Delivering an Integrated Cyber Platform for DoD

Executing commander's intent at machine speed

Introduction

The operationalization of data has changed the nature of operations around the globe and across all industries. It has also changed the demands on and capabilities of the medium of maneuver for this data – the network. With the need for more operationalized data in today's environment, the network is the platform for cyberspace.

The Department of Defense (DoD) has long recognized the decision advantage that data provides to military operations. The establishment of U.S. Cyber Command underscores the significance of and need to protect and control data's medium of maneuver as essential for operational success – both in the cyber domain and in support of all other physical operational domains (land, sea, air and space).

Now more than ever, the demands on military networks in cyberspace require the DoD to operate the network as it would any platform (ship, tank, aircraft) in the physical space, not only to command and control operations in cyberspace, but also to ensure the network supports outcomes and decision advantage in the physical space.

Cisco's integrated platform provides exceptional capabilities for DoD entities to operate, secure, and defend DoD networks as an integrated cyberspace platform – at machine speed – and thus enable information effects across multiple domains. Cisco networks automatically interpret, implement, and enforce commander's intent and, as a single cyber platform, integrates and executes the core joint military operational functions.

With these integrated capabilities, the network functions as a single platform capable of autonomously acting as the "On-Scene Commander" to automatically detect and react to threats; provide unprecedented situational awareness; enforce policy and procedure; execute advanced schemes of maneuver; and provide decision advantage to the DoD through the secure, seamless maneuvering of data.

Fundamentals

Joint Publication 5.0 defines the six joint operational functions: **command and control, intelligence, maneuver, protection, sustainment,** and **fires**. In order to operate, secure, and defend DoD networks and produce operational outcomes in cyberspace, Cisco's integrated cyber platform allows for the seamless and automated integration of the first five operational functions – leveraging the components that form the foundation of the platform's infrastructure.

Operational Functions

(1) **Command and control** is defined as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission." Hence, the function consists of two parts: (1) the inherent authority vested in the entity to (2) issue controlling actions that support mission accomplishment.

Effective **command and control** is the result of multiple successful exchanges of information that occur across and through people, processes, and technology. Ultimately, complex and timely information must be conveyed to the right decision-maker(s) in command authority, and the appropriate controlling orders must be conveyed for action and execution. Observing all the data and information flowing from the multitude of devices that make up the cyber platform is essential; but the near-simultaneous orientation to the significance of the associated data and information for the decision entity remains critical to realize the cyber platform's **command and control** function.

Cisco's integrated cyber platform provides comprehensive and automated cyber **command and control** through Cisco's Digital Network Architecture (DNA) Center, along with the seamless integration of Identity Services Engine (ISE), TrustSec, Firepower Management Center, and Stealthwatch Management Center – together, exercising **command and control** over all the devices and appliances on the network and in the cloud. These capabilities operate at machine speed not only to **command and control** the cyber platform, but also to augment and assist the cyber **intelligence, maneuver, protection,** and **sustainment** functions – providing multiple, seamless, successful exchanges of information for decision and action.

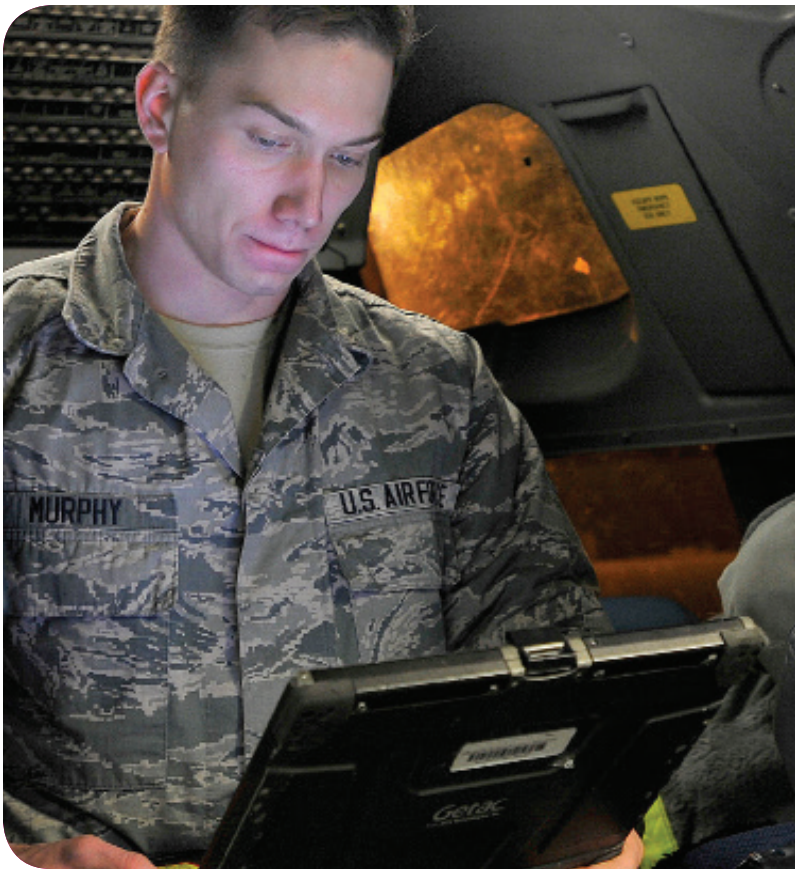
Joint Function	Cyber Operational Function	Cisco Cyber Platform Capability
Command and Control	▪ Exercising centralized management – informed by threats and extreme visibility of all network flows and devices ▪ Handling network authentication, granular access control, and rapid device discovery ▪ Executing protective segmentation orders when necessary ▪ Provisioning all devices at scale per commander's intent ▪ Conducting continuous monitoring and enforcing policy ▪ Making adjustments for optimal performance across network, devices, and applications	Identity Services Engine (ISE) DNA Center Stealthwatch TrustSec Firepower Management Center

(2) **Intelligence** is "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning . . . hostile or potentially hostile forces or elements." Threat **intelligence** combined with situational awareness of one's own forces (or network devices) provides to the entity vested with **command and control** authority the critical pieces of observable information and orients the central authority to the threat with context and relevance to the force.

In order to operate the network as a cyber platform, threat **intelligence** must be ingested and evaluated rapidly to allow for fast orientation to the threat in relation to the entire cyber platform. Decisions and network actions can then be executed rapidly across the entire platform. The platform's data flows of the many devices, routers, switches, firewalls, sensors, and appliances that constitute a modern network provide the greatest situational awareness of all: *The cyber platform is the best sensor* when all of these network flows and device telemetry can be integrated and analyzed automatically – and understood in relation to any threats.

Cisco's integrated cyber platform **command and control** capabilities integrate directly with the cyber platform's **intelligence** capabilities: Talos, Advanced Malware Protection (AMP), Threat Grid, Stealthwatch, Encrypted Traffic Analysis, and Cognitive Threat Analytics. Together these capabilities, which leverage integrated network flows and telemetry, provide unmatched visibility and situational awareness. The platform's tight integration of these functions accelerates John Boyd's famous *Observe – Orient – Decide – Act* loop to machine speed.

The core component of any operation in any domain is solid, actionable intelligence. Cisco Talos has the most comprehensive cyber intelligence, surveillance, reconnaissance, and analysis platform in the industry. Cisco Talos analyzes numerous public and private intelligence feeds every day, looking for new threats and acting on information in real time to develop new detection indicators and content. Cisco Talos collects more than 1.1 million malicious software samples per day by compiling data acquired from product telemetry along with honeypots, sandboxes, and industry partnerships in the malware community. Each day, Talos inspects more than 300 billion emails, drawing on layering detection technologies such as outbreak filters and machine learning-based reputation filters and Cisco Advanced Malware Protection (AMP). Cisco Web Security technologies detect and identify new and emerging web exploitation techniques and provide Talos insight into nearly 20 billion cyber threats each day.



Combined with Talos' unprecedented threat visibility, Talos advanced analysis capabilities automatically analyze samples and rapidly generate detection content to mitigate threats daily. This provides the cyber platform with meaningful, contextually relevant insight into the threat landscape with an unparalleled global perspective of the cyber domain. At machine speed, Cisco Talos provides actionable threat **intelligence** directly to the components of the cyber platform, including:

- Next-Generation Intrusion Prevention System (NGIPS)
- Next-Generation Firewall (NGFW)
- Advanced Malware Protection (AMP)
- Email Security Appliance (ESA)
- Cloud Email Security (CES)
- Cloud Web Security (CWS)
- Web Security Appliance (WSA)
- Cisco Umbrella
- Threat Grid
- Numerous open-source and commercial threat protection systems

Joint Function	Cyber Operational Function	Cisco Cyber Platform Capability
Intelligence	• Dedicated worldwide intelligence, surveillance, and reconnaissance with integrated detection and prevention techniques to discover, assess, and respond to the latest trends in hacking activities, intrusion attempts, malware, and vulnerabilities • Automatic detection of anomalous behaviors and detection of anomalous actions by potential insider threat • Protection from malicious code using big data analytics, point-in-time detection, and retrospective security (continuous analysis) capabilities • Detection of malware in encrypted traffic by passive monitoring of relevant data elements and supervised machine learning	Talos Advanced Malware Protection (AMP) Threat Grid Stealthwatch Cognitive Threat Analytics Encrypted Traffic Analytics (ETA) Firepower Management Center

Thus, the cyber platform's **intelligence** capabilities automatically identify a wide range of threats, including malware (even in encrypted traffic), zero-day attacks, distributed denial-of-service (DDoS) attempts, advanced persistent threats (APTs) and insider threats. The cyber platform automatically interprets the *recognized threat in context* across all the key terrain of the cyber platform instantly – from cloud services, network devices, endpoints, email services, and web services. The integrated **intelligence** capabilities enable the cyber platform's **command and control** function to act as the first operational On-Scene Commander in the presence of a threat to the platform.

(3) **Maneuver** is the action or movement of forces to a position of relative advantage over the threat. Just as modern warfare recognizes that static defenses can be easily overwhelmed whereas **maneuver** forces can rapidly and dynamically achieve relative advantage, modern cyber defenses require network agility, resiliency, and automated segmentation – all in a dynamic way to respond to everything from the most seemingly benign unpatched endpoint to numerous or even massed cyber threats.

One of the complexities of the human-made cyber domain is that it continues to grow dynamically in size and shape. The operationalization of data to enhance operational outcomes has resulted in an unending explosion of more devices, including the addition of more sensors to the cyber platform and with more data to **maneuver** across the platform. The **maneuver** function in cyberspace directly supports the **protection** function through an adaptive security architecture that implements advanced network segmentation and network access capabilities in order to prevent, detect, respond to, and even predict intrusions or malicious activity through continuous visibility and validation.

The integrated platform's **command and control** and **intelligence** functions enable the network to act as the best sensor, and the platform to execute and enforce the commander's intent. The integrated platform automatically provides continuous detection, response, and predictive capabilities to issue **maneuver** orders to segment, block and control access across the cyber platform to ensure cyber platform **protection**.

Cisco ISE discovers and dynamically profiles endpoints the moment they attempt to connect to the platform – identifying the type of device and the corresponding unique MAC address or 802.1x credential. After the identity and session context characteristics of the device are established, Cisco ISE applies network access control security policies. If an unknown or unpatched device connects to the platform, Cisco ISE can immediately segregate the endpoint into an isolation enclave. This allows the device a limited connection while it undergoes further automated or manual classification and compliance checks. Once the device is classified and is considered compliant, it is automatically given an enforced, role-based authorization to access the platform.

Using Cisco's open-standards software-defined segmentation approach, TrustSec enables the cyber platform's **maneuver** function with agility and security by classifying devices (and users and applications) into groups (called Scalable Group Tags [SGT]) that can be used to isolate and segment traffic as it flows across the cyber platform. This approach decouples cyber platform **maneuver**-based segmentation policies from the underlying platform's infrastructure. SGTs are dynamically assigned to an endpoint when it authenticates to the platform and are applied to network traffic (packets) as they enter the platform, whether wired or wireless. The cyber platform uses SGTs along with the infrastructure topology to selectively isolate endpoint layer 2 and layer 3 communications across the whole platform.

Even more powerfully, whether dynamically reacting to a threat (in support of the **protection** function) or managing day-to-day platform access operations, Cisco's Next-Generation Firewall (NGFW) and Firepower Management Center, together with ISE, **maneuver** access, connections, and communications across the cyber platform automatically and with high velocity to execute commander's intent are for agility and resilient response.

Joint Function	Cyber Operational Function	Cisco Cyber Platform Capability
Maneuver	▪ Adaptively implement advanced micro-segmentation to enforce policy ▪ Execute cyber platform orders across the network by unique identities, roles, applications, and/or ports – not by IP addresses alone ▪ Segregate endpoints into an isolation enclave to ensure protection and risk mitigation ▪ Execute actions at high velocity to support platform agility and resiliency	Identity Services Engine (ISE) DNA Center Stealthwatch NGFW Firepower Management Center TrustSec

(4) **Protection** is fundamental to network security and seeks to preserve the effectiveness of the network; network access; and the assured access, availability, and integrity of the data on the network. As they are in the physical world, the **protection** and defensive capabilities are layered across the entire fabric of the cyber platform, including the cloud. **Intelligence, maneuver,** and **command and control** functions work together to support and enable cyber platform protection.

As discussed above in the description of cyber platform **maneuver,** micro-segmentation delivers secure network access using a comprehensive, integrated network access and policy control solution with granularity that enables access authorization down to individual devices, individual users, individual ports, and individual applications – as well as specified combinations of all of these.

Cisco's integrated security solution provides the cyber platform with detailed, real-time continuous monitoring of activity to enforce dynamic access control using the Cisco Identity Services Engine (**command and control** function). ISE automatically enforces Comply to Connect-based commander's intent by:

- Authenticating the endpoint and determining whether a device complies with the security posture (including the latest operating system patches and antivirus software)
- Automating remediation (quarantining noncompliant devices and remediating quickly with minimal user effort), which saves time and improves productivity
- Enabling the creation of custom profiles for proprietary systems and devices unique to defense (such as maintenance systems)

Cisco ISE is easily combined with third-party partner products such as Tenable Nessus, Tanium, and Splunk Enterprise or Enterprise Security (using pxGrid) to augment additional **protection** capabilities with seamless integration into the cyber platform.

Cisco ISE **command and control** functions support cyber platform **protection** by working together with the Firepower Management Center (the security administrative nerve center for complete and unified

management of next-generation firewalls), application control, intrusion, detection and prevention, URL filtering, and advanced malware protection. The Cisco Next-Generation Firewall (NGFW) provides adaptive, threat-focused, superior, multilayered protection; improves visibility; and reduces security costs and complexity. Firepower Next-Generation Intrusion Prevention System (NGIPS) provides essential defense-in-depth capabilities that inspect network traffic to understand network behavior, detect traffic anomalies, and identify and block breaches.

Cisco's Advanced Malware Protection (AMP) has specific cyber platform **protection** versions for networks, endpoints, email, and the web, as well as direct integrations into firewalls, integrated service routers, and the cloud. AMP is the only malicious code protection solution that combines the power of big data analytics, point-in-time detection, and retrospective security (continuous analysis) capabilities. AMP also works with Cisco Threat Grid to provide sandbox functionality to unknown or suspicious samples. While AMP provides near-instant disposition with regard to any sample, Threat Grid allows security operations center personnel to actually see what the potentially malicious file will do and provide threat **intelligence** back into the cyber platform.

Coupled tightly with the intelligence function, Cisco Stealthwatch serves as the eyes and ears for protection of the cyber platform through its "own-force monitoring" capability with advanced security analytics. Stealthwatch rapidly collects and analyzes massive amounts of NetFlow data to deliver in-depth visibility and actionable information to security and response teams. Unlike many other technologies that monitor only traffic going in and out of the network (north-south), Stealthwatch also monitors lateral (east-west) traffic to detect attacks spreading inside the network and to identify insider threats. Stealthwatch provides cyber platform baselining through sophisticated behavioral analytics and deep platform understanding, which are critical for establishing strong incident response procedures. Stealthwatch dramatically reduces the manual analysis associated with incident investigation – reducing troubleshooting time from days or even months to just minutes. Intuitive dashboards and reports rapidly provide information to orient the platform's command and control function and enable surgical security and incident response.

Cisco Solutions for Cloud Security provides a wholly integrated protection capability for the Cisco cyber platform. The extension of the cyber platform to include multiple cloud-enabled architectures ("multi-cloud") is creating the opportunity for new operational outcomes. Cloud is an integral part of the cyber platform and must benefit from the same protection, command and control, and intelligence-based visibility functions and associated capabilities. Hence, Cisco's Cloudlock is a Cloud Access Security Broker that accelerates secure cloud adoption by protecting users, data, and applications across cloud-computing architectures, such as software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and identity-as-a-service (IDaaS). Cloudlock monitors usage in real time and extends essential controls into cloud applications. Additionally, Cisco Umbrella creates a new DNS layer of cloud-delivered protection in the network security stack, protecting users anywhere they go. Extensive real-time threat intelligence works in conjunction with DNS to keep users from connecting to malicious sites. Since DNS precedes all internet activity, it is a powerful way to enforce security and gain insight across the cyber platform. Protection is built in and enabled by default.

Cisco Cognitive Threat Analytics (CTA) provides a breach detection solution analyzing all forms of web traffic, whether over HTTP, HTTPS, or even anonymous protocols such as Tor. Using machine learning and a statistical modeling of networks, Cognitive Threat Analytics deliberately creates a baseline of normal activity and identifies anomalous traffic occurring within the cyber platform. CTA analyzes device behavior and web traffic to pinpoint illicit command and control communications and data exfiltration. CTA turns the web proxy into a security sensor that automatically identifies and investigates suspicious web-based traffic.

Joint Function	Cyber Operational Function	Cisco Cyber Platform Capability
Protection	▪ Integrated network access and policy control solution with device granularity ▪ Unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection ▪ Inspection of network traffic to understand network behavior, detect traffic anomalies, and identify and block breaches ▪ Protection from malicious code using big data analytics, point-in-time detection, and retrospective security (continuous analysis) capabilities ▪ Analysis of device behavior and web traffic to pinpoint command and control communications and data exfiltration ▪ Extension and integration of protection across the local platform with the cloud as one platform	Identity Services Engine (ISE) DNA Center Stealthwatch Advanced Malware Protection (AMP) Cognitive Threat Analytics Firepower Management Center TrustSec NGFW Threat Grid Security Appliances

5) **Sustainment** is described as the provisioning of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment. In the cyberspace domain, sustaining the delivery of data to the right decision-maker or into the hands of the correct consumer to provide decision advantage remains the main purpose and function of the cyber platform and its operators, 24 hours a day, 365 days a year.

The **sustainment** and underlying management of the cyber platform must leverage automation, ensure security and be able to **maneuver** rapidly to meet the demands of fast-paced, data-intensive operations – and adapt to new demands. As discussed, the cyber platform must be able to integrate **intelligence, command and control, maneuver,** and **protection** operational functions while understanding and autonomously acting on commander's intent as the first On-Scene Commander – and hand off only the most complex actions to its operators to resolve. **Sustainment** of operations on the cyber platform requires simplified interfaces to maintain situational awareness and execute complex cyber platform operations on a single pane of glass – quickly, efficiently, and with economy of force.

As discussed, the Cisco Digital Network Architecture (DNA) Center is a centralized management application for the cyber platform. DNA Center simplifies network management to move more quickly, lower costs through automation, boost network performance through assurance and analytics, and continuously ensure comprehensive security. With Cisco DNA, the cyber platform can:

- **Move faster:** Provision thousands of devices across the network. Act fast with centralized management and automated device deployment.
- **Reduce risk:** Predict problems easily. Use actionable insights for optimal performance of the network, devices, and applications.
- **Cut costs:** Reduce errors with automation. Policy-driven deployment and onboarding deliver better uptime and improved security.

Complicating the **sustainment** function in cyber operations, the rise of cloud-based applications, hybrid-cloud networks, and IoT is impacting existing network operations. The need to maximize bandwidth utilization, optimize cloud connectivity and globally improve security posture is challenging with traditional wide area network (WAN) architectures. Furthermore, the disparate nature of traditional WAN infrastructures makes it hard to gain comprehensive visibility of applications and infrastructure, which hinders failure resolution and effective forecasting of resources.

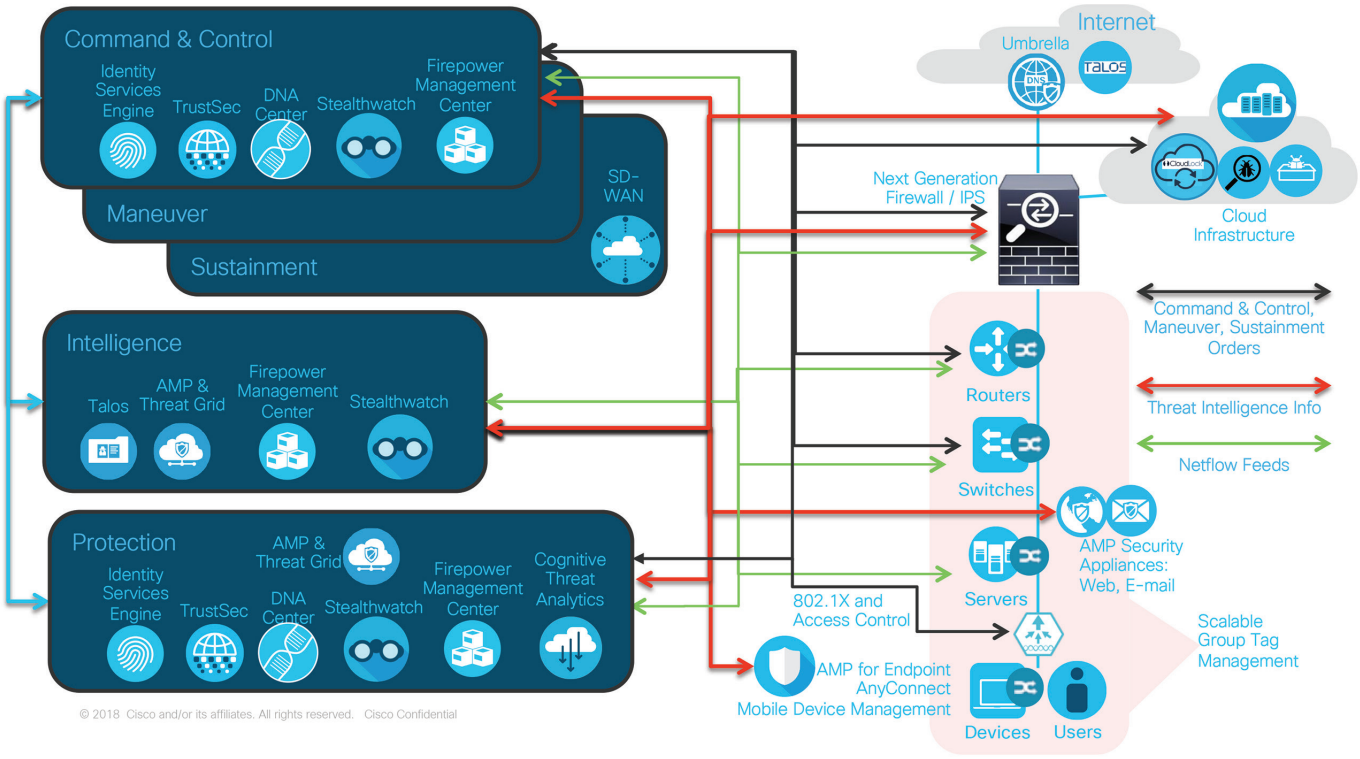
Cisco's integrated Software-Defined WAN (SD-WAN) technology addresses the challenges of the increasing demand to sustain cyber operations for today and tomorrow – with greater agility, security, and simplicity for the cyber platform. Cisco SD-WAN is a cloud-delivered overlay WAN architecture that enables digital and cloud transformation across the cyber platform. SD-WAN significantly lowers traditional WAN costs, reduces the time to deploy services, builds application resiliency and provides a robust security architecture for hybrid networks.

Cisco's SD-WAN solution provides an enhanced cyber platform solution with advanced routing, segmentation, and security capabilities for interconnecting the most complex enterprise networks – enabling **sustainment** of cyber platform **maneuver** at the largest scale. Its centralized network management plane and intuitive orchestration and overlay technologies make it easy to deploy and manage next-generation WAN architectures. SD-WAN technology allows organizations to build and re-architect secure, policy-controlled, and cost-effective WANs in months, not years — **agility** is a must-have characteristic of the modern cyber platform. SD-WAN implementations have reduced operating costs of the platform by more than 50 percent and have increased access bandwidth by 10x and have significantly improved security and uptime performance.

With battle-tested capabilities and deployment worldwide, the Cisco cyber platform has proved highly sustainable, with documented case studies showing decreased operating complexity as an integrated solution; reduced capital expenses and operating costs; increased cyber personnel productivity; and reduced threat of security breaches to the cyber platform and its data and applications.

Joint Function	Cyber Operational Function	Cisco Cyber Platform Capability
Sustainment	▪ Integrated, end-to-end cybersecurity technology architecture improves incident prevention and detection, automates and orchestrates response, and streamlines and simplifies security operations ▪ Tracks and controls all users and devices connected to the platform, including bring-your-own-device and guest access ▪ Implements software-defined network segmentation and enforces policy at the routing and switching layer ▪ Tightly integrates with a wide range of technology partner solutions	DNA Center Identity Services Engine (ISE) SD-WAN

The Integrated Cyber Platform



Summary

Cisco technologies and solutions provide DoD with an integrated cyber platform that automatically interprets, implements, and enforces commander's intent. The cyber platform integrates and executes the military operational functions of **command and control, intelligence, maneuver, protection,** and **sustainment** – simply, effectively, with agility, and at machine speed. The cyber platform's uniquely integrated capabilities – across individual devices, the network topology, and in the cloud – enables the platform to autonomously act as the On-Scene Commander to automatically detect and react to threats, provide unprecedented situational awareness, enforce policy and procedure, and execute advanced schemes of maneuver.

Ultimately, this cyber platform, operationally implemented as the medium of maneuver for data, provides decision advantage and enables information effects across multiple domains for the DoD.

To learn more about Cisco solutions for the DoD, please visit cisco.com/go/DoD.