Zero Trust OT Cybersecurity Protection for Governments

Governments are entrusted with safeguarding the very foundations of nations, protecting critical infrastructure that underpins public safety and security. BlastWave understands the immense responsibility you carry. Our Zero Trust solutions are purpose-built to fortify government OT networks against today's sophisticated threats, eliminating the root causes of cyberattacks and providing an impenetrable defense for your most vital assets. We empower governments to secure essential services with confidence, ensuring operational continuity and protecting the well-being of citizens.

Governments are responsible for keeping a nation's critical infrastructure operational for their citizens, but they are also responsible for securing government-operated networks. In the US, published specifications like NIST 800-207 (Zero Trust Architecture), CISA's Zero Trust Maturity Model 2.0, and the DoD Zero Trust Reference Architecture have helped government enterprises build secure networks.

The government sector runs Operational Technology (OT) networks like the commercial sector. Military bases and government facilities have power, water, and logistics infrastructure. Governments directly run water utilities, communications networks, national power grids, pipelines, and other OT infrastructures. Each agency responsible for that infrastructure must secure it per the relevant regulations and guidelines. These facilities are increasingly under attack by bad actors of all types.

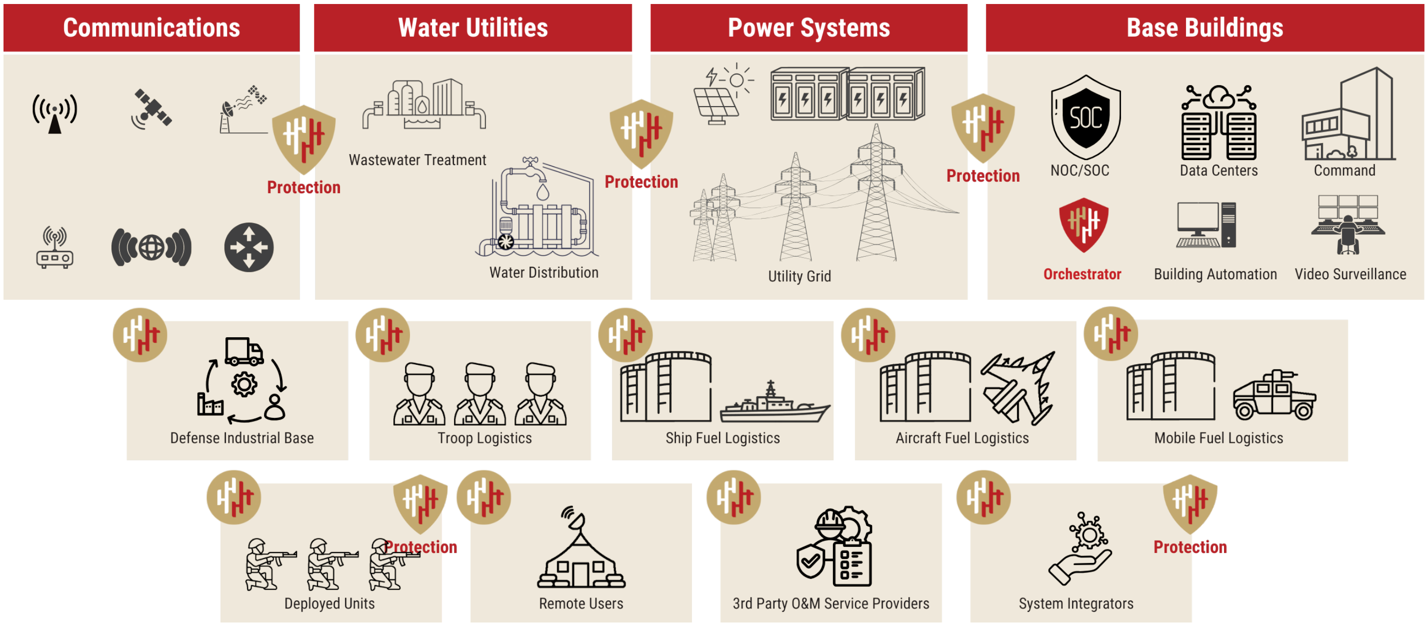
BlastShield

Rapid Deployment in 10% of the time required for comparable solutions and can be operated by traditional OT professionals and installed in hours, not days or weeks.

Zero Trust Protection that meets government needs across the globe and protects from hostile nation-states and AI-powered attack vectors.

Lowest Cost Of Ownership at 25% the cost of acquisition of traditional IT solutions and 50% less maintenance.

Figure 1 Defense OT Networks



BlastShield™: Zero Trust OT Protection For Government Critical Infrastructure

With BlastShield, government organizations gain secure remote access, network segmentation, and network cloaking, rendering critical systems undiscoverable to attackers and mitigating the risk of unauthorized access. BlastWave is aligned with NIST 800-53, 800-207 (Zero Trust), CISA Zero Trust Maturity Model, and the DoD Zero Trust Reference Architecture.

The scale and scope of the risk to government networks, especially its critical OT infrastructure, cannot be underestimated. Multiple reports have detailed the use of AI to aid attacks and hacking of government networks worldwide. The first line of defense in depth for government OT networks must be a solution that resists the initial threat vectors, phishing, reconnaissance, and no-code tools that are uplifted by AI, as reported by the UK government **(Table 1)**.

BlastShield presents a minimal attack surface toward the world, with only biometric-authenticated connections allowed to enter secure OT enclaves. Here are some of the government use cases BlastWave delivers:

Securing Water/Wastewater Infrastructure:

- Protecting water treatment and distribution systems from unauthorized control and contamination.
- Securing wastewater collection and treatment facilities.

Protecting Power Grids and Energy Systems:

- Securing power generation, transmission, and distribution networks.
- Protecting renewable energy infrastructure (solar, wind).

Enabling Secure Remote Access:

- Providing secure remote access for government employees and contractors.
- Facilitating secure collaboration between agencies.

Table 1

ROM Severity	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	**Moderate uplift**	**Moderate uplift**	Uplift
Social engineering, phishing, passwords	**Uplift**	**Uplift**	**Significant uplift (from low base)**
Tools (malware, exploits)	**Realistic possibility of uplift**	**Minimal uplift**	**Moderate uplift (from low base)**
Lateral movement	**Minimal uplift**	**Minimal uplift**	No uplift
Exfiltration	**Uplift**	**Uplift**	**Uplift**
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations - increasing volume of successful compromise of devices and accounts.

Securing Transportation Systems:

- Protecting traffic management systems (signals, control centers).
- Securing rail and subway control systems.
- Securing airport and aviation systems.

Protecting Public Safety Networks:

- Securing emergency communication systems (911, dispatch).
- Protecting HVAC, lighting, and security systems in government buildings.

Securing Defense Systems:

- Protecting military installations and bases.
- Securing weapon systems and control networks.
- Protecting communication and intelligence networks.

Compliance with Government Security Standards:

- Assisting with compliance requirements (NIST, CMMC, DoD Zero Trust, etc.)

Protecting Against Advanced Threats:

- Protecting against AI-powered reconnaissance and phishing.
- Mitigating the risk of Advanced Persistent Threats (APTs).

Network Security Fundamentals:

- Using network cloaking to hide critical assets.
- Using passwordless MFA to prevent credential theft.
- Using segmentation and microsegmentation to limit the impact of breaches.
- Implementing a Zero Trust architecture.
- Securing unpatchable legacy devices.

v20250408

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