eBook

Forcepoint | Powered by ConversationalGeek

Federal Remote Work Year in Review:

Stories from the Field about How Government Agencies Adjusted to Pandemic Pressures

Introduction

2020 presented unprecedented challenges to Federal Government Information Technology (IT). The COVID-19 pandemic took the world by storm as people fled their offices to work from home. Organizations scrambled to adapt, with IT departments working overtime, implementing infrastructure changes to accommodate the new work dynamic. This was an enormous challenge for commercial organizations. However, the situation was even more dire for the United States Federal Government. Many federal jobs, especially those in classified environments, could not be easily transitioned to remote working. For mission-critical employees, there was no choice but to continue reporting for duty. But for the vast majority of federal workers, government agencies were able to come up with innovative solutions to keep their employees safe and productive while working remotely. And this is what this eBook is about: real-world anecdotes from the field about how different government organizations and their contractors were able to persevere in the face of adversity and stay true to their mission through the pandemic.

> "It's been as intense and focused as it was from day one. And it's still that way today because there's a deep understanding of the criticality of our mission."
>
> **DAVE MCDONALD**
> **NAVY CIO, NCTAMS PAC**

The Army story of enabling remote classified work

We start with an account of how the Department of the Army maintained its critical mission operations throughout the pandemic.

We spoke with Major General (MG) Joseph Brendler about his experiences in tackling the challenge of classified network access from warfighters' home offices[1]. MG Brendler spent 32 years on active duty in the Army, where he was Chief of Staff for the United States Cyber Command (USCYBERCOM) and, prior to that, the US Army Director of Architecture, Operations, Networks, and Space under the Army CIO/G6.

[1] Brendler, Joseph and Kamis, G. "Blueprint for the Future of Cloud Multi Domain Operations." AFCEA SIGNAL, 6 October 2020

Obviously we cannot go into specifics, but we can describe the challenges and solutions in general terms. The Department of Defense (DoD) global combatant command has a requirement for its operators to access multiple networks at different security classification levels, potentially all at the same time. These networks may include:

- **Open public Internet**
- **Non-classified Internet Protocol Router Network (NIPRNet)**
- **Secret Internet Protocol Router Network (SIPRNet)**
- **Joint Worldwide Intelligence Communication System (JWICS)**
- **Government Wide Area Network (GWAN)**
- **Mission specific networks and many more**

For the longest time, most DoD offices that required this kind of network connectivity looked something like the picture to the right:

Figure 1 - The world before Cross Domain Solutions (CDS)

With the miniaturization of technology over the years, an office full of computers and monitors has morphed into a desk full of computers and monitors. The picture to the right shows a typical workstation setup inside of a Sensitive Compartmented Information Facility (SCIF) for multi-domain operations.

Come March 2020, the pandemic hits and the government orders everyone to go into lockdown and work from home. The challenge is, how do you take the setup pictured to the right to your home office?

This is where the National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) program came to the rescue. The CSfC program was developed by the NSA to allow commercial technology vendor products to be used for access to National Security Systems (NSS). A vendor who wishes to be included on the CSfC-approved product list must build their product in accordance with U.S. Government Protection Profiles and submit their products using the Common Criteria process. The NSA then enters into a Memorandum of Agreement (MOA) with the vendor and places their product on the CSfC-eligible commercial products list.

Figure 2 - Typical Workstation Setup for Multi-Domain Operations in Classified Environment

Through innovative use of commercial technologies, the U.S. Army was able to consolidate multiple monitors, computer enclosures, KVM switches, and network connections into a single system called Cross Domain Solution, or CDS. The user-facing component of CDS is a thin client: a monitor and a connection box with no local persistent storage to eliminate the need for further CSfC data at rest encryption requirements. This allows the end user device to be considered classified only when connected to a Virtual Private Network (VPN) with a virtual desktop infrastructure (VDI) session open. Common VDI and redisplay technologies supported include Citrix, Microsoft, and VMware. When disconnected and powered off, the end user thin client device reverts to an unclassified state per Defense Information Systems Agency (DISA) guidelines. For remote worker deployment, the CDS thin client is packaged into a kit with portable security gateways (e.g., small form factor firewalls) that provide inner and outer tunnels for dual encryption. Dual encryption is required by the NSA's CSfC for transmitting classified data over an unclassified network. An Army employee can then take this "remote work kit" home and perform his or her NSS job duties from the comfort of their home office.

Several commercial vendors took the thin client idea to the next level by creating a thin client remote app that can be installed on a CSfC-approved laptop computer. This approach eliminates the need for "kits" of equipment to be shipped out to remote workers. MG Brendler describes how he embraced this technology to enable continued Army mission support during the pandemic:

> "We have government customers who simply ran out of space under their desks for all the boxes associated with different networks. So, a CDS Thin Client solution was readily welcomed."
>
> GEORGE KAMIS, FORCEPOINT FEDERAL CTO

"I was thrilled to see an example of this in action. The Army's Seventh Signal Command has been using a combination of Trusted Thin Client and CSfC to re-wire its campus at Ft Gordon. When requirement to respond to COVID-19 emerged, command was asked if the same technology would support remote work environments. The answer was a resolute YES. We now have the ability to do classified work while working remotely."

MG Brendler further emphasized the importance of convergence for multi-domain solutions:

"Convergence is the notion that you converge the capabilities from all the domains operating simultaneously to achieve the desired effect – overwhelm the adversary. This requires continuous real-time connectivity between sensors and shooters in all those domains. Since all are operating at various levels of sensitivity, we need to provide intentional cryptographic isolation, while also allowing operatives to share information between them. This is only possible with a Cross Domain Solution."

The positive experience of implementing CDS functionality as a thin client app paves the way for cloud providers to explore CDS-as-a-Service offerings in the future. Taking an on-prem CDS VDI solution and pushing to in the cloud offers tremendous financial savings and enables resilience for the Army as a whole. No need to buy hardware, just subscribe to it in the cloud. Transformational technologies like this are removing the complexities of IT, providing endless scalability, v and giving users the seamless ability to connect to multiple classification levels and cloud resources at the same time. In the near future, Army users will be able sign into Microsoft 365 (M365) and drag and drop files to a classified environment, and this will all be enabled by Cross Domain in the Cloud. As Joint Enterprise Defense Infrastructure (JEDI) and Commercial Cloud Services (C2S) continue to grow, the Army will be bringing in new technology partners to these environments. There are currently multiple pilots, that will continue past the pandemic. One thing is for certain: the pandemic accelerated the Army's transition to a new model of multi-domain environment consumption and fast-tracked the development of a CDS-as-a-Service consumption model.

The Pentagon success story of 1 million remote workers

We just reviewed the classified side of the Defense business.

But what about unclassified environments? We're talking Microsoft 365, Word, Excel, email, and teleconferences. It all started on 19 March 2020. That day, California issued the nation's first stay-at-home order for residents, and on the same day, the DoD began sending employees home. This day marked the beginning of a race to set up telework for the largest employer in the world – the United States Department of Defense - with almost 1 million civilian employees and close to 2 million active-duty military, National Guard, and reservists.

The race to set up telework began with the obvious: upgrade network infrastructure, increase circuit size, and expand VPN capacity. However, the DoD still needed a collaboration platform. The solution came in the form of a Commercial Virtual Remote Environment, or CVR. The platform bundled Microsoft 365 and Teams to enable teleconferencing, chat, and document sharing. Unlike typical software procurements and deployments that take months or years, the new CVR platform was rolled out in a matter of weeks and boasted over 1.3 million users[2]. It quickly became the largest Microsoft Teams deployment in the world and brought department-wide collaboration tools to the DoD after years of less successful attempts[3].

[2] Eversden, Andrew. "Pentagon shattered speed record to give [1] million people remote work tools." C4ISRNET, [11] January 2021
[3] Schneider, Troy. "Sunsetting CVR but keeping the collaboration." Federal Computer Week (FCW), 23 April 2021

> "I would argue that if we had brought in Teams and had done the normal research, testing, socialization, pilot rollouts ... [CVR deployment would have taken] the better part of a year."
>
> DANA DEASY, DOD CIO

What makes the story of CVR special is that it showcases the DoD overcoming typical IT contracting barriers to fast-track the software development process on a massive scale. It disproves the myth that the DoD is a slow-moving behemoth incapable of resiliency. The CVR roll out is heralded as the ultimate example of flexibility and speed in the U.S. Federal Government. Cloud Computing Program Office (CCPO) Director Sharon Woods describes the process: "people gave up full nights of sleep to deploy the software. Naps came intermittently throughout the day. Showers? Rare. Baseball caps covered unwashed hair. Coffee was king. Looking back on it, it's almost a little surreal."

In early March 2020, the DoD CIO's office created a telework task force that included all the Pentagon IT leaders: service CIOs, representatives from the Joint Chiefs of Staff, Cyber Command, the NSA, and DISA. The task force had to deliver a suite of tools to employees that differed from the ones with which they were familiar. Beyond the issue of scaling the CVR platform to more than a million people, the next challenge was training all those people how to use it. And before training could begin, the task force needed to understand the collaboration requirements of the different DoD components.

"Oftentimes, you spend the first few years just trying to make sure that everybody clearly and completely agrees on the requirements," said Vice Admiral Nancy Norton, director of DISA. "Well, we didn't do that for this at all. We said: 'OK, here are the basics for the requirements. Now let's start building and let's start delivering, and that's the minimum viable product.'"

The CVR Environment on which the telework task force settled was a temporary platform accredited at DoD Impact Level 2 (IL-2), which allows for transmission of unclassified information approved for public release. To roll out the CVR platform, the Pentagon leadership decided to undertake a DevOps approach, whereby a minimum viable product (MVP) is delivered first and additional capabilities are added incrementally over time. For the small CCPO team, March 19 marked the start of a nearly nonstop effort to roll out the CVR platform. "We worked 24 hours a day, seven days a week, and that's not an exaggeration," Woods said. The CVR MVP that CCPO introduced was a "bare bones" version of Teams. The first test accounts were online by March 20, about 24 hours after the telework task force started work on CVR requirements. By March 25, the first pilot users were live, including testers at the highest levels of the Pentagon: flag officers, general officers, and senior executive servants (SES). Within a week, CVR was cleared for department-wide use. That's resiliency!

> "CVR just obliterated the myth that it takes years for the department to deploy a capability at scale."
>
> SHARON WOODS, CCPO DIRECTOR, DOD

The CCPO continued to enhance the CVR platform throughout the pandemic. The success of the CVR initiative led the DoD to develop a permanent remote collaboration solution with a stronger security component. The new collaboration solution is being rolled out in the summer of 2021.

Stories of COVID burnout and fatigue from Department of the Navy

In this section, we would like to shift gears from discussing the technology of enabling remote work to the human element of dealing with the pandemic. For this section we spoke with Dave McDonald, who is the CIO for Naval Communications (NCTAMS) Pacific (PAC) 4. Below, we present Dave's insights into how the Navy and the greater DoD workforce was coping with the pandemic on a human level.

[4] McDonald, David, Trexler, E., Ford, C. "Dave McDonald: The Crisis CIO, Marathon Mode, Part 1 – Episode 109." To the Point Cybersecurity, 15 December 2020

The early months of the pandemic felt like a sprint to quickly adapt to the new normal and deploy the infrastructure to accommodate the remote work force. However, the entire workforce soon settled into "marathon mode," but without knowing when the marathon will end. No one knew what was coming next or when the pandemic would end, and it created psychological strain on the workers.

> "There's a fatigue and a burnout that's making its way in trying to execute these critical missions. It's making it all look normal when there's really nothing normal about it. I think really attentive, in-tune leaders need to pay attention to people and constantly ask and probe."
>
> DAVE MCDONALD, NAVY CIO, NCTAMS PAC

Dave emphasized that we have to remind ourselves that the work of the DoD is "not that much different than other significant, mission-essential segments of our economy, our nation, our culture, our world." The work is vital to national security and must get done, but now within the new parameters of the pandemic. Adapting to the multitude of changes happening at once is incredibly challenging for most humans. But the Navy workforce was able to hit a stride, like how runners hit their stride while running a marathon. "You know what the [marathon] is going to be because you've trained for it. And you count yourself as pretty resilient, pretty tough. But there's this notion of hitting stride and overcoming pain, overcoming the fatigue."

Dave further elaborates on what "hitting the stride" looked like for his Navy team:

"Our missions are all critical, we have to execute them. We are actually hitting stride in the sense that we've learned a lot in adapting to new routines. We've figured out how to host visitors that are essential. Maintenance, systems engineering visits, installation visits, things that are really critical business that have to be carried on. We've learned how to protect our critical watches, the 24/7 operations and maintenance crews. We have learned how to do that with really remarkably good success."

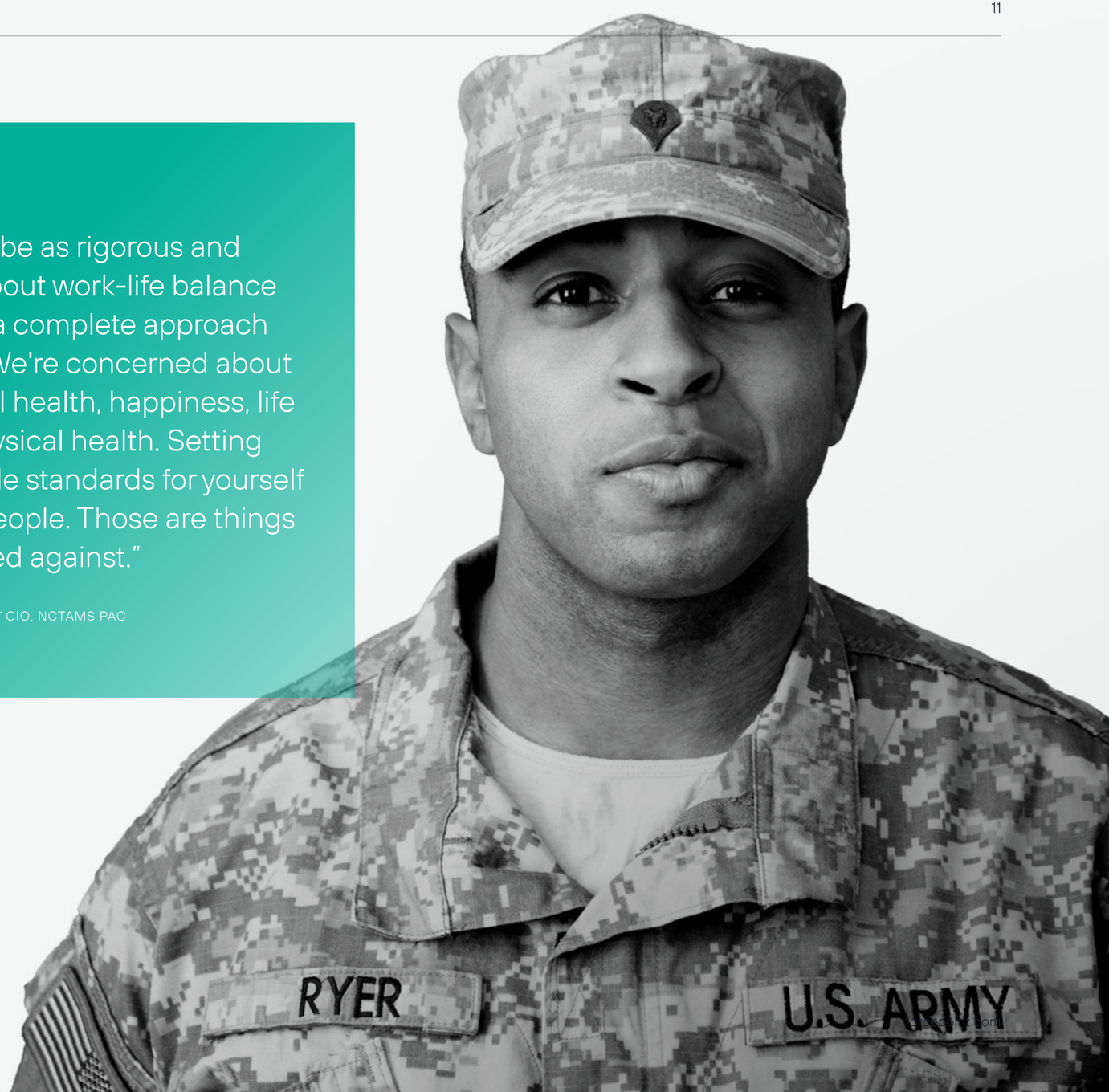
In tackling the issue of human stressors, Dave pointed out that military personnel should not be afraid to ask for help. Many people in the military tend to regard themselves as warriors.

"They pride themselves on stoicism and courage and taking the pain, muscling through. The whole traditional cultural foundation of special operations is a silent, stoic, tough, resilient warrior."

But that mentality is fraught with peril. People hold too much in, suffer in silence, and end up with PTSD and other mental health issues when they leave the service. So, what do we do to help people? "Number one is, making sure they know they're part of a team. They're part of a professional family. Their leaders and supervisors and peers care about them. They should not suffer in silence. There is mentorship, life coaching, and life counseling help to be found." The DoD and Department of the Navy offer many resources to help personnel deal with burnout and fatigue. The main message is to NOT hesitate to ask for help. Everyone is mission critical.

"You want to be as rigorous and complete about work-life balance and having a complete approach to your life. We're concerned about you – mental health, happiness, life balance, physical health. Setting unreasonable standards for yourself or for your people. Those are things to be guarded against."

DAVE MCDONALD, NAVY CIO, NCTAMS PAC



IT Supply Chain Lessons Learned from CISA

Even though this is not exactly an anecdote from the field, the 2020 pandemic did highlight weaknesses in the world's supply chains. These supply chains affect not just commercial vendors but also the government agencies that rely on technologies provided by these vendors. Therefore, it is essential for U.S. national security to understand the supply chain vulnerabilities uncovered during the pandemic and potential ways to address them going forward as life returns to normal. To that end, Cybersecurity and Infrastructure Security Agency (CISA) put out a publication outlining practical recommendations that can support policy and operational decisions to strengthen and build additional resilience into federal government supply chains in the future[5].

It's a lengthy read, but we will summarize the salient points here.

1. The pandemic highlighted the need for diversifying supply chains to a broader array of geographic locations and away from single-source / single-region suppliers.
2. The pandemic exposed vulnerabilities of manufacturing companies with reliance on lean inventory models, which provide great efficiency and cost effectiveness in normal environments.
3. COVID-19 underscored the difficulties that companies face in understanding their second- and third-tier (junior-tier) suppliers, and often lack transparency about their geo-location and business practices.

[5] CISA, Building a More Resilient ICT Supply Chain: Lessons Learned During the COVID-19 Pandemic: An Analysis, November 2020

The pandemic has been a wake-up call for both the commercial sector and the U.S. Government. Technology vendors, after assessing costs and benefits, need to adjust their supply chains to reduce future risk. This may include moving in and out of certain geographic regions, developing enhanced but practical approaches to risk mitigation, and diversifying supply sources. Based on industry research and analysis conducted by CISA's Supply Chain Risk Management (SCRM) Task Force, CISA makes the following practical recommendations to U.S. Government agencies to increase their supply chain resiliency:

- **Proactive risk classification:** Agencies may consider deploying a systematic classification of risks, continually analyzing development and events that are happening around the world, and undertaking the development of a response strategy to improve supply-chain resiliency strategically.
- **Map vendors' corporate supply chains:** Agencies may want to work with their vendors to develop a detailed map of junior-tier suppliers as a critical step to detect hidden relationships that impede adding resilience.
- **Look for vendors with broad supplier network:** Eliminate and reduce the risk of a single source of critical components when possible; look for technology vendors that increase resiliency and redundancy in their networks by dual-sourcing supply from multiple or lower-risk regions.
- **Development of Standardized Mapping Tools:** Agencies may benefit from the development of standardized approaches and tools for supply chain mapping that would more effectively identify locations of sub-tier suppliers and help uncover upstream logistical bottlenecks.
- **Work with vendors to ensure they have the optimal amount of inventory:** Agencies should work with suppliers to make sure they maintain an adequate amount of inventory for expedited equipment servicing and replacement.

The pivot to mass remote work for U.S. Customs and Border Protection

Like the rest of the U.S. Federal Government agencies, U.S. Customs and Border Protection (CBP) was forced to send most of its employees home in mid-March 2020, and support agency-wide telework.

For this section, we lean on personal accounts of Edward Mays, executive director of the Enterprise Data Management and Engineering Directorate at CBP[6]. Overall, the transition to support 7,000 employees across CBP was a scramble, but not anything traumatic. CBP has been doing emergency exercises to support remote workers even before the pandemic, so, Mays feels, the agency was ready and able to deliver.

[6] Hennick, Calvin. "The Pivot to Mass Remote Work: CBP Found a 'Great Opportunity to Learn'." FedTech Magazine, 21 July 2020

When asked about technologies that were already in place and whether CBP needed to adopt any new ones, Mays explained that before the pandemic, CBP primarily relied on VPN services provided by a large legacy network vendor. In the first weeks of March, CBP was able to literally "dig out of the closet" old VPN appliances and get them operational as a temporary measure. However, within weeks, CBP brought online additional remote-access technologies from a large firewall manufacturer that provided CBP "the ability to remain connected even when away from the site. It's important from the perspective of cybersecurity, because newer technology allowed [CBP] to get updates to laptops and other mobile devices in a better manner than the previous tool."

Similar to how the Pentagon was able to roll out the CVR Environment, CBP implemented its own version of Microsoft 365 deployment. "We took on about 73,000 individual customers, updated 10,000 dynamic distribution lists, and we were able to do that in six months. Our mission in terms of trade, travel, law enforcement, border security, all those things, demands that we have that capability, and we were able to push that out to all those users. With the Microsoft 365 toolset, you get an incredible amount of collaboration tools, such as Teams, video streaming – just a plethora of capability."

Initially, the IT leadership was apprehensive about scaling the M365 solution too quickly because of the reduction of on-site personnel supporting the CBP enterprise operations center, which is the nerve nexus for the monitoring of all CBP applications and infrastructure, both on-premises and in the cloud. "Having those people not there, having [enterprise operations center] only minimally manned, was a bit of a concern. But people are adjusting and using collaboration tools, doing their monitoring from wherever they are physically, and it's worked out well."

> "It's a little bit different from being able to turn to your left and two feet away would be a peer whom you could ask a question. We're having to do that virtually, but we're getting it done."
>
> EDWARD MAYS, EXECUTIVE DIRECTOR, U.S. CBP

When asked about how he sees the pandemic affecting the future of work, Mays said he believes that "this event is going to force us to push more capability down to mobile users in terms of their phones, their iPads, etc., where that capability, which may have been more office-centric in the past, will be much more available to [workers] on mobile platforms. Just having that capability at hand inherently will cause some sort of organizational change and drive us to become more effective and efficient. That's what technology does for us."

> "I think technology will inherently change the way we do business in the future, and, hopefully, facilitate efficiency and effectiveness for our frontline teammates, which is where it really counts."
>
> EDWARD MAYS, EXECUTIVE DIRECTOR, U.S. CBP

A story of a Defense Contractor

We conclude with a story of implementing novel technologies to overcome encumbrances posed by legacy VPNs.

Over the course of 2020 we read many stories about "working from home," and most of the technology coverage touched on the topic of VPN and how legacy VPN concentrator appliances were buckling at the load of remote users connecting back into the corporate data centers. Here we would like to present another VPN story, but one that relies on an innovative firewall technology to enable remote workers instead of creating a bottleneck. A technology that integrates full SD-WAN connectivity, advanced high-availability clustering, and strong security in compact desktop appliance, managed at enterprise scale from a single pane of glass.

A Defense Contractor, who shall remain nameless for security reasons, was performing classified work in support of the U.S. Government cyber operations. The contractor had several hundred engineers developing cyber capabilities for the DoD. The work required staff to access an isolated engineering environment, which provided tools and network infrastructure required for product development and testing. Because of the sensitivity of the cyber capabilities being developed, it was critical that this environment remain isolated from all other networks and enterprise systems. Staff were approved to connect to the engineering environment on a limited, as-needed basis. Remote connectivity was enabled by a custom VPN solution from a legacy network vendor that was challenging to maintain and required components with extended lead times.

In March 2020, when virtually everyone was sent into lockdown and ordered to work from home, access to the engineering environment became a challenge. The legacy VPN solution was unable to meet the new demand of the entire engineering staff trying to access the environment remotely. Work couldn't get done. A new scalable solution was needed.

While evaluating vendors for a replacement solution, it became clear that legacy firewall vendors could not accommodate this particular use case. What was required was having hundreds of compact desktop firewall appliances distributed to all engineering staff and maintaining persistent, high bandwidth connections to the isolated engineering environment. Moreover, the appliances aggregating the connections had to offer advanced clustering capabilities to eliminate downtime and to accommodate firmware updates and hardware failure. Additionally, appliances needed to have built-in SD-WAN traffic management capabilities to enable links from more than one Internet Service Provider (ISP) to be used at the same time to further reduce the chance of outages.

Within just a couple weeks from initial evaluation, the Defense Contractor was able to successfully deploy over 300 firewall appliances and two central management servers operating in High Availability (HA). The final solution was able to support key technical requirements outlined above as well as provide encryption of data in transport and isolation of network traffic. Thanks to the robust central management capability, the solution was rolled out in days, with consistent policies and rule sets deployed on all remote devices. Following the deployment, the solution continues to provide a strong return on investment (ROI) by allowing Defense Contractors to support complex firewall rule sets across all devices, secure re-provisioning of devices, authenticate users via a capture portal, and report security concerns withing external remote work environment networks.

Parting Words

The world changed in profound ways in the face of the COVID pandemic. Work-from-home is the “new normal” and will remain so even as the world is slowly coming out of crisis. the U.S. Federal Government faced unique challenges in that, traditionally, most federal employees work out of an office.

The pandemic forced federal agencies to rethink the old way of doing things, which is never easy. Ultimately, as we’ve seen from the anecdotes in this eBook, most agencies have come through with resounding success and established a path forward for their employees to work better. The silver lining of the pandemic is that it accelerated the digital transformation of U.S. Federal Government departments and agencies, made them more resilient, and enabled them to better serve their mission.

“I use the old military adage “mission first, but people always,” It’s easy to task people when you really can’t see all the additional things that they’re having to deal with in this environment, and this definitely is a different environment than anyone has ever worked in before. We definitely have to make sure we take care of our people.”

EDWARD MAYS, EXECUTIVE DIRECTOR, U.S. CBP

Glossary

C2S	Commercial Cloud Service for U.S. Intelligence Community
CBP	Customs and Border Protection
CCPO	Cloud Computing Program Office (Pentagon)
CDS	Cross Domain Solution
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CSfC	Commercial Solutions for Classified
CVR	Commercial Virtual Remote Environment
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
HA	High Availability
IL	Impact Level
IP	Internet Protocol
ISP	Internet Service Provider
JEDI	Joint Enterprise Defense Infrastructure
JWICS	Joint Worldwide Intelligence Communication System
KVM	Keyboard Video Mouse switch
MG	Major General
MOA	Memorandum of Agreement
MVP	Minimum Viable Product
NCTAMS	Naval Computer and Telecommunications Area Master Station
NIPRNet	Non-classified Internet Protocol Router Network
NSA	National Security Agency
NSS	National Security Systems
O365	Microsoft Office 365
PAC	Pacific
PTSD	Post-Traumatic Stress Disorder
ROI	Return on Investment
SD-WAN	Software Defined Wide Area Network
SCIF	Sensitive Compartmented Information Facility (SCIF)
SCRM	CISA Supply Chain Risk Management Task Force
SIPRNet	Secret Internet Protocol Router Network
USCYBERCOM	United States Cyber Command
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Federal Remote Work Year in Review eBook Geek Guide 20AUG2021