SEALINGTECH®
a PARSONS Company

Secure Enterprise Modernization *in Action*

How do our integration, hardware and engineering services help the federal government stay safe in cyberspace?

We don't just develop and deliver our own advanced hardware for federal defense agencies and their partners around the world. Sealing Tech can also assist with repairing, modifying, installing and connecting the other digital solutions you rely on for safe field work. Thanks to our dedicated integration facility — not to mention the vast, evolving expertise we've accumulated over 15 years at the vanguard of cybersecurity — there are no limits to the configurations we can handle on your entire team's behalf.

Whether we're remotely upgrading and customizing your hardware in record time or visiting your site ourselves to discover what you need, it's all part of our Secure Enterprise Modernization (SEM) service. Want to see what this entails and how we've saved countless hours, filled talent gaps and covered major security risks on projects in the past?

Here are our SEM capabilities at a glance:

Configuring and installing system architecture

Upgrading legacy technology, migrating to the cloud and deploying the latest prevention, detection or mitigation techniques are the backbone to a robust security posture. We give DoD customers the ability to modernize their networks' edge rapidly without in-house engineering experience.

This involves:

- Sizing out suitable hardware, components and subcomponents for cyber operations.
- Handling significant network loads across locations.
- Integrating hardware with existing network systems.
- Designing solutions around general and regional cybersecurity compliance.

SEALINGTECH
a PARSONS Company

Once we configure hardware to meet the demands of your missions and security environment, we hand over simple build guides, showing you how each component can be plugged in and activated. "Rack and stack" integration collects switches, servers, cables and equipment in a bundle ready for launch. Furthermore, we apply Item Unique Identification (IUID) labels to show specific information through the item's lifecycle and retain a real-time serial number inventory, thereby bolstering security awareness for DoD contracts.

Ultimately, instead of spending months on installation, you can complete it within just a few weeks, substantially reducing required resources and billable time as new systems go live.

CASE STUDY: THE GLOBAL ENTERPRISE FABRIC (GEF)

SealingTech recently worked with the Army PEO EIS on its GEF program, designed to unify armed services applications across the globe. Our experts ensured that cyber equipment was prepared for quick, painless installation throughout 70 CONUS and OCONUS sites. We accomplished this by receiving inventory, adding IUID labels, performing hundreds of configs and upgrades, drawing up Q&A documentation, revising site installation guides and bundling everything for unique locations before shipping them out.

CASE STUDY: VOICE OVER INTERNET PROTOCOL (VOIP)

We assisted the Army's PAC VoIP-Pacific IP P2E transition over several years, replacing existing analog voice service exchanges and implementing Telephone Management Systems (TMS) for designated B/C/P/S/P/P. Meanwhile, we configured the equipment for relevant unified call managers, so they could set up connectivity and contact field operatives anywhere via voice or video. Again, we utilized site-specific configurations, IUID labels, burn-in, inventory assessments, in-depth documents and a carefully managed shipping schedule to Okinawa, Alaska and Hawaii.

Round-the-clock monitoring

Setting up the right hardware is half the battle for reliable cyber activity that never leaves you exposed unawares. Much of our SEM work encompasses intrusion detection for enterprise security, finding and stopping threats before they emerge. SealingTech's Critical Response Team (CRT) specialists use cutting-edge threat intelligent tools to analyze, triage and respond to potential breaches with:

- Firewalls and intrusion detection systems.
- Automated processes to block or contain certain users and endpoints.
- Sweeping forensic capabilities backed by rich reports.

In essence, we prevent genuine threats from entering your network or causing widespread damage. This relies on determining a security tool's entire lifecycle from inception to installation and beyond, watching out for anomalous behavior on a daily basis. The CRT works from multiple security centers. They can discover, for example, why failover configurations aren't replicating properly or whether attackers have hidden rootkit in your system for backdoor access.

SEALINGTECH
a PARSONS Company

CASE STUDY: GUARD ENTERPRISE CYBER OPERATIONS SUPPORT (GECOS)

Even our closest competitors don't have the same breadth and depth of cybersecurity awareness to give huge modernization projects the protection they deserve. SealingTech's role in the ARNG's GECOS development is a case in point. We offered 24/7 maintenance and monitoring as this federal force sought to guard its new infrastructure, applications, hosts and digital programs. By gathering security specialists in NOC, SOC and CIRT, we've given the ARNG a defense perimeter it can trust for decades ahead.

Consolidating the virtual and physical environment

What drives efficiency in federal-level cybersecurity? Comprehensive, capable IT architecture can bring high energy, manpower and security costs if hundreds or thousands of devices are spread across disparate locations without unified standards to install and maintain them. That's why SealingTech also provides SEM consolidation to reduce the number of facilities, servers and staff required to keep your systems safe and productive.

We pull this off using:

- Assets that we and our customers can remotely manage.
- Hardware such as Cisco and VMWare for virtualization.
- Combinations of node clusters and sites with standalone hosts.

By helping our DoD clients become more efficient, we've generated specific templates and repetitive process automations that cut even the most complicated projects down to size.

CASE STUDY: NIPR, SPPN AND ENTERPRISE SERVER REFRESH

The CSRA/Army National Guard Bureau headquartered in Arlington, VA, used SealingTech for consolidated cybersecurity in 2019. We implemented a standardized architecture and virtualized platform, complying with operations orders on a Windows Server 2012R2 with room for expansion. A "single pane of glass" was subsequently achieved, halving the CSRA's four SPPN sites down to two. We then helped replace outdated, out-of-warranty, inconsistent legacy environments, making them fit for modern security challenges.

Seal the deal on critical defenses with SEM

In 2022 alone, we configured and/or installed over 20,000 devices for the DoD, shipping to 138 CONUS and 22 OCONUS locations. Our speed, compliance and quality remained undiminished at every turn. What's next for your own cybersecurity modernization efforts?

SPEAK TO A SEALINGTECH REPRESENTATIVE FOR A CONFIDENT HAND WITH THE HARDWARE YOU TRULY NEED. →