PLAYBOOK

EITaaS

Transforming the DoD to Meet Tomorrow's Mission, Today

Sponsored by:

Table of Contents

Introduction

As the world changes so does the military battlespace. Today, the Defense Department contends with an expansive digital landscape and digital transformation is only going to accelerate in years to come. To enable agencies and warfighters with transformation, there will be a growing need for new tools and capabilities. The DoD will continually need to evolve the transformation of its network, security and cloud capabilities. Enterprise IT as a Service, or EITaaS, aims to move away from today's government-owned and operated IT by turning to industry to help provide a more reliable, resilient and secure network that enables the mission of the end users it supports.

What is EITaaS exactly and how can it support DoD's current transformation and modernization efforts? Here, we answer those questions and more.

Learn more about modern solutions for defense and civilian agencies from the experts at Verizon.

EITaaS Provides a Foundation for DoD's Digital Modernization

EITaaS is more than technology upgrades or tech refresh. EITaaS objectives are to use technology to make mission operations more effective by providing enhanced capabilities and tools combined with responsive and proactive services that improve IT operations and mission processes. EITaaS focuses on consolidation and areas for reducing costs. By adopting EITaaS, the DOD can help solve many network, security and cloud management and information sharing challenges. The department's **Digital Modernization Strategy**, intended to form the foundation for a Joint Force, focuses on innovation and supporting the National Defense Strategy "through the lens of cloud, artificial intelligence, command, control and communications, and cybersecurity."

By unifying three typically separate service areas — network, end-user services and computing platforms — EITaaS helps eliminate many of the silos that complicate management of the cloud infrastructure while also providing software-defined orchestration of the environment. It accommodates essential features such as identity-based authentication and zero trust — key elements to unified operations — and opens the door for incorporating new technologies via the cloud.

For the Army, "EITaaS provides a platform and greenfield for piloting new technologies and processes" said Verizon's Director of Federal Solutions Architecture Lamont Copeland, who has been working with the Army and Air Force on their respective **EITaaS pilots**. "We are providing a more reliable commercial Network as a Service (NaaS) model comprising a subset of Software-Defined Enterprise Network Fabrics seamlessly integrated, secure and

interoperable. Our well-orchestrated end-user migration plan brings new devices, a standard desktop and mobility capabilities with access to EITaaS and Army services.”

EITaaS is a key contributor to the Army’s Installations of the Future initiative. The clean-slate approach allows the Army and Air Force to evaluate legacy technology and focus on improving capabilities, mission effectiveness and quality of life for our warfighters.

With an eye toward the future, EITaaS provides a foundation to help the DOD to achieve its digital modernization goals — which include innovating to improve its competitive advantages over adversaries, optimizing for improved efficiency and capabilities, and developing agile and resilient cybersecurity — while taking advantage of new and emerging technologies.

A Slice of 5G

5G wireless technology tends to conjure images of high-speed consumer apps and support for services such as telemedicine or self-driving cars. “But the other key piece of 5G is the actual network transport itself,” said Verizon’s Enterprise Architect Chris Everich. “5G not only provides high bandwidth/low latency connectivity, it will provide revolutionary advances in network virtualization with network slicing.” Software-defined networking is the key enabler of 5G transport and allows for fine grained control of the data plane. With network slicing, the users’ resources and network topology can be optimized, providing guaranteed performance levels to meet the individual use cases or applications.

“Network slicing will allow us to deliver, from edge-to-core or edge-to-edge, the performance guarantees based on the service being consumed,” Everich said. In the DOD, it could allow bandwidth to be allocated based on mission needs, whether it’s for video in a forward- deployed area or for virtual reality apps used in location-based training.

> **“Network slicing will allow us to deliver, from edge-to-core or edge-to-edge, the performance guarantees based on the service being consumed.”**
>
> **Chris Everich**
> Enterprise Architect, Verizon

Using EITaaS in concert with 5G will also allow the DOD to take greater advantage of the Internet of Things by enabling better control of large-scale sensor deployments and incorporating new technologies. An IoT deployment can, for instance, involve a widespread distribution of security sensors, each with low power requirements and limited built-in functionality. The capabilities of the next generation of wireless communications ultimately allows for greater control.

“With 5G, it’s now possible to create a sensor network at tremendous scale,” Everich said.

An EITaaS environment, meanwhile, allows for deployment of technologies such as machine learning and artificial intelligence to those sensors, giving them an ability to learn, carry out additional functions and gain efficiency. Another advantage of ML and AI is in automating processes that now are done manually, greatly increasing speed while helping to reduce error rates.

Personification of Security

The DOD is moving away from outdated authentication and access models based on location and toward its **Identity, Credential and Access Management (ICAM) Strategy**. ICAM is based on continuous authorization of users and devices, with the eventual goal of establishing a full zero trust security model, which is seen as essential to effective, secure cloud-based operations.

"If you move to a zero trust model, you change the whole security framework," said Verizon's Principal Architect Eric Hardie. "In traditional networks, you trust the network itself," and its array of firewalls, endpoint security and other controls, he said. "In the new zero trust model, instead we build trust around the identity."

Access is determined on a per-session basis, based on the user's identity, the device they're using and what level of access they have. "You protect the data by ensuring that the identities that connect to that data are secured and authenticated and authorized each time they connect," Hardie added.

Verizon already uses identity-based authentication as part of its EITaaS environment. ICAM will greatly streamline access for personnel on the move, whether as individuals or in entire units. Currently, a soldier moving from Fort Polk, LA to Fort Benning, GA, for example, faces a number of time-consuming steps before gaining network access.

"In today's environment, he's got to leave his laptop at [his] home base, go to another base and get in the queue and get access to the network and get credentials," Copeland said. "It'll take some time before he or she is able to step up and do their job. In an

"If you move to a zero trust model, you change the whole security framework. In traditional networks, you trust the network itself. In the new zero trust model, instead we build trust around the identity."

Eric Hardie
Principal Architect, Verizon

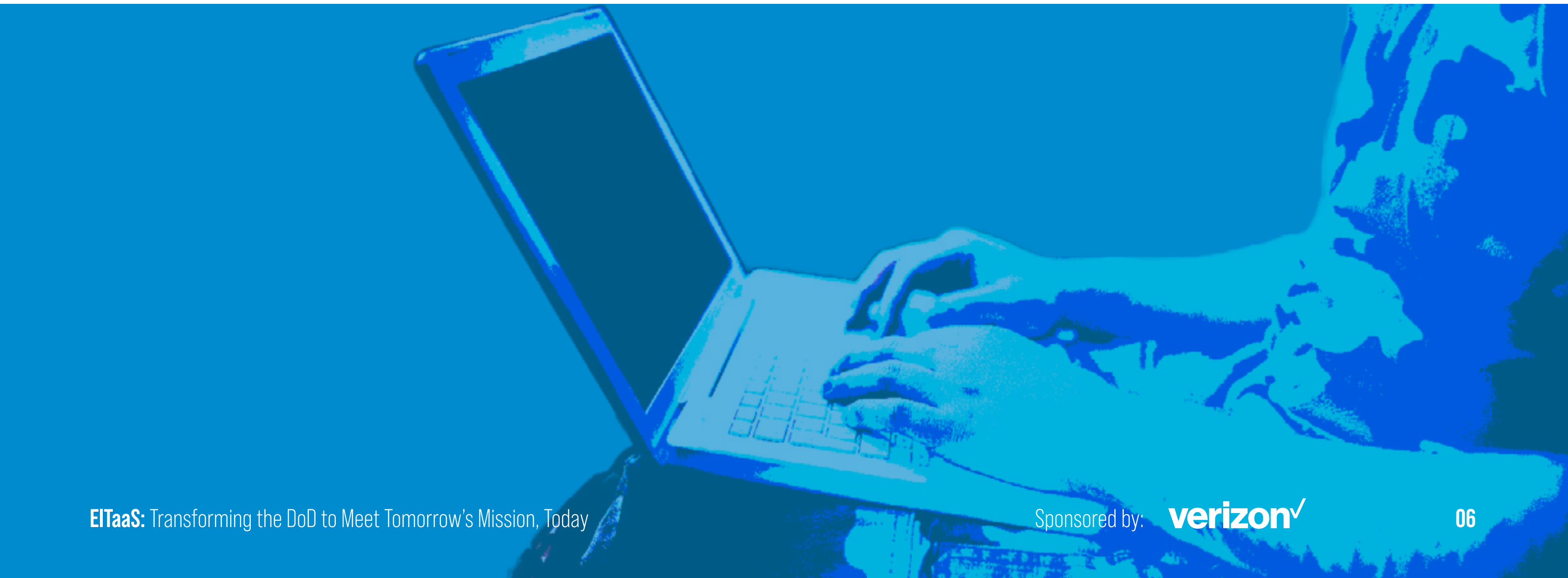
EITaaS environment, you've got devices that are provisioned to the network, and you can roam about the network freely, from base to base. Until it's time to upgrade your device, you are in the EITaaS environment. You don't have to get provisioned by the local network folks when you change bases or get assigned somewhere on temporary duty."

The same concept can apply to units operating in deployed areas.

Foundation for the Future

By helping improve the current state of the DOD's cloud environment, EITaaS can enable the adoption of innovative technologies and processes down the road. The Army and Air Force are running EITaaS pilots, each initiated under Other Transaction Agreement (OTA) awards and each with a goal of turning over basic IT operations to private providers in order to allow their personnel to focus on mission-critical activities. But they're also blazing a path for other services and DOD components with regard to EITaaS and laying the groundwork for the future of the department's digital modernization.

"It's an exciting time to be bringing capabilities to the Department of Defense through acquisition strategies like OTAs, which allows the government to collaborate throughout the process with industry partners and experiment, to pilot and try it on for size, so to speak," Copeland said. "And then scale it to production levels that allow them to improve warfighter effectiveness and mission effectiveness."



How EITaaS Puts DOD Cloud Services on the Same Page

If you ask any large enterprise what's putting a damper on their ability to process and share information, many will point to data silos as the largest offender. The Department of Defense has found, like enterprises everywhere, that adopting cloud can eliminate many of these on-premises silos.

The issue, however, is that cloud services can result in silos of their own. With as-a-service operations for networking and desktop support deployed separately, it can hinder the speed, efficiency, information sharing and security the DOD needs as it strives to support anytime, anywhere, any-device access for an increasingly mobile workforce. The COVID-19 pandemic has only compounded these challenges, with widespread telework and virtual meetings adding to the connectivity and security concerns that come with a more remote and disparate workforce.

Those are among some of the reasons that two military services within the Defense Department are implementing Enterprise IT as a Service pilot programs, which aim to arm the military with unified cloud services.

The Army is piloting an EITaaS model that will be deployed at nine locations over the course of about three years, with the goal to "increase mission effectiveness, increase IT user efficiencies and establish standardized, innovative IT services," according to the **Statement of Objectives** for the project. By consolidating services through a single provider, EITaaS can better enable cloud adoption and the integration of new technologies, while improving the user experience for personnel all the way out to the edge of DOD deployments. Along with the Air Force, which also is piloting EITaaS, the Army is testing the feasibility of using a commercial provider to not only improve services but to allow its own IT personnel to focus on mission-critical activities rather than managing email servers or desktop support.

EITaaS combines three major areas of IT that currently are handled separately — Network-as-a-Service, End User Services, and Compute and Storage — each of which covers essential components for military operations. Together, they can also enable cross functionality among the services and other components that the DOD requires as a part of joint operations.

Network-as-a-Service

Network-as-a-Service (NaaS) allows organizations to outsource parts of their infrastructure to a virtual environment, allowing for greater flexibility and dynamic service, but it also can create siloed operations in different parts of the network. This affects performance and network security, said Verizon Principal Architect Eric Hardie, one of three contractors working with the Army on its pilot program.

“Performance issues always turn into one organization not sure of who’s responsible for performance degradation,” Hardie said. “The same thing applies to troubleshooting.” If a connectivity problem exists across two or four organization boundaries, it creates a challenge pinpointing where the problems are.

EITaaS eliminates those kinds of IT inefficiencies by putting services into one basket.

“A big benefit of the whole EITaaS model is that they can consolidate who’s providing the service, and they can consolidate what they’re asking the service provider to give them,” rather than having separate agreements scattered across different devices and services, he said.

It allows the DOD to approach networking from the perspective of the warfighters, said Verizon Enterprise Architect Chris Everich.

“The warfighter doesn’t care where he or she logs into,” he said. “What they want is access to the service where they need it, when they need it, with high performance and high reliability.” And it also gives the Army greater control of their services through service level agreements (SLAs).

A consolidated environment enables greater efficiencies and data sharing across the enterprise, while providing the foundation for the DOD to incorporate new capabilities provided by emerging technologies such as 5G, and the ability to tap into the distributed potential of the Internet of Things.

Identity Is Everything

The whole point of mission effectiveness is lost if users, such as military commanders, can't get into the network in a timely fashion. In some instances, personnel at bases could take as much as 20 minutes to log onto the system, noted Anita Stanton, Verizon's Senior Client Executive for the Army.

> **"Providing the remote network capability [the DOD needs to work remotely] is a key component of how EITaaS has moved forward in making sure they're on virtual private networks, they have the security they need and also access to those applications from their home office."**
>
> **Anita Stanton**
> Senior Client Executive, Army, Verizon

"Personnel on the move, individuals or entire units may have a similar experience when they travel from site to site. It's not a simple thing to log into a new environment with a government-furnished laptop and plug into the local network to receive services," Hardie said. Logging in requires getting approval to connect to the network, followed by administrators setting up access requirements to allow a user to connect any time from anywhere. It's a time-consuming series of procedures, often done manually, and could be particularly risky in a deployed environment where fast action is required.

With EITaaS, Verizon helped automate such processes, which can help increase speed, while enabling more efficient and secure **Identity, Credential and Access Management** (ICAM) — something the DOD is developing while working toward a **Zero Trust Architecture**. "The identity solution allows them to validate whothey are and what they have access to," Hardie said. "Where they are located in the network is not really relevant. It's only relevant who they are, what their mission is and what they do."

An identity-based solution also allows an organization to better accommodate the growing amount of remote work resulting from the global pandemic, which has prompted the Defense Information Systems Agency (DISA) to adopt a **zero trust approach** in order to protect its networks.

Integrated Security

By unifying networking and end user services with compute and storage platforms, EITaaS also bolsters security — the top priority for any DOD system.

"The DOD has already moved to a very complex private cloud solution, with varying security levels," Hardie said.

"What we're building is a solution that is considered Impact Level 5," on **DISA's Cloud Computing Security Requirements Guide**.

By consolidating those Lines of Effort (LOEs)— networking, under services, and compute and storage—into a single architecture, EITaaS also enables cross functionality among the military services and other components. "If the Air Force and Army want to collaborate, that's based on their identity," Hardie said. Separate systems for separate services are no longer necessary.

"Security just becomes an integral part of EITaaS," Everich said.

The DOD's effort toward **digital modernization** rides on the cloud, and its success depends on systems within the cloud working together. Partnering with a commercial provider for EITaaS can help enable that, but that, too, involves working together.

"It has to be a close partnership," Hardie said. "We're really learning as we go."
Under the old model, five-year tech refreshes may have brought it new technologies, but the network stayed essentially the same.

"This is an entirely different approach, where they're letting go of a lot of controls they have internally and allowing us, as a commercial company, to provide them with real commercial innovation," he said. "But they're still the Army, they have a mission. So, it's a real partnership."

Click Here

To learn more about Verizon's solutions for defense agencies.