Case Study

Securing the Foundation of the Fight

How Swish and Check Point are Hardening the Critical Infrastructure Needed to Ensure Department of War's Logistical Combat Readiness

THE CUSTOMER & THE MISSION

A combat force is only as capable as the supply chain behind it. As one of the largest logistics enterprises in the world, a Department of War agency that sustains the warfighter with everything from fuel and repair parts to medical supplies and subsistence operates across more than 80 sites worldwide. It supports a force of hundreds of thousands of personnel and maintains a presence on virtually every base across the globe with a footprint that has roughly doubled in five years.

That scale carries tangible strategic impact, because logistics is the foundation that mission readiness is built upon. In modern warfare, the first salvos are rarely kinetic as adversaries often target mission infrastructure, logistics, and supply chains through quiet cyber pre-positioning long before any shot is fired. Securing that foundation is no longer a back-office concern. It is a frontline mission.

THE CHALLENGE

To modernize and protect its physical infrastructure, including the warehouses, distribution operations, and industrial control systems that keep goods moving, the agency turned to its long standing partners Swish and Check Point to set up a new, dedicated Operational Technology (OT) security enclave spanning 24 to 25 sites. OT is a harder problem than traditional IT. Built around SCADA and industrial control systems, these environments were originally designed for isolated, reliable operation. They were never meant for today's hyper-connected, adversary-saturated threat landscape.

Two pressures were converging at once. The first was the threat. Basic packet filtering firewalls are no longer adequate against modern full-stack intrusions, and nation state actors are actively mapping and pre-positioning inside exactly the kind of critical infrastructure this agency runs. The second was the operational burden. With a fleet approaching 200 firewalls across physical, cloud, and scalable platforms, the daily work of administering security, configuring rules, hardening devices, and proving compliance, was consuming the very people whose attention the mission most needed on detection and response across their complete cyber landscape. Manual, device-by-device administration introduced inconsistency, human error, and delay, eroding mission effectiveness one change request at a time.

THE SOLUTION

Swish and Check Point built a defense on two pillars: next generation protection and intelligent automation.

At the IT/OT perimeter, Swish deployed Check Point next-generation firewalls across the OT enclave's hardware and cloud footprint. Unlike legacy firewalls that only check packets coming and going, Check Point's industry-leading next-generation firewalls inspect the full OSI stack and deliver intrusion prevention, identity awareness, and application-level control, all purpose built for an evolving threat environment. Swish brought deep OT expertise to the table, making sure the platform was scoped correctly, licensed efficiently, and implemented in alignment with the DoW OT Zero Trust Reference Architecture.

On top of that foundation, Swish engineered an automation and orchestration layer using Red Hat Ansible. What started as a handful of bare bones playbooks grew into a scalable enterprise capability: one touch provisioning, automated user administration, infrastructure deployment, repeatable security policies, and built in compliance checking, including automated STIG enforcement across every device. A task that once meant logging into 200 firewalls one at a time now runs in a single pass using Infrastructure as Code (IaC). Adding a security policy across the entire fleet dropped hours of manual work to roughly ten minutes.

THE OUTCOME

The combined solution delivered a more secure OT environment and a more capable team at the same time. By automating the repeatable administrative work, Swish stripped away the everyday toil that had been quietly draining mission effectiveness. That freed scarce cybersecurity talent to focus on optimizing posture and defending the enclave instead of chasing routine changes.

Just as important, the platform is built to flex to rapidly changing mission requirements and geopolitical realities. Through a flexible enterprise agreement, the agency can reprioritize requirements as needs shift, which is exactly the agility that mattered when the OT project surfaced on short notice. The result is critical infrastructure that is measurably harder to compromise and a security workforce focused on the threats that matter most to the mission.

THE IMPLICATION FOR GOVERNMENT

Every defense and federal agency now operates critical OT that cannot be compromised and most face the same twin pressures of nation-state cyber threats and a stretched workforce. This engagement offers a repeatable blueprint. Pair Check Point next-generation security solutions with Swish engineered OT security and automation capabilities to protect critical infrastructure while giving operators their time back to focus on the mission of the organization.

What sets Swish apart is not a product. It is partnership. Swish embeds knowledgeable, experienced engineers alongside the customer, understands the OT and defense landscape deeply, and develops optimized capabilities. Swish brings both the platform and the expertise to plan, implement, manage and optimize for mission outcomes. If the Department of War's Organic Industry Base (OIB) or critical infrastructure are the foundation of the fight, Swish and Check Point are the partners who keep that foundation secure.