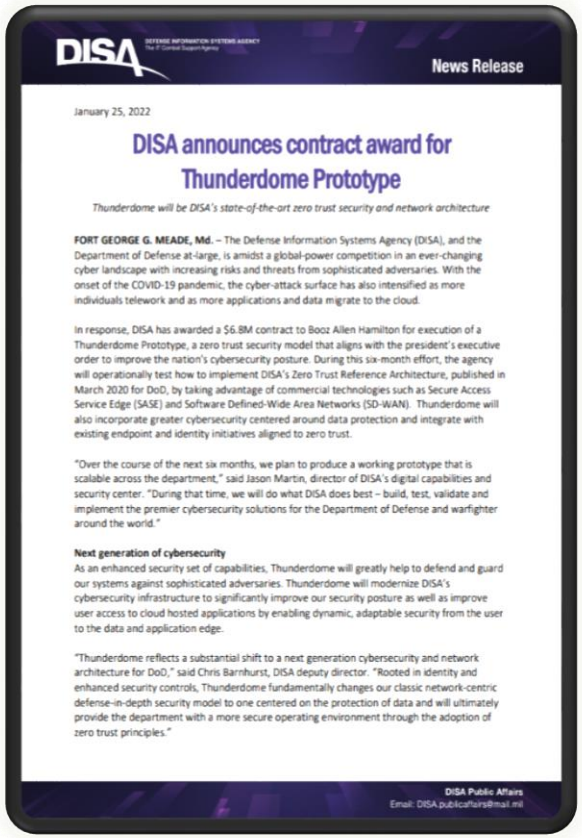
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Thunderdome

A Year In Review

Julian Breyer
Defense Information Systems Agency
Thunderdome PMO
February 2023

Thunderdome Pilot



DISA News Release

January 25, 2022

DISA announces contract award for Thunderdome Prototype

Thunderdome will be DISA's state-of-the-art zero trust security and network architecture

FORT GEORGE G. MEADE, Md. – The Defense Information Systems Agency (DISA), and the Department of Defense at-large, is amidst a global-power competition in an ever-changing cyber landscape with increasing risks and threats from sophisticated adversaries. With the onset of the COVID-19 pandemic, the cyber-attack surface has also intensified as more individuals telework and as more applications and data migrate to the cloud.

In response, DISA has awarded a $6.8M contract to Booz Allen Hamilton for execution of a Thunderdome Prototype, a zero trust security model that aligns with the president's executive order to improve the nation's cybersecurity posture. During this six-month effort, the agency will operationally test how to implement DISA's Zero Trust Reference Architecture, published in March 2020 for DoD, by taking advantage of commercial technologies such as Secure Access Service Edge (SASE) and Software Defined-Wide Area Networks (SD-WAN). Thunderdome will also incorporate greater cybersecurity centered around data protection and integrate with existing endpoint and identity initiatives aligned to zero trust.

"Over the course of the next six months, we plan to produce a working prototype that is scalable across the department," said Jason Martin, director of DISA's digital capabilities and security center. "During that time, we will do what DISA does best – build, test, validate and implement the premier cybersecurity solutions for the Department of Defense and warfighter around the world."

Next generation of cybersecurity

As an enhanced security set of capabilities, Thunderdome will greatly help to defend and guard our systems against sophisticated adversaries. Thunderdome will modernize DISA's cybersecurity infrastructure to significantly improve our security posture as well as improve user access to cloud hosted applications by enabling dynamic, adaptable security from the user to the data and application edge.

"Thunderdome reflects a substantial shift to a next generation cybersecurity and network architecture for DoD," said Chris Barnhurst, DISA deputy director. "Rooted in identity and enhanced security controls, Thunderdome fundamentally changes our classic network-centric defense-in-depth security model to one centered on the protection of data and will ultimately provide the department with a more secure operating environment through the adoption of zero trust principles."

DISA Public Affairs
Email: DISA.publicaffairs@mail.mil

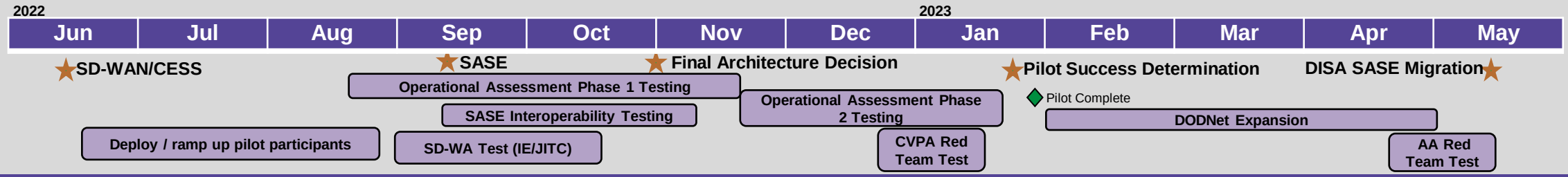
DISA awarded an OTA for a prototype-driven pilot concluding in Q2 of FY23

GOALS

- Implement Zero Trust Network Access on an existing network
- Develop operational experience for Enterprise ZTNA Deployment
- Lay foundations for enterprise service offering and broader ZTA adoption

SCOPE

- Leverages OTA allowing adjustments to technology components
- Currently supports 1,500 users at three DISA sites
- DISA is collaborating with the U.S. Army on conditional remote access pilot
- Includes Red Team as part of operational assessment



Project Scope

The Thunderdome prototype is not the end state of DISA's Zero Trust Architecture (ZTA) implementation but rather a building block that will help the DOD accelerate toward a modern cybersecurity architecture.

Thunderdome will

- Deemphasize perimeter-focused defense and trusted networks and devices in favor of authentication of individual resource requests and micro-perimeters
- Enhance the visibility and analytics of cloud security to support Defensive Cyber Operations (DCO)
- Increase automation in network and security deployment and management and reduce the time to react to emerging threats and network conditions

Thunderdome Components

Thunderdome's components work together to modernize DISA's infrastructure and integrate with other agency-efforts to increase automation, efficiency and security.

SASE

- Highly available Palo Alto Prisma cloud service replaces Remote Access VPN services
- Remote Users are authenticated using enterprise identity services
- Users get conditional access to applications and resources based on identity attributes, device posture, geo-location and time of use
- Remote user traffic no longer traverses the Defense Information System Network (DISN) to reach cloud services* or internet services

SD-WAN CESS

- Customer Edge Security Stack (CESS) moves security functions (NGFW, IPS/IDS) closer to the user at the customer edge
- Users get conditional access to applications and resources based on identity attributes, device posture, geo-location and time of use
- Provides software-defined routing capabilities
- Is an overlay to the existing DISN routing infrastructure
- Creates multi-tenancy hierarchy with Parent / child relationships for baseline and secondary security policies for on prem users

AppSS

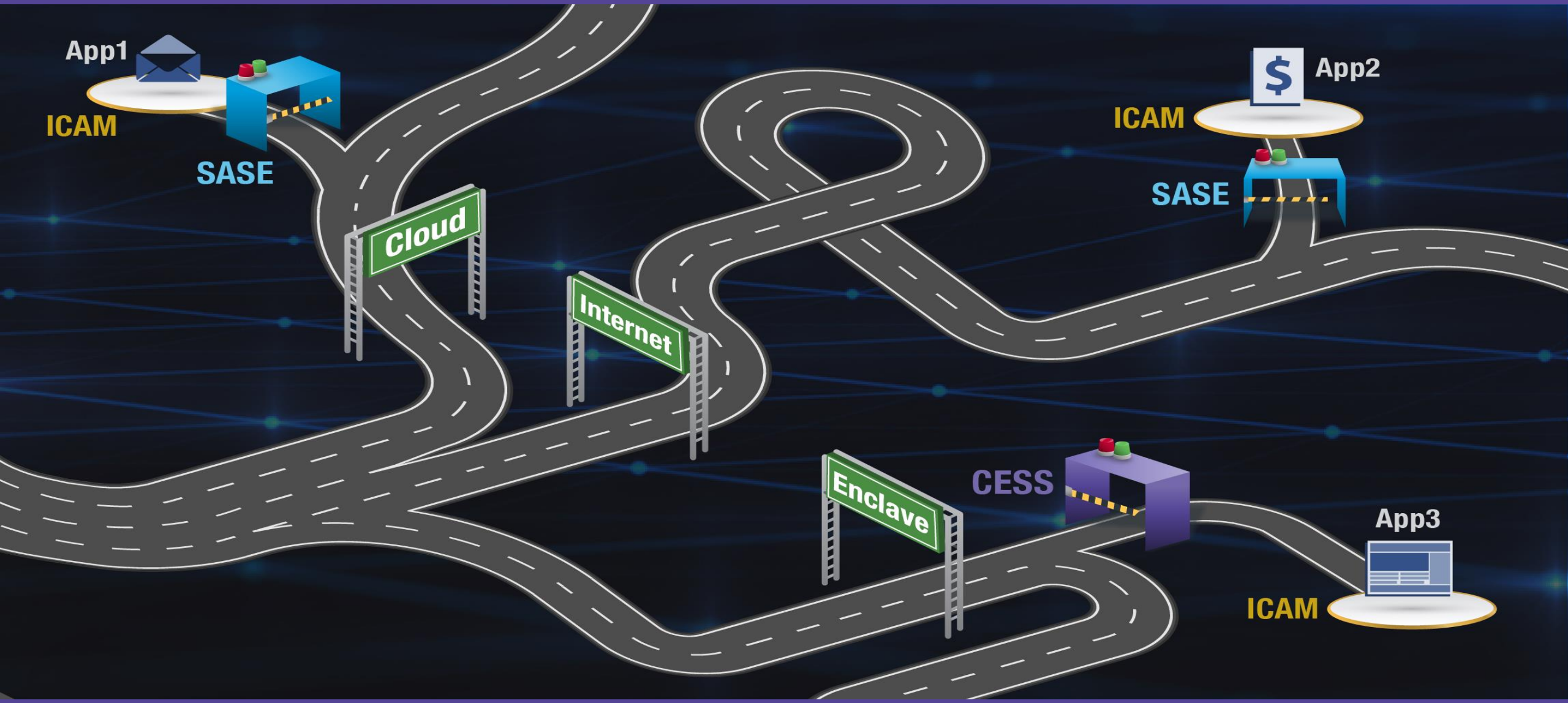
- Provides containerized, readily deployable security solution
- Reduces the burden of application security on individual applications owners
- Multiple solutions with either Palo Alto Container Security, F5 WAF and Palo Alto Next Gen Firewalls managed by Palo Alto Panorama
- DISA will provide Infrastructure as a Code (IaC) templates to automatically provision VM's or leverage Ansible for physical devices

CyberSA

- Increases visibility across the DOD's Cloud applications
- All user and telemetry data will be ingested, enriched and filtered w/o the need to duplicate data
- Normalize data, automate analyst workflows and enable analysts to apply Machine Learning (ML) models to streaming data
- Cloud agnostic architecture can leverage commercial cloud services or reside on-premise

Thunderdome Components

Thunderdome's components work together to modernize DISA's infrastructure and integrate with other agency-efforts to increase automation, efficiency and security.



Thunderdome's Role in Zero Trust

1 Endpoint
Connects remote or on-premises user to network and applications via ZTNA

2 Zero Trust Network Access (*ZTNA*)
Implements conditional access to the network based on endpoint device posture and user identity provided by ICAM

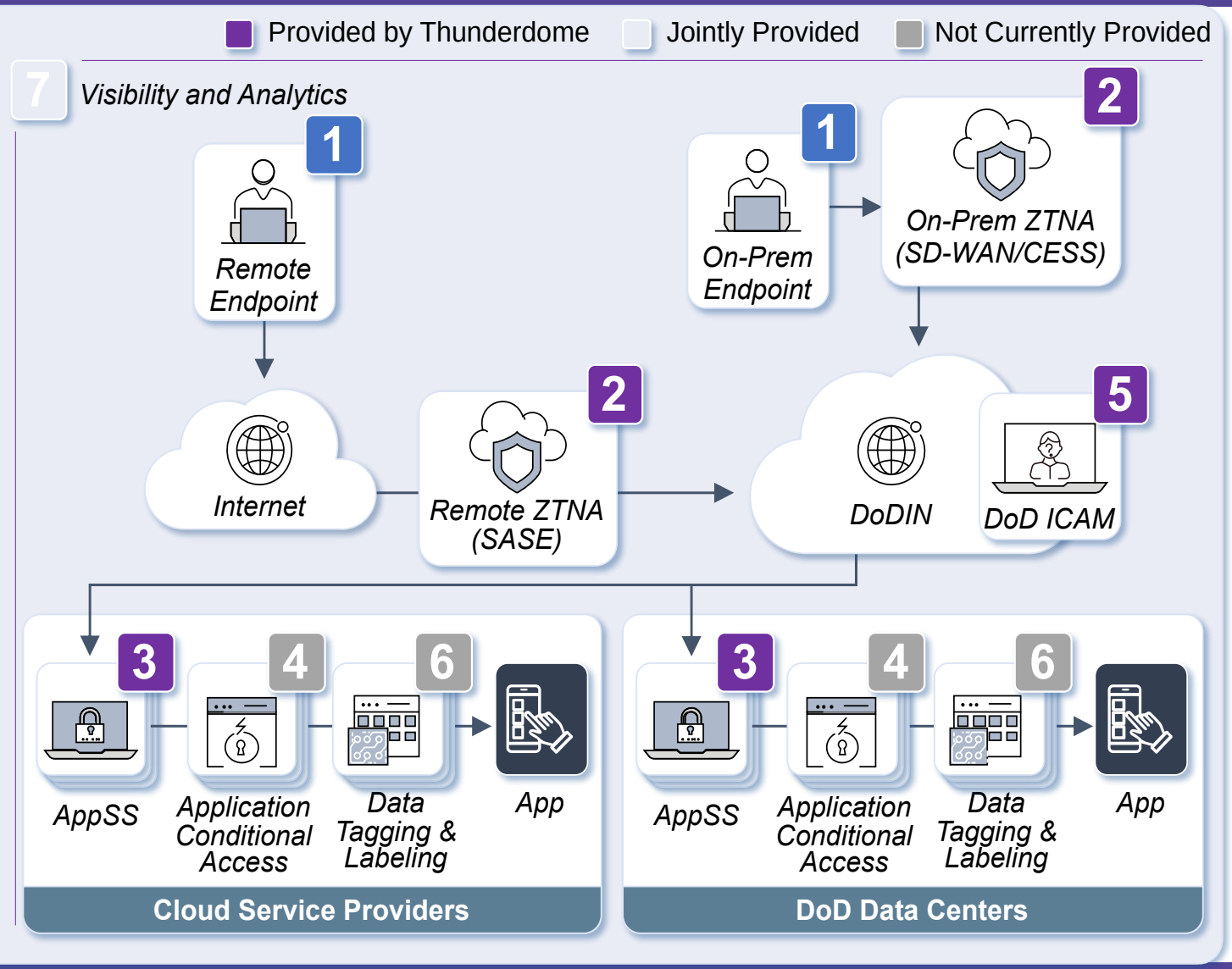
3 Application Security Stack (*AppSS*)
Scalable security stack providing micro segmentation, intrusion, and lateral movement protections against network and application-layer based attacks

4 Application Conditional Access
Provides application-specific conditional access checks

5 ICAM
Leveraged by ZTNA & App Conditional Access component to provide user identity information

6 Data Tagging and Labeling
Identify data for policy enforcement

Visibility and Analytics
Monitors all components, providing analytics and incident response



Thunderdome Pilot Retrospective

During the past 12 months, we have

- Integrated Thunderdome components with each other and the DISA Enterprise ecosystem
- Achieved issuance of an Authorization To Operate (ATO)
- Migrated 1,500+ pilot users at three DISA sites to our solution for Zero Trust Network Access to DODNet
- Completed a Cooperative Vulnerability and Penetration Assessment (CVPA) and Operational Assessment (OA)
- Demonstrated conditional access for remote and on-prem users
- Collaborated with mission partners to ensure alignment between Zero Trust pilots and exchange of lessons learned
- Collaborated with vendors to increase performance for OCONUS users

Challenges/Lessons learned

- DOD sites are highly variable and complex – implementation and migration time varies greatly
- Technology deployment is the easy part – evolving culture, policies and procedures are long-term challenges
- Interoperability with other ZT efforts
- Mobile user access leveraging derived credentials
- Lack of DOD-wide endpoint credentialling solution

DISA ZT Roadmap

Next Steps for Thunderdome

- Site designs for 4th Estate (4ENO)/Joint Regional Security Stack (JRSS) customer migrations
- Development of conditional access policies and application security stack requirements for DISA/4ENO
- Expansion on NIPRNet and SIPRNet
- Pursue Cloud Access Point (CAP) equivalence for remote users

Additional ZT-related DISA efforts

- Next-gen Anti Virus (AV)/Endpoint Detection and Response (EDR)
- Unified Endpoint Management (UEM)
- Automated security validation
- Security Orchestration and Automated Response (SOAR)
- Advanced Application Programming Interface (API) security
- Virtual Desktop Infrastructure (VDI)
- Advanced micro-segmentation and flow mapping
- Data labeling/tagging, Digital Rights Management (DRM), and Data Loss Prevention (DLP)

Questions?

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

/DISA **@USDISA** **/USDISA** **DISA.mil**