ARTICLE

COMPLY TO CONNECT: MAINTAINING A SECURE ENVIRONMENT REQUIRES AN INTEGRATED RISK VIEW

Separate Network Access Control Solutions Struggle Against DoD's Sprawling Attack Surface

The United States Department of Defense (DoD) regularly confronts a daunting mission-critical task: Providing continuing cybersecurity over its own complex and vast Infrastructure & Communications Technology (ICT) while protecting against an onslaught of sophisticated adversarial cyber intrusions, along with furnishing the same cyber defense for thousands of shared DoD Information Network (DoDIN) systems, networks, applications and millions of connected end-user devices. DoD must protect all of its equities, without exception.

Each potentially adverse encounter begins when an endpoint device, situated anywhere in the world, attempts to connect to a DoD network. In turn, the vital first line of DoDIN defense increasingly represents the Department's promising enterprise Comply to Connect (C2C) program. C2C collectively signifies a framework for validating new devices, evaluating their compliance with DoD security policies and continuously monitoring these assets to ensure they remain secure. Applying this framework, the Defense Department seeks cybersecurity situational awareness (SA) — that is, to comprehensively understand what devices are on the network, what assets or software is deployed on the device requesting access and ultimately who that particular device is associated with — all enabled through beneficial advances in digital automation and data analytics.

Securing DoD networks against vulnerable endpoints — ranging from laptops and desktops to scanners, printers, smartphones, switches, cameras and USB thumb drives — imposes significant mission assurance challenges for the Defense Department. Can it be surmounted? Yes. Through application of Security Orchestration Automation and Response (SOAR), operational advances evidence that the integration of the underlying mission, relevant technology and continuing innovation produce a viable and cost-effective solution for DoD's cyber defense. Under DoD guidance, a mission partner integrator applying a standards-based solution architecture — connected by a new orchestration layer that can synthesize each proprietary vendor product — can effect a holistic, integrated and optimized force-multiplier solution readily tailored for compliance-related cyber defense.

In the FY19 National Defense Authorization Act, Congress refocused national attention on the C2C program and cited it as a sound method to help reduce DoD cyber risk and secure DoD's ever-expanding number of network endpoints (FY19 NDAA, Section 1647)[1].

While DoD's network numbers rise, the attack surface also expands. Distinct and separate network access control solutions — though independently effective — consistently lag behind the advances of ever-changing intrusion and attack methods. Worse, these point-defense devices inevitably introduce coverage seams (with a latent attack surface) within DoD's Information Enterprise.

The Defense Department can continue spending on this point-solution technology, though they represent an increasingly fragile, expensive and fixed security approach.

Senior Defense leadership also recognizes that no single security technology, like C2C, offers extensive (or extensible) cybersecurity. Fortunately, a recognized security integrator that uses these C2C products in unison provides much greater assurance against intrusion. In addition, implementing a new, broadly based, compliance-predicated Solution Architecture can successfully deliver significant results, fortified by cyber defense continuous management (for situational awareness) and agile management (for adaptive, rapid defensive maneuvering). The integrator would devise this architecture in the context of well-defined and thoughtfully considered risk. This risk approach derives from an understanding of what comprises the understood risk formulation components — threats, vulnerabilities and the likelihood and impact — for DoD's most crucial assets:

PEOPLE:

The most vital resource, they also represent the most likely primary targets for malign cyber actors, who can supply a myriad of sophisticated and treacherous phishing methods. Ensuring a proper configuration baseline of the devices from which personnel access email denotes the first critical line of defense.

MISSION SYSTEMS:

Successful operational mission execution mandates the continuing protection of DoD operational infrastructure against network intrusion and infiltration, enduring mission assurance and the provision of cyber resiliency plans in the face of formidable digital adversaries.

MISSION-ENABLING SYSTEMS AND MISSION PARTNERS:

The business of government is supported by hundreds of thousands of staff in the Pentagon's "Fourth Estate" — who require assured access to business and mission-enabling systems across multiple DoD networks for daily operations. Similarly, partner civilian agencies, contractors, allies and other business mission partners inevitably expand the attack surface, which introduces increased risk into the DoD Information Environment — if not closely managed.

Effective C2C Mission Execution Requires an Integrator Partnered with Key Solution Providers

The dilemma of protecting DoD's people, networks and assets is not easily solved — not by finding the "right" technological solution, or even "staffing up" with cybersecurity experts who would physically monitor the networks. DoD is understandably inundated by the sheer number of computing devices, as well as the need for mobility, cloud access and complex joint operations — pitted against the increasing lethality of cyber adversaries. This dire situation deserves careful examination and consideration of more sophisticated automation than currently exists. It also unmistakably requires an updated Security Solution Architecture managed by a dedicated integrator that provides a holistic view,

along with the ability to orchestrate from the endpoint to the visual data layer.

To protect against stealthy and rapidly spreading cyber threats, each of the steps in the C2C process — from identification to quarantine to remediation — should, ideally, be automated, swift and require minimal human intervention by technical personnel — thereby reducing delays and wait times, as well as minimizing network vulnerability.

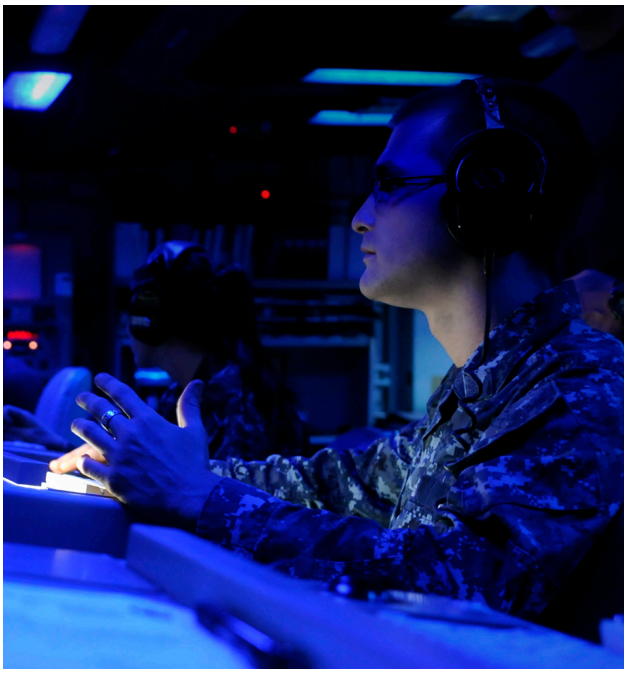
At the same time, functionality is neither "out-of-the-box" from the patchwork of vendor C2C products in use, nor can vendors offer proprietary tools that will be easily integrated or regularly upgraded. This instead requires careful governance and tuning to relevant DoD security policies. To date, initial attempts to deploy these tools have resulted in unacceptably long login times of 15-20 minutes — to simply identify and validate new devices attempting to join a network.

At present, C2C in its current capacity offers only a point-check or snapshot-in-time, while an endpoint device attempts to connect to a network. Devices that are already connected thus need to constantly be re-evaluated, in order to ensure that they have not drifted out of compliance.

A USG-Specified Standard for C2C Interoperability Embodies Another Vital C2C Mission Ingredient

Today, no single product is designed to meet the full spectrum of compliance and remediation requirements. Moreover, the Defense Department's need for layered cyber defense — both defense-in-depth and defense-in-breadth — precludes a mission-limiting "lock-in" with a single vendor solution. Given the constant and unceasing proliferation of new cyber threat vectors, developing an independent integration layer equipped with data analytics enables DoD to leverage specialized technological innovations from many C2C vendors simultaneously.

Still, C2C interoperability standards remain unrealized and the tools have yet to be optimally configured. Some vendors restrict access to certain proprietary functionality through their application program interfaces. No standardization yet exists for these interfaces to work and interoperate, or for how data will be represented or processed. Streamlined and effective interfaces for these objectively interconnected and "meshed" tools must also be undertaken, ideally through extensive data dictionary and data management efforts. Similarly, careful governance must be authored



PROPERLY PLANNED AND IMPLEMENTED, THE INTEGRATION AND ORCHESTRATION LAYER SIGNIFIES A READILY ADAPTABLE, NIMBLE, FIX-ON-THE-FLY C2C ENVIRONMENT THAT WILL ARM DOD NETWORK CYBER DEFENSES AGAINST NEW AND KNOWN THREATS

and applied to ensure that DoD cybersecurity policies are being followed.

Most current network access control solutions focus on achieving minimal C2C compliance, not building in interoperability for new and evolving missions — or for sustained resilience against new threats. Past efforts at integrating independent, discrete tools fell short of budgetary and delivery targets. Despite these factors, the goal of advancing beyond rudimentary monitoring of network endpoints, to automatically remediating security issues, remains an attainable objective. The DoD can propose, develop and champion a provisional government standard for C2C-accordant interoperability, in concert with the Department of Commerce's National Institute of Standards and Technology (NIST). Indisputably, this standard represents a critical underlying ingredient in the ability to integrate, update or replace the multitude of C2C toolsets the Department's complex missions accumulated.

DoD Can Develop, Deploy and Continually Improve an Integrated, Optimized C2C Solutions Suite

To fully deliver on the vision presented by the C2C proposal, certain elements are foundational: a renewed emphasis on open, modular architectures, improved network flexibility and a crucial new integration and orchestration layer, capable of harmonizing proprietary vendor technologies into a holistic system. Properly planned and implemented, the integration and orchestration layer signifies a readily adaptive, nimble, fix-on-the-fly C2C environment, which thereby fortifies and underpins the layered, hardened and reinforced DoD network cyber defenses — urgently needed to remediate today's threats or any new "zero-day" attacks that inevitably arise.

Improved network security visibility, faster response times and automated security patching can combine to significantly reduce risk each time a device connects to the DoD network infrastructure. These automation, visibility and speed improvements can eliminate many of the recurring tasks, updates, patches and fixes that currently occupy help desk teams across DoD.

How will senior leaders be able to measure the success of C2C? For the first time ever, C2C capacity will enable operators to have visibility into asset inventories and configuration baselines. Through direct reporting and analytics, totaling basic assets and surveying the network estate, furnishing immediate answers on patch deployments and eliminating unmanaged devices from accessing the network, susceptibility to potential threats can be rapidly and meaningfully identified. Assets and configuration baselines, with discrete operational and performance attributes, can also be similarly measured.

Securing DoD networks against millions of vulnerable endpoints remains a complex challenge. A solution exists at the intersection of mission, technology and innovation. Deploying a new solution architecture, along with defined data integration standards, enables the Department to collectively harness and optimize the C2C tools already deployed. The role of integrator will also be vital in enabling a holistic operational system, expressly tailored for the specific mission need of a more nimble, robust, adaptable and secure environment.

For more information please contact our Experts:

Alice Fakir
Vice President
Fakir_Alice@bah.com

Dan Kirkpatrick
Distinguished Technologist
Kirkpatrick_Daniel@bah.com

Ryan Zacha
Chief Technologist
Zacha_Ryan@bah.com

NOTES

1. *FY19 National Defense Authorization Act, Section 1647, January 3, 2018:*
   https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia and more than 80 offices worldwide, our firm employs more than 26,400 people and had revenue of $6.7 billion for the 12 months ending March 31, 2019. To learn more, visit BoozAllen.com. (NYSE: BAH)