

Protection Zero Trust des réseaux industriels (OT)

Les réseaux industriels (OT, Operational Technology) assurent le fonctionnement des infrastructures qui alimentent nos villes et nos industries. Ils doivent garantir la continuité des opérations, protéger les équipements critiques et faire face à des cybermenaces qui évoluent. Une interruption peut avoir des conséquences physiques immédiates sur la sécurité des personnes, la fiabilité des installations et les services essentiels. Ces enjeux exigent une protection adaptée aux réseaux OT.

Aux États-Unis, plusieurs référentiels guident les exploitants d'infrastructures critiques dans la conception de réseaux sécurisés. Citons NIST SP 800-207 (Zero Trust Architecture), le NIST Cybersecurity Framework 2.0, le Zero Trust Maturity Model 2.0 de la CISA et la Zero Trust Reference Architecture du département de la Défense (DoD). Protéger le réseau en amont réduit la charge de détection, de réponse aux incidents et de rétablissement.

La matrice MITRE ATT&CK for ICS décrit notamment trois tactiques qui menacent les réseaux OT, de l'extérieur comme de l'intérieur : la découverte, l'accès initial et les mouvements latéraux. BlastWave indique que sa solution Zero Trust bloque des catégories entières de risques. En limitant l'exposition à distance et en réduisant la surface d'attaque, l'éditeur estime obtenir, face à d'autres solutions OT, un meilleur retour sur les investissements de réduction du risque (**Return on Mitigation**, ROM). Il annonce une protection réseau pour 84 des 90 risques étudiés.

BlastShield™

Bloquer la découverte

La dissimulation du réseau (**Network Cloaking**) empêche les outils de reconnaissance, y compris ceux utilisant l'IA, de repérer les équipements et leurs vulnérabilités.

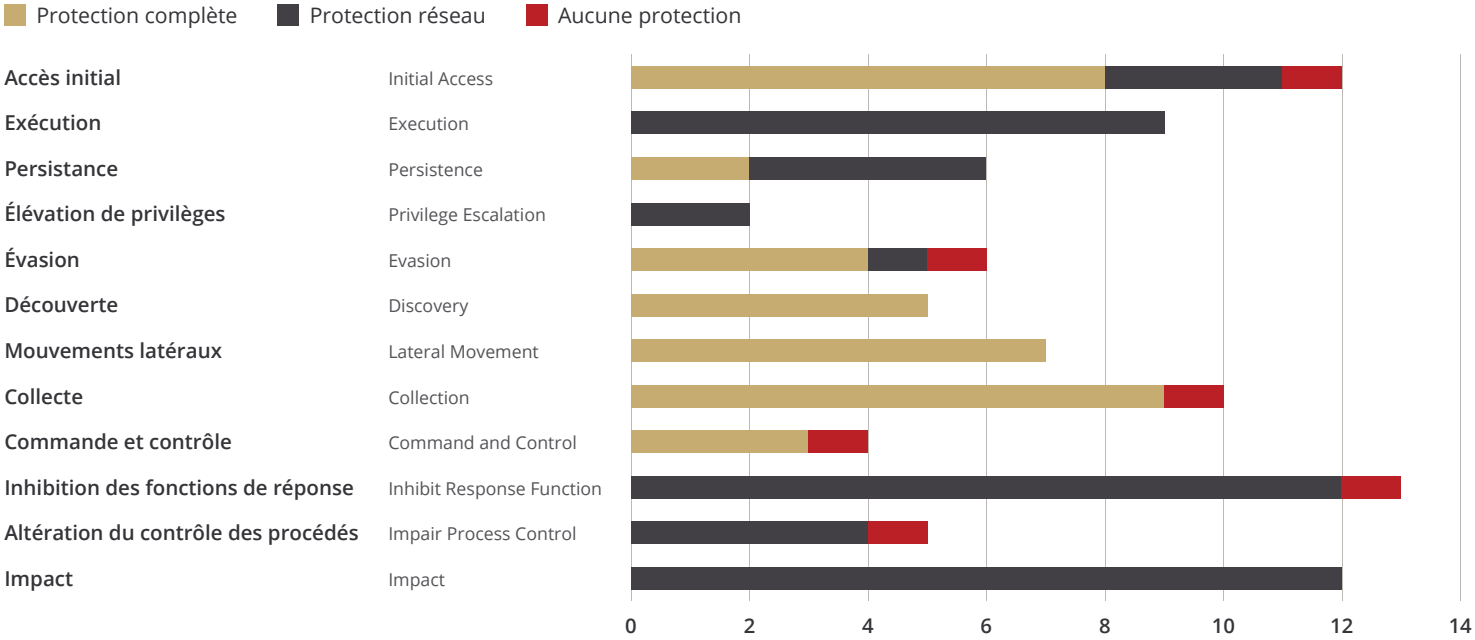
Bloquer l'accès initial

L'authentification multifacteur (MFA) biométrique résiste au phishing, sécurise les accès distants et contribue au respect des exigences réglementaires.

Bloquer les mouvements latéraux

BlastShield applique le principe du moindre privilège (**Least Privilege**) et la microsegmentation définie par logiciel.

Couverture de la matrice MITRE ATT&CK for ICS



Source : BlastWave.

La protection Zero Trust en environnement OT

Les priorités opérationnelles des réseaux industriels diffèrent de celles des systèmes d'information (IT). Le Zero Trust doit répondre aux contraintes de l'OT. Selon BlastWave, les pare-feu déployés ces dernières années n'ont pas, à eux seuls, apporté la protection attendue.

BlastWave cible les faiblesses à l'origine des cyberattaques. Sa plateforme étend la gestion des identités et des accès en combinant la dissimulation du réseau, l'authentification multifacteur sans mot de passe (**passwordless MFA**) et la segmentation définie par logiciel.

La dissimulation rend les équipements critiques invisibles aux utilisateurs non autorisés. Elle empêche leur reconnaissance et ferme ainsi une voie d'entrée. La MFA sans mot de passe élimine les failles liées aux mots de passe classiques et protège contre le phishing et le vol d'identifiants. Une segmentation fine crée des micropérimètres qui limitent les mouvements latéraux et la propagation d'une compromission.

Conçue pour l'OT, cette approche permet de traiter en amont les faiblesses exploitées par les attaquants. Elle renforce la protection des infrastructures critiques face à l'évolution des menaces et simplifie l'administration de la sécurité.

En associant dissimulation du réseau, accès distant sécurisé sans mot de passe et microsegmentation définie par logiciel, BlastWave vise à éliminer plusieurs catégories de risques et à améliorer le retour sur les investissements de réduction du risque (ROM).

Dissimulation du réseau

Network Cloaking

La dissimulation soustrait les équipements des réseaux OT aux scans et aux sondes externes. Elle ferme ainsi une voie d'entrée aux attaques assistées par l'IA et contribue au respect des principes Zero Trust en empêchant l'accès aux équipements vulnérables. Même assistés par l'IA, les outils de reconnaissance ne disposent d'aucun chemin vers le réseau OT interne pour en examiner le fonctionnement.

Accès distant sécurisé

Secure Remote Access

BlastShield permet d'administrer les systèmes OT à distance en temps réel, sans les exposer directement. Sa MFA biométrique résiste au phishing, y compris aux tentatives qui exploitent l'IA générative, ainsi qu'au détournement de la MFA. Un maillage complet de tunnels chiffrés de pair à pair (P2P) protège les flux sensibles mais non classifiés entre les utilisateurs distants, les réseaux OT et les systèmes équipés d'un agent. Ces tunnels protègent contre les attaques de l'homme du milieu (**Man-in-the-Middle**, MitM), sans imposer une interface unique accessible par navigateur et susceptible d'être vulnérable.

Segmentation du réseau

Network Segmentation

BlastShield simplifie la microsegmentation définie par logiciel (**Software-Defined Microsegmentation**). Des tunnels P2P chiffrés et authentifiés relient chaque équipement ou groupe d'équipements, sans jeu complexe de règles de pare-feu. Les équipes IT et OT et les prestataires temporaires accèdent uniquement aux systèmes dont ils ont la charge. Les droits peuvent être accordés ou révoqués en temps réel. BlastShield bloque les mouvements latéraux depuis les accès distants et peut aussi les bloquer sur les connexions locales en couche 2 (**Layer 2**).

Les six mécanismes de protection

1	2	3	4	5	6
Se protéger des attaques externes	Bloquer l'accès à Internet depuis les systèmes internes	Réserver l'accès initial à l'enclave OT aux identités authentifiées	Associer la MFA sans mot de passe à l'authentification de l'appareil	Limiter les droits au strict nécessaire pour bloquer les mouvements latéraux	Sécuriser les communications entre enclaves
					
Pare-feu de dissimulation Cloaking Firewall	**Isolement virtuel** Virtual Air Gap	**VPN d'accès distant sécurisé** Secure Remote Access VPN	**Biométrie et authentification de l'appareil** Biometric and Device Authentication	**Réseau local défini par logiciel** SD-LAN	**VPN maillé** Mesh VPN