypted tunnels is created to secure traffic from remote users to the network and any agent-enabled systems, protecting against Man-in-the-middle attacks.

Network Segmentation (Microsegmentation):

BlastShield simplifies the challenge of microsegmentation by creating software defined segments operating at both Layer Two and Layer Three, resulting in a secure infrastructure that operates as a single, cohesive policy infrastructure regardless of location or device type.

IT and OT network staff and temporary contractors are permitted access to only the systems they are responsible for, and privileges can be granted and revoked in real-time. BlastShield prevents lateral movement by Secure Remote Access users within the network and can even provide lateral movement protection at Layer 2 for local network connections.

CONTENTS

Use Case: Prevent Reconnaissance

TLDR: You Can't Attack What You Can't See

Stop attackers before they even know what you have. Network cloaking makes your critical OT systems invisible to cyber threats. Think of it as a digital force field: hackers can't find what they can't see. This means less risk of costly downtime, fewer security breaches, and more peace of mind. By eliminating reconnaissance, you dramatically reduce the attack surface, allowing your operations to run smoothly and your team to focus on what matters most, not constant fire drills. Simply put, cloaking protects your assets, saves money, and keeps operations uninterrupted.

Challenge Met:

Eliminate the Ability of Attackers to Exploit a Zero Day Vulnerability

Network cloaking addresses the technical challenge of reconnaissance by fundamentally altering the network's address space and visibility. Instead of relying on traditional IP address-based routing, cloaking technology utilizes dynamic, ephemeral identifiers and overlays.

This means that standard network scanning tools, used by attackers for reconnaissance, return no results. Critical OT devices are effectively hidden, typically exposed through static IP addresses and open ports. The network appears as a "dark space" to unauthorized users, preventing them from mapping the network topology or identifying vulnerable assets. Furthermore, cloaking requires pre-authenticated communication to reveal any network services.

This combination of address obfuscation, dynamic identifiers, and pre-authentication effectively eliminates the ability of attackers to perform successful reconnaissance, thus significantly reducing the attack surface.

The Ideal World:

Cloak to meet business needs

In an ideal, cloaked OT network, hackers are met with an impenetrable digital void. They initiate scans, probing for vulnerabilities, but find nothing. Their reconnaissance tools return empty results, leaving them utterly blind. Critical control systems, legacy devices, and sensitive data are effectively removed from the attack surface, hidden behind layers of dynamic, ephemeral identifiers.

Attempts to establish unauthorized connections are met with silence. No open ports, no responding services, no visible network topology. The network behaves as if it doesn't exist, rendering traditional attack vectors useless. Even sophisticated AI-powered reconnaissance tools are thwarted, unable to penetrate the cloaked environment.

Operators, meanwhile, work seamlessly. Authorized users, with their verified BlastShield clients, access the network effortlessly, their connections authenticated and their activity monitored. Legacy systems, once a security liability, now operate safely, shielded from external threats. The OT environment runs smoothly, efficiently, and securely, free from the constant threat of cyberattacks. Downtime is minimized, productivity is maximized, and peace of mind is restored. The network, protected by cloaking, becomes an invisible fortress, safeguarding critical infrastructure and ensuring uninterrupted operations.

BlastShield

Network Cloaking as a Digital Shield

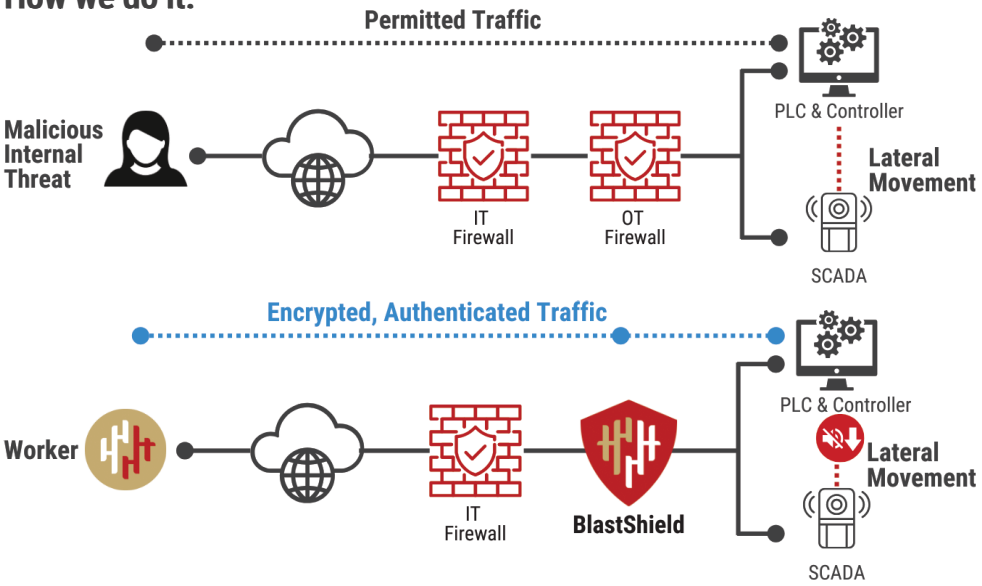
In a network environment, if you can't see an OT system, you can't hack or attack it. Network cloaking is industry's best opportunity to prevent hacks. IT/OT administrators cannot patch legacy systems; zero-day vulnerabilities are even in VPN products.

BlastShield cloaks the network to make it invisible to hackers, providing a layer of defense that is impossible with firewall or VPN solutions today. BlastShield protects against inbound attacks, lateral movements, and diverse cyber threats, including stolen credentials and malware delivery, enhancing operational integrity.

With BlastShield, crucial components like workstations and building management systems remain uninterrupted and secure from outside threats.

Prevent Reconnaissance (cont'd)

How we do it:



Network Cloaking for OT Network Reconnaissance Protection

Network cloaking aims to obscure the presence and characteristics of an OT network, making it significantly harder for attackers to gather information during reconnaissance phases. The key technologies for Network Cloaking are:

Network Address Translation (NAT):

Implementation: Deploy BlastShield to perform cloaking and hide the internal IP address space and topology from external view.

Configuration:

- Deploy in the OT DMZ with a Zero Trust Configuration
- Block all external connections from the OT network except authorized users
- If an OT device needs to talk to specific servers or services, create a secure connection between the devices to prevent session hijacking

Benefit: Prevents direct scanning and enumeration of internal OT devices.

Dynamic DNS and IP Address Overlay:

Implementation: Employ dynamic DNS services and IP address overlays to change the network's external appearance and force all traffic through the BlastShield gateway.

Configuration:

- Use dynamic DNS to map external hostnames to overlay IP addresses.
- Utilize the BlastShield client for encrypted tunnels with the BlastShield gateway to enable access to OT endpoints.

Benefit: It makes it difficult for attackers to maintain a consistent network view.

Zero Trust Encrypted Remote Access:

Implementation: Force all remote access to the OT network through authenticated, passwordless, and encrypted VPN tunnels.

Configuration:

- Implement passwordless multi-factor authentication for secure access.
- Ensure all communications are encrypted.
- Segment Zero Trust access based on roles.

Benefit: Hides the OT network behind an encrypted tunnel, and requires authentication for access.

Important Considerations:

OT Protocol Awareness: Ensure that any security measures do not interfere with legitimate OT protocol traffic.

Performance Impact: Evaluate the performance impact of network cloaking techniques on OT network operations.

Maintenance: Regularly update security configurations and monitor for suspicious activity.

Defense in Depth: Network cloaking should be part of a layered security approach.

Testing: Regularly test the effectiveness of network cloaking techniques.

By implementing these configurations, organizations can significantly reduce the visibility of their OT networks to attackers, making reconnaissance more difficult and time-consuming, and increasing the overall security posture.

Use Case: Protect Legacy OT Devices

TLDR: Virtual Air Gaps for OT Devices

A Zero Trust gateway creates a "virtual air gap to protect unpatchable legacy OT devices. It acts as a strict gatekeeper, verifying every connection and only allowing authorized traffic. This isolates your old gear from cyber threats, like a physical air gap, but without disrupting operations. It's a secure, software-defined barrier, keeping hackers out and your critical systems running.

Challenge Met:

Virtual Patching for Unpatchable OT Devices

Zero-day vulnerabilities in unpatchable OT devices pose a critical threat. While traditional patching is impossible, virtual air gaps and network cloaking offer a powerful, proactive defense, effectively acting as a "virtual patch." By making these devices invisible to unauthorized users and external threats, network cloaking eliminates the attack surface, preventing exploitation even if a zero-day vulnerability exists. The devices are hidden in plain sight, accessible only to verified, authorized users.

Simultaneously, the virtual air gap, created by a Zero Trust gateway, enforces strict access control, verifying every connection before allowing traffic to reach the protected devices.

This prevents unauthorized access and limits the potential impact of a successful exploit, even if an attacker discovers a zero-day. Essentially, these technologies create a protective barrier, isolating the vulnerable devices from the outside world and minimizing their exposure to potential attacks. They provide a layer of security that operates independently of the device's inherent vulnerabilities, buying critical time until a permanent patch or replacement can be implemented.

The Ideal World:

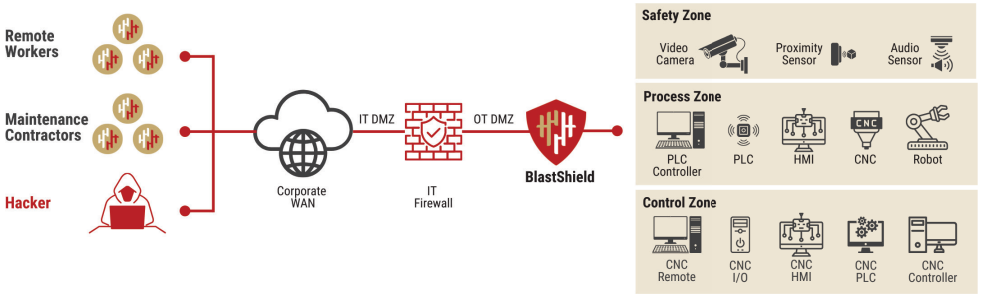
Cloaked and Segmented Virtual Air Gaps

Imagine creating a virtual air gap, a secure isolation zone, for your vulnerable legacy OT devices, without physically disconnecting them. Network cloaking achieves just that. By rendering these unpatchable systems invisible to unauthorized users and external threats, cloaking effectively simulates the security benefits of an air gap, but without the operational limitations.

These legacy devices, often critical to operations but lacking modern security features, become hidden in the digital shadows. They remain accessible to authorized personnel with verified BlastShield clients, but are completely undetectable to external attackers. This means that even if a breach occurs elsewhere in the network, the cloaked devices remain protected, isolated from the threat.

This virtual air gap provides a powerful defense against known and unknown vulnerabilities. It prevents lateral movement within the network, limiting the impact of a successful attack.
It also protects against zero-day exploits and other emerging threats to which legacy devices are particularly susceptible. Network cloaking allows you to maintain the functionality of your critical legacy systems while significantly reducing their risk exposure, effectively bridging the gap between operational necessity and security imperative.

How we do it:



Virtual Air Gap for Unpatchable OT Devices using Network Cloaking and Zero Trust Access

Unpatchable OT devices pose significant security risks due to known vulnerabilities. An actual air gap is often impractical, but a virtual air gap aims to replicate its security benefits by minimizing network exposure and enforcing strict access controls.

Key Technology Configuration:

Network Cloaking:

Deploy Network Cloaking as a secure overlay to the OT network:

- Deploy BlastShield in front of the unpatchable OT segment.
- Implement cloaking overlay to hide the internal IP address space.
- Deny all external connections except Zero Trust Access

Protocol Filtering and Obfuscation:

- Allow only essential OT protocols required for operation for each device or group of devices.

Dynamic DNS for the Overlay Cloak:

- Use dynamic DNS to map device hostnames to cloaked IP addresses

Zero Trust Access:

Deploy BlastShield

- Deploy a BlastShield gateway between the cloaked OT segment and the rest of the network.
- Configure the gateway to act as a micro-segmentation controller.

Identity-Based Access Control:

- Activate Secure Remote Access and Authentication on BlastShield
- Optionally, Integrate BlastShield with an IdP (e.g., Active Directory, Azure AD).
- Define granular access policies based on user/device identities.

Least Privilege Principle:

- Grant access only to authorized users or devices based on the principle of least privilege.
- Require explicit authorization for all access requests.

Contextual Access Control:

- Consider factors like time, location, and device posture when granting access.
- Implement multi-factor authentication (MFA) for all access attempts.

Microsegmentation:

- Create micro-segments within the cloaked OT network based on device function or criticality.
- Enforce strict access control policies between micro-segments.

Secure Remote Access (If Required):

- Force all remote access through the BlastShield gateway.
- Implement strong authentication and encryption for remote sessions.
- Segment remote access based on roles and responsibilities.

Implementation Considerations:

OT Protocol Awareness: Ensure security measures do not interfere with legitimate OT protocol traffic.
Performance Impact: Evaluate the performance impact of network cloaking and ZTA on OT network operations.
Redundancy: Implement redundancy for critical components to minimize downtime.
Security Hardening: The BlastShield gateway can only be accessed with Passwordless MFA and from authorized devices.
Documentation: Maintain detailed documentation of the configuration.
Regular Audits: Conduct regular security audits to ensure ongoing compliance and effectiveness.
Change Management: Implement strict change management procedures for OT devices and security configurations.
Monitoring: Implement robust logging and monitoring for the BlastShield systems.

Benefits:

Reduced Attack Surface: Network cloaking minimizes the visibility of unpatchable OT devices.
Granular Access Control: BlastShield enforces strict access controls, limiting the potential impact of a breach.
Enhanced Compliance: Helps meet regulatory requirements and industry standards.

By combining network cloaking with zero trust access, organizations can create a strong "virtual air gap" for unpatchable OT devices, significantly reducing their risk of compromise.

Use Case: Protection Against AI-Powered Attacks

TLDR: Stop AI-powered attacks before they start

AI-powered attacks are getting scarily good at spying on your network and tricking your people. But here's the good news: cut off their intel, and they're powerless. You take away AI's biggest weapons by preventing external reconnaissance (think network cloaking) and eliminating phishing. No more easy targets, no more stolen passwords. It's like taking the "smart" out of their "smart" attacks.

Challenge Met:

Blocking AI Attack vectors

Stopping reconnaissance and phishing requires a multi-layered approach, and a Zero Trust solution that combines network cloaking and passwordless MFA offers a powerful defense against these evolving threats.

Here's how it works:

Network cloaking: By rendering critical assets undiscoverable to unauthorized users, network cloaking effectively neutralizes reconnaissance attempts. Attackers can't gather the information they need to launch targeted attacks, including phishing campaigns. The network becomes a "black box," preventing internal system mapping and identifying vulnerabilities.

Passwordless MFA: Traditional passwords are vulnerable to phishing attacks, where attackers trick users into revealing their credentials. Passwordless MFA eliminates this vulnerability using stronger authentication methods like biometrics or hardware tokens. This ensures that even if an attacker obtains a user's password through phishing, they still can't access the network.

Zero Trust Framework: The Zero Trust framework underpins this approach by assuming no user or device is inherently trustworthy. Every connection attempt is verified, authenticated, and authorized before access. This limits lateral movement within the network and prevents attackers from exploiting compromised credentials.

This combination of technologies creates a proactive defense against reconnaissance and phishing, two of today's most common AI-powered attack vectors. BlastShield significantly reduces the attack surface and strengthens the overall security posture by making the network undiscoverable and eliminating password vulnerabilities.

The Ideal World:

AI-Resistant OT Cybersecurity Protection

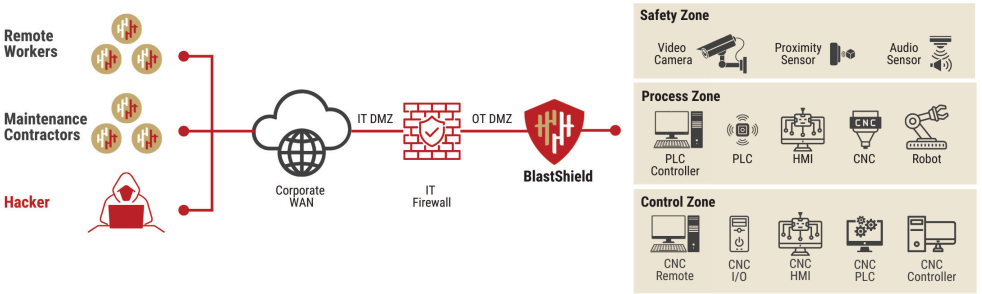
Imagine a world where AI-powered attacks are rendered powerless, their sophisticated reconnaissance and cunning phishing schemes thwarted before they begin. This is the promise of a security approach that prioritizes proactive defense.

By preventing AI reconnaissance, we effectively blind the attackers. Network cloaking, secure overlays, and other advanced techniques make critical infrastructure invisible to malicious AI algorithms, denying them the information they need to launch targeted attacks. The network becomes a fortress, hidden in plain sight.

Simultaneously, eliminating phishing removes the human element from the equation. Passwordless authentication, robust identity verification, and ease-of-use create a human firewall, impervious to even the most sophisticated social engineering tactics. AI-powered phishing attacks, designed to exploit human psychology, are rendered ineffective against a workforce that no longer uses credentials.

In this ideal world, critical infrastructure operates securely and reliably. Operators focus on their core tasks, free from the constant threat of cyberattacks. Innovation flourishes, unhindered by the fear of disruption. Society benefits from the uninterrupted flow of essential services, powered by a secure and resilient digital foundation. This is the future we can achieve by proactively addressing the evolving threat of AI-powered attacks, building a world where technology empowers, not endangers.

How we do it:



Network Cloaking and Passwordless MFA for OT Reconnaissance and Phishing Prevention

AI-driven reconnaissance can rapidly map network vulnerabilities, while sophisticated phishing attacks bypass traditional security measures. Passwordless MFA and network cloaking are crucial in mitigating these threats.

Key Technology Configuration:

Network Cloaking:

Deploy Network Cloaking as a secure overlay to the OT network:

- Deploy BlastShield in front of the unpatchable OT segment.
- Implement cloaking overlay to hide the internal IP address space.
- Deny all external connections except Zero Trust Access

Protocol Filtering and Obfuscation:

- Allow only essential OT protocols required for operation for each device or group of devices.

Dynamic DNS for the Overlay Cloak:

- Use dynamic DNS to map device hostnames to cloaked IP addresses

Passwordless Multi-Factor Authentication (MFA):

Deploy BlastShield

- Deploy a BlastShield gateway between the cloaked OT segment and the rest of the network.
- Configure the gateway to act as a micro-segmentation controller.

Identity-Based Access Control:

- Activate Secure Remote Access and Authentication on BlastShield

Biometric Authentication:

- Utilize fingerprint scanning, facial recognition, or other biometric methods for user authentication.
- Ensure that biometric data is securely stored and processed.

FIDO2 Security Keys:

- Deploy FIDO2 security keys to users for strong, phishing-resistant authentication.
- Enforce the use of FIDO2 keys for all access attempts.

Device-Based Authentication:

- Utilize device-based authentication methods, such as push notifications or device certificates.
- Ensure that devices are registered and managed securely.

Least Privilege Principle:

- Grant access only to authorized users or devices based on the principle of least privilege.
- Require explicit authorization for all access requests.

Contextual Access Control:

- Consider factors like time, location, and device posture when granting access.
- Implement multi-factor authentication (MFA) for all access attempts.

Microsegmentation:

- Create microsegments within the cloaked OT network based on device function or criticality.
- Enforce strict access control policies between micro-segments.

Implementation Considerations:

OT Protocol Compatibility: Ensure security measures do not interfere with legitimate OT protocol traffic.

Performance Impact: Evaluate the performance impact of network cloaking and passwordless MFA on OT network operations.

User Experience: BlastShield's user-friendly passwordless MFA solution minimizes disruption to OT operations.

Device Compatibility: Ensure BlastShield's passwordless MFA solution is compatible with all devices used to access the OT network.

Redundancy and Failover: Implement redundancy and failover mechanisms to ensure high availability of the security infrastructure.

Security Hardening: Secure all security components according to best practices.

Regular Audits and Penetration Testing: Conduct regular security audits and penetration testing to identify and address vulnerabilities.

Continuous Monitoring and Logging: Implement comprehensive logging and monitoring to detect and respond to security incidents.

Benefits:

Enhanced Security Posture: Network cloaking and passwordless MFA significantly reduce the attack surface and prevent AI-powered reconnaissance and phishing attacks.

Reduced Risk of Data Breaches: Passwordless MFA eliminates the risk of stolen credentials, preventing unauthorized access to sensitive data.

Increased Operational Resilience: Organizations can maintain operational continuity and minimize downtime by preventing successful attacks.

Improved Compliance: Helps meet regulatory requirements and industry standards.

Use Case: Phishing-Resistant OT Secure Remote Access

TLDR: You can't steal a password that doesn't exist

Passwordless MFA stops hackers from stealing your passwords because there's no password to steal. It uses things like your fingerprint or a unique code on your phone to verify it's you. Even if a hacker tricks you with a phishing email, they can't log in because they don't have your finger or your phone. It's strong security that's super easy to use.

Challenge Met:
Eliminate phishing as an initial attack vector

Passwordless MFA eliminates the primary attack vector exploited in phishing campaigns: the reliance on vulnerable passwords. By removing passwords from the authentication process, organizations significantly reduce the risk of credential theft through phishing attacks.

This, in turn, diminishes the need for extensive employee training focused on identifying and avoiding phishing scams, lowering associated training costs. Additionally, it reduces the reliance on regular phishing tests to assess employee susceptibility, further minimizing expenses. Moreover, passwordless MFA eliminates the overhead associated with password administration, such as password resets, complexity enforcement, and help desk support, freeing up IT resources and reducing operational costs.

By shifting to a more secure and user-friendly authentication method, organizations can mitigate the financial burden associated with phishing and password management, while simultaneously strengthening their overall security posture.

The Ideal World: "Yet another day where you don't need to change your password"

Imagine the OT administrator, freed from the tyranny of password resets and the looming threat of phishing attacks. No more late-night calls to unlock critical systems, no more scrambling to contain a breach caused by compromised credentials. Instead, they confidently monitor the network, ensuring the smooth operation of essential infrastructure.

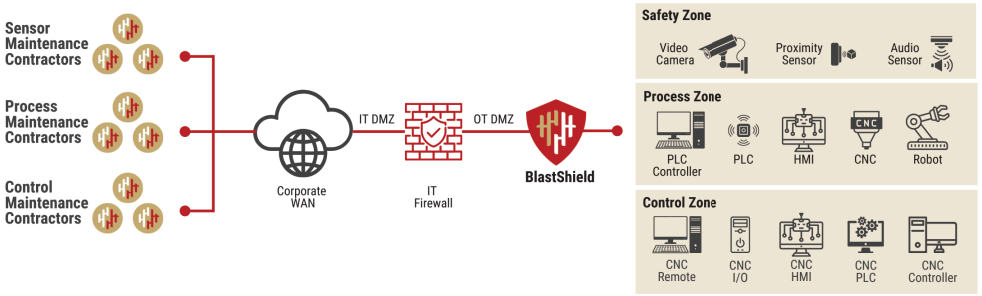
Phishing, once a major vulnerability for OT environments, is neutralized. Operators authenticate seamlessly with passwordless MFA, using biometrics or hardware tokens that are immune to social engineering tactics. The risk of credential theft, and the potential for catastrophic consequences, fades into the background.

This administrator proactively manages the network, focusing on optimizing performance and ensuring the uninterrupted flow of vital services. They leverage their expertise to enhance security, implement new technologies, and strengthen the resilience of critical infrastructure. No longer bogged down by password management and phishing remediation, they become a guardian of operational efficiency and safety.

In this ideal world, the OT administrator enjoys a sense of calm and control. They trust the security of their systems, knowing that passwordless MFA provides a robust defense against phishing and credential theft. Their focus shifts from reactive firefighting to proactive optimization, ensuring the continuous and secure operation of essential services that power our communities. This is the future of OT security, where technology empowers, not hinders, the guardians of critical infrastructure.

Phishing-Resistant OT Secure Remote Access (cont'd)

How we do it:



Passwordless MFA for OT Network Phishing Prevention

Phishing relies on obtaining user credentials (usernames and passwords). Passwordless MFA directly addresses this vulnerability by eliminating passwords, making phishing attacks significantly less effective.

Key Technology Configuration:

Passwordless MFA Solution:

Deploy BlastShield OT Security Gateway:

- BlastShield's passwordless MFA solution that supports FIDO2 security keys, biometric authentication (fingerprint, facial recognition), and/or device-based authentication (mobile push notifications, device certificates).

Implementation of Biometric Authentication:

- If biometric authentication is chosen, ensure that employees use compatible biometric devices.
- Configure the MFA solution to enroll users' biometric data with a device-based invitation securely.
- Ensure that users' mobile devices are registered and managed securely.
- Configure the MFA solution to verify device integrity and security status.

(Optional) Implementation of FIDO2 Security Keys:

- Deploy FIDO2 security keys to all users who require access to the OT network.
- Configure the MFA solution to use FIDO2 keys for all authentication attempts.
- Educate users on the proper use and security of their FIDO2 keys.

Configuration of Access Control Systems:

BlastShield OT Security Gateway:

- Configure BlastShield to enforce passwordless MFA for all access attempts.
- Configure remote access accounts to require passwordless MFA.
- Ensure that remote access sessions are encrypted and secured.

Implementation of Zero Trust Principles:

Continuous Authentication and Authorization:

- Implement continuous authentication and authorization to verify user identity and device security throughout the session.
- Use contextual factors (location, time, device posture) to adjust access privileges dynamically.

Least Privilege Access:

- Grant users only the minimum necessary access to OT resources.
- Implement granular access control policies based on user roles and responsibilities.

User Training and Awareness:

Train Users on Passwordless MFA:

- Provide clear instructions on how to use FIDO2 keys, biometric authentication, or device-based authentication.
- Address any user concerns and provide ongoing support.

Monitoring and Logging:

Implement Comprehensive Logging:

- Log all authentication attempts, access requests, and security events.
- Monitor logs for suspicious activity and potential security incidents.

Security Information and Event Management (SIEM) Integration:

- Integrate logs with a SIEM system for centralized monitoring and analysis.
- Configure alerts for suspicious authentication patterns.

Benefits:

Eliminating Phishing Vulnerability: Passwordless MFA eliminates the primary vulnerability that phishing attacks exploit.

Enhanced Security Posture: Strengthens authentication and access control for the OT network.

Improved User Experience: Passwordless authentication can be faster and more convenient for users.

Reduced Risk of Data Breaches: Prevents unauthorized access to sensitive OT data.

Increased Compliance: Helps meet regulatory requirements and industry standards.

Stronger Defense Against Social Engineering: Even if a user is tricked into clicking a malicious link, the attack will fail without the presence of a password.

Use Case: Secure Remote Maintenance Access to OT Networks

TLDR: Exactly the right amount of access for OT Maintenance

You need to give outside vendors secure access to your OT network, but only to the right devices at the right times. Combine passwordless MFA with segmentation, ensuring strong authentication without risky passwords, and put up virtual segmentation fences, limiting access to only what's needed. Give your outside vendors a personalized keycard that only works on certain doors at certain times, keeping your systems safe and giving you total control.

Challenge Met:

Don't let contractors be the Achilles heel in your cybersecurity framework

Organizations can leverage a combination of passwordless MFA and network segmentation to enable secure third-party maintenance access to OT networks.

Passwordless MFA, utilizing methods like biometrics or hardware tokens, eliminates the risk of credential theft and phishing attacks, ensuring that only authorized contractors can access the network. This is further enhanced by network segmentation, which allows granular control over access permissions. By creating isolated network segments, organizations can restrict contractors to only the specific devices and systems they need to access for maintenance. This least-privilege approach minimizes the potential impact of a compromised contractor account. Additionally, access can be time-limited, granting access only during scheduled maintenance windows, further reducing the risk of unauthorized access.

This strong authentication and granular access control combination provides a robust security framework for managing third-party access to sensitive OT environments.

The Ideal World:

"Yet another day where you don't need to change your password"

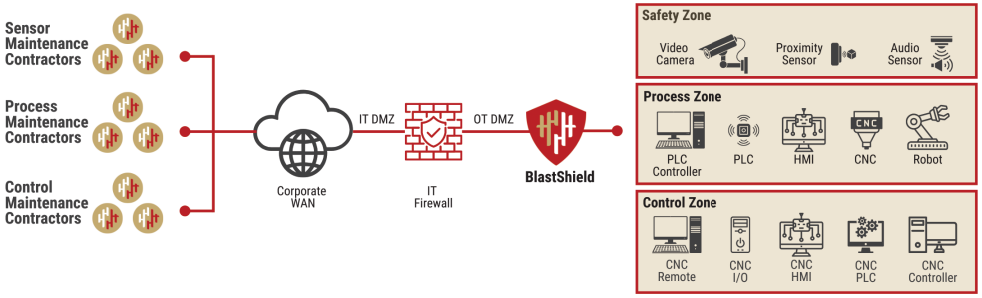
Imagine a world where bringing in outside help doesn't mean compromising your OT network security. Third-party contractors, essential for specialized maintenance, seamlessly connect with passwordless MFA, eliminating the risk of shared or stolen credentials: no more insecure passwords or phishing vulnerabilities.

Like virtual guardrails, segmentation guides them directly to the specific systems requiring attention. Access is precisely limited to the necessary devices and only during scheduled maintenance windows. The rest of your critical infrastructure remains invisible and untouchable, shielded from unintended access or potential mishaps.

This granular control fosters a secure ecosystem where external expertise is welcomed without compromising operational integrity. OT administrators breathe easy, knowing maintenance tasks are completed efficiently and securely, with minimal risk to their critical systems. It's a world where collaboration and security coexist, empowering organizations to leverage external expertise without compromising the safety and reliability of their operations.

Secure Remote Maintenance Access to OT Networks (cont'd)

How we do it:



Secure Remote Maintenance for OT Networks Using Passwordless MFA and Segmentation

Remote maintenance by contractors introduces security risks. Passwordless MFA and segmentation are critical to ensure secure access while minimizing the attack surface.

Key Technology Configuration:

Network Segmentation:

Dedicated Maintenance User Group:

- Create a dedicated user group for remote maintenance activities.
- Microsegmentation within the OT and Maintenance Zone:
- Segment the maintenance zone based on contractor roles and responsibilities.
- Use BlastShield's software-defined segmentation to restrict communication between micro-segments.

OT Device Isolation:

- Isolate the specific OT devices requiring maintenance within their own microsegments.
- Limit communication between these devices and other network segments.

Passwordless MFA Implementation:

Deploy BlastShield's Passwordless MFA Solution:

- Deploy BlastShield's passwordless MFA supporting FIDO2 security keys, biometric authentication, and/or device-based authentication.

Contractor Identity Management:

- Create dedicated contractor accounts with their user profiles and secure device enrollment

Biometric Authentication:

- If biometric authentication is used, ensure contractors have compatible devices and enroll their biometric data securely.

Device-Based Authentication:

- If device-based authentication is used, ensure contractor devices are registered and managed securely.

(Optional) FIDO2 Security Key Deployment:

- Provide FIDO2 security keys to all authorized contractors.
- Configure the MFA solution to require FIDO2 key authentication for all remote access attempts.

Remote Access Configuration:

Deploy BlastShield OT Security Gateway:

- Deploy BlastShield in the OT DMZ.
- Configure the gateway to require passwordless MFA for all access attempts.

Zero Trust Network Access:

- Implement ZTNA to enforce granular, identity-based access controls.
- Require continuous authentication and authorization throughout the remote session.
- Use contextual factors (location, time, device posture) to adjust access privileges dynamically based on the maintenance access needs for different device groups.

Time-Based Access Control:

- Implement time-based access control to restrict access to specific maintenance windows.
- Automatically revoke access after the maintenance window expires.

Security Policies and Procedures:

Contractor Agreement:

- Establish a formal agreement with contractors outlining security responsibilities and policies.

Security Training:

- Provide security training to contractors on passwordless MFA, remote access procedures, and OT security best practices.

Incident Response Plan:

- Develop an incident response plan for handling security incidents related to remote maintenance activities.

Regular Audits:

- Conduct regular security audits to ensure ongoing compliance and effectiveness of the remote maintenance configuration.

Monitoring and Logging:

Centralized Logging and Monitoring:

- Implement centralized logging and monitoring for all remote access activities, network traffic, and security events.
- Integrate logs with a SIEM system for analysis and alerting.

Benefits:

Reduced Attack Surface: Network segmentation isolates remote maintenance activities from critical OT networks.

Enhanced Security Posture: Passwordless MFA eliminates the risk of stolen credentials and phishing attacks.

Granular Access Control: ZTNA enforces strict access controls based on identity and context.

Increased Operational Resilience: Secure remote maintenance minimizes the risk of disruptions to OT operations.

Improved Compliance: Helps meet regulatory requirements and industry standards.

Use Case: Segment Flat Networks

TLDR: Software Defined Segmentation Beats Hardware Segmentation Every Day

OT Security should take advantage of software agility, not be stuck with hardware rigidity. Software-defined segmentation liberates you from the limitations of traditional firewalls. Instead of costly hardware upgrades and complex physical reconfigurations, you gain the power to create and modify network segments instantly, with a few clicks.

Challenge Met:

Segmentation Contains Threats and Minimizes Attacks

Network segmentation significantly reduces the attack surface and contains threats by dividing the network into isolated zones. This limits lateral movement, preventing an attacker who has gained initial access from traversing the entire infrastructure.

By enforcing strict access control policies between segments, organizations can restrict communication to only necessary traffic flows, effectively containing malware propagation and minimizing the impact of a breach.

This granular control enhances security posture and translates directly into business value by protecting critical assets, ensuring operational continuity, and reducing the potential for costly data breaches and regulatory fines. Segmentation transforms a monolithic, vulnerable network into a series of fortified micro-perimeters, bolstering resilience and preserving business integrity.

The Ideal World:

Segment to meet business needs

Picture this: granular control at your fingertips. You can micro-segment your network based on business needs, risk profiles, or even individual device vulnerabilities, without the constraints of physical cabling or appliance limitations. Need to isolate a compromised device? Done. Need to create a secure enclave for a new project? Instantly done.

This isn't just about saving money and time; it's about gaining unparalleled flexibility and responsiveness. Hardware firewalls are static, slow to adapt, and often create bottlenecks. Software-defined segmentation is dynamic, agile, and scalable. It's about empowering your security team to respond to real-time threats without disrupting operations. It's about building a security architecture that evolves with your business, not against it. It's OT cybersecurity security, redefined.

Configuring Port Isolation and Software-Defined Segmentation with a Managed Switch and BlastShield

This details the technical steps for configuring port isolation on a managed switch, followed by enabling software-defined segmentation (SDS) using a BlastShield device. This approach offers enhanced security by isolating ports and applying granular access control through BlastShield.

Components:

Managed Switch: Supporting port isolation, VLANs, and trunking.
BlastShield Device: Acting as a Zero Trust controller for microsegmentation.
Endpoints: Devices to be isolated and segmented.

Key Technology Configuration:

Port Isolation on the Managed Switch:

Implement Private VLANs (Recommended):

- Private VLANs provide Layer 2 isolation. Ports are designated as primary, isolated, or community.
- Isolated ports can only communicate with the primary port (BlastShield uplink).
- Repeat for all ports needing isolation, associating them with the appropriate isolated VLAN.

Alternative: Protected Ports (If Private VLANs are not supported):

- Protected ports prevent communication between other protected ports on the same switch.
- This is less granular than private VLANs but provides basic isolation.

BlastShield Integration:

Trunk Port Configuration: Configure the switch port connected to the BlastShield device as a trunk port. This allows all necessary VLANs (including the primary VLAN of private VLANs, or the native VLAN) to pass.
BlastShield Network Interface Configuration: Configure the BlastShield device's network interface to handle VLAN tagging, matching the trunk port configuration on the switch.
VLAN/Segment Mapping: Within the BlastShield management console, create network segments corresponding to the VLANs used for isolation.
Enable Zero Trust Authentication: Activate BlastShield's passwordless authentication or integrate BlastShield with an IdP (e.g., Active Directory, Azure AD) for user authentication and authorization.
Policy Creation: Define microsegmentation policies within BlastShield, specifying which resources users or devices can access.

- **Use zero-trust principles:** default deny, least privilege, and context-aware access.
- **Example:** Only authorized OT engineers can access specific OT devices within the isolated segment.

Policy Deployment: Deploy the BlastShield policies to the BlastShield device.

Endpoint Configuration:

Default Gateway: Set the BlastShield device as the default gateway for all endpoints within the isolated segments.

BlastShield Client (Optional): Install the BlastShield client on endpoints for enhanced security features and identity-based access.

Verification and Testing:

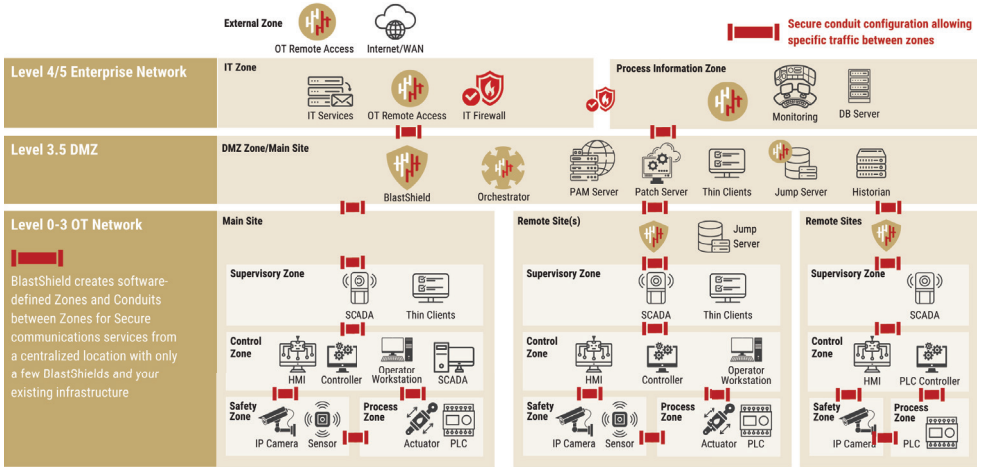
Port Isolation Verification: Verify that endpoints on isolated ports cannot communicate with each other directly.
BlastShield Policy Verification: Test the BlastShield policies by attempting to access resources from authorized and unauthorized endpoints.
Network Connectivity Testing: Verify that authorized endpoints can access resources through the BlastShield device.
Logging and Monitoring: Review switch and BlastShield logs for policy enforcement and network traffic analysis.

Key Considerations:

Private VLANs vs. Protected Ports: Private VLANs offer more granular isolation and are generally preferred.
BlastShield Placement: Ensure the BlastShield device is placed where it can inspect and control all traffic between isolated segments.
Performance: Evaluate the performance impact of BlastShield on network traffic.
Redundancy: Implement redundancy for critical components to minimize downtime.
Documentation: Maintain detailed documentation of the configuration.
Regular Audits: Conduct regular security audits to ensure ongoing compliance and effectiveness.

This configuration provides a strong foundation for securing sensitive network segments. The specific commands and options may vary depending on the vendor and model of the managed switch and BlastShield device.

How we do it:



BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to www.blastwave.com

v20250423

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use.
Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499