Booz Allen | District Defend®

CHALLENGE: AS ORGANIZATIONS ADOPT SECURE ENTERPRISE MOBILITY, THEY FACE A WIDE RANGE OF SECURITY THREATS.

Threats organizations face include:

Insider Threats

- An insider threat is the theft or misuse of organizational trade secrets or intellectual property by disgruntled employees. The average cost of a data breach due to internal threats can cost organizations up to $8.7M to rectify.

Average cost of a breach due to internal threats: $8.7M

External Attacks

- An external attack is characterized as unauthorized access to an organizations data or networks, usually through extortion, forced breach, or device hack. These attacks can be initiated through malware links, key-loggers, air-gap-jumpers, man-in-the-middle attacks, to name a few.

Average cost of cyber-attack: $5.9M

Human Error

- Humans innately make mistakes. Whether an employee downloads unauthorized content, accesses an insecure network, does not use the VPN, has a weak password, or loses their computer - these mistakes can expose organizations to data breaches or hacks.

Average cost of 100 lost devices: $4.7M

These threats can have tangible impacts to organizations.

- To name a few: compromised devices, hardware replacement costs, ”time on keyboard” reprovisioning of end user devices, intellectual property loss, employee attrition, forced breaches, device hacks, malware links, regulatory fines, disruption of business operations, etc.

CHALLENGE: WHILE MULTIPLE SOLUTIONS EXIST TO PROTECT MOBILE WORKING CONDITIONS - NOT ONE SOLUTION ADDRESSED ALL VULNERABILITIES… UNTIL NOW.

STRENGTHS OF EXISTING SOLUTIONS IN MARKETPLACE:

Capability	VPN	VDI	Zero/Thin Client	District Defend®
Enables rapid deployment to users	✓			✓
Allows for reuse of existing hardware components	✓			✓
Reduces risk of sensitive data being stored on devices and potential offline compromise		✓		✓
Leverages backend resources that can be monitored for key work functions		✓		✓
Minimizes attack footprint on endpoint			✓	✓
Limits users' ability to interact with underlying device and download harmful content			✓	✓

DISTRICT DEFEND COMBINES STRENGTHS OF MULTIPLE EXISTING SOLUTIONS

MEET OUR SOLUTION: DISTRICT DEFEND, A SECURITY SOFTWARE THAT TRANSFORMS THE SECURE MOBILITY PARADIGM FOR WORKFORCES EVERYWHERE.

Availability on almost any Windows 10 compatible device

Built by Booz Allen, District Defend is security software that proactively protects and manages enterprise assets, while enforcing zero trust access to your networks and data, everywhere you do business.

Proactive Protection

District Defend proactively protects the organizations's data, devices and networks with automated and intelligent safeguards tailored to enterprise security rules.

Unmatched Asset Management

District Defend gives organizations critical insights into their device inventory, location and behavior with a single administrator tool.

Zero Trust Access

Ensures your enterprise devices are in a secure, trusted state prior to, during, and after users attempt to gain access to sensitive Enterprise resources.

Everywhere You Do Business

Enables devices to dynamically react to security threats in real-time based on custom protection profiles for secure access to and storage of data inside and out of Enterprise facilities.

PROACTIVELY PROTECT YOUR ORGANIZATION'S DATA, DEVICES, AND NETWORKS WITH DISTRICT DEFEND'S TAILORED SOLUTION

Proactive Protection

District Defend proactively protects your organization's data, devices and networks with automated and intelligent safeguards tailored to enterprise security rules.

Dynamic Command & Control

Automated configuration of endpoint security settings based on organizational policies, location, and user behavior.

Automated Policy Validation

Ensures devices have the requisite security mechanisms in place before allowing user access to the operating system, networks, or data.

Pre-Boot System Health Checks

Prevents low-level endpoint attacks and enables organizations to disable devices without enterprise network connection.

Enhanced Data Security

Automatically powers off, or securely wipes, devices outside approved spaces and enforces CSfC-compliant data-at-rest encryption.

GAIN CRITICAL INSIGHTS INTO YOUR ORGANIZATION'S ASSETS WITH DISTRICT DEFEND VIA A SINGLE PANE OF GLASS MANAGEMENT INTERFACE

Risk Management and Notification

Admins maintain situational awareness to device and overall system health.

Inventory Management

Reliable real-time context of where devices are and when they leave authorized spaces, as well as simplified user experience from not relying on multiple devices and/or paper notes to support the mission.

Analytical Insights and Control

Device/server usage data allows for advanced counter-intelligence analytics with tools such as Splunk to understand device behaviors and risks.

Simple Administrator Interface

Real-time configuration control of all enterprise devices without requiring physical access to the endpoint.

Unmatched Asset Management

District Defend gives organizations critical insights into their device inventory, location and behavior with a single administrator tool.

IMPLEMENT A ZERO-TRUST FRAMEWORK WITH THE HELP OF DISTRICT DEFEND

Zero Trust Access

Ensures your enterprise devices are in a secure, trusted state prior to, during, and after users attempt to gain access to sensitive Enterprise resources.

Isolated User Work Environments

Optional custom OS and kiosk mode prevents unauthorized applications and data from being stored on endpoints.

Comply-to-Connect Enforcement

Ensures endpoints are compliant with Enterprise policies and expected user behaviors prior to enabling access to vulnerable networked resources; and persistent monitoring to ensure on-going compliance and safeguarding.

Configurable User Access Controls

Supports access control decision frameworks for applications, VDI environments, and network resources, eliminating reliance on end-user compliance and manual system administration.

Seamless Infrastructure Assimilation

Augments existing security and management solutions without rearchitecting complex infrastructure components.

WHEREVER YOUR WORKFORCE IS LOCATED, PROTECT THEM WITH DISTRICT DEFEND

Safeguard Enterprise Spaces

Devices respond to environmental and user behavior triggers wherever they are – from office space, to classified environments, to aircraft and ground vehicles in the field.

Remotely Deliver on Sensitive Missions

Establishes CSfC-compliant mobile access solutions to wirelessly connect devices with classified environments, ensuring secure access to the right data at the right time – even outside of Enterprise-managed facilities.

Adaptive Security Enforcement

Automatically responds to changes in user or environmental conditions to enforce pre-defined defensive actions – reducing the potential and impact of unauthorized device access or use.

Locked-In-Transit Secure Transport

Encrypt and block power-on attempts while a device is being shipped, carried, or transported from one location to the other – preventing unauthorized access or actions by attackers.

Everywhere You Do Business

Enables devices to dynamically react to security threats in real-time based on custom protection profiles for secure access to and storage of data inside and out of Enterprise facilities.

HOW IT WORKS: DISTRICT DEFEND SOFTWARE OFFERS A SEAMLESS CONSUMER EXPERIENCE WHILE ENTERPRISE SECURITY PROTOCOLS ARE MAINTAINED

PRODUCT FEATURES:

CUSTOM POLICY DEFINITIONS

Endpoint Policies are easily defined by groups of devices, breaking the one-size-fits-all model. Select from a library of pre-written PowerShell scripts to enforce firmware controls, on-device monitoring and remote management or craft new scripts to meet the organization's needs.

WIRED & WIRELESS MANAGEMENT

District Defend Policies can be delivered directly to the endpoints via **Network Connection**, or **WiFi**. This allows organizations to augment existing security & management solutions without rearchitecting complex infrastructure.

VPN & VDI SUPPORT

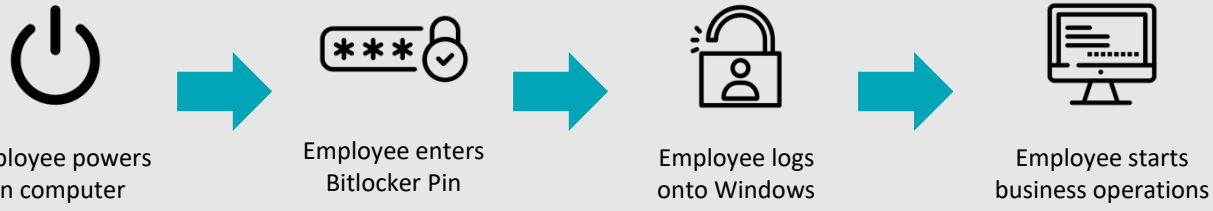
District Defend can lock users directly into a secure environment through automatic launch of VPN and VDI sessions; completely locking user out of native OS and prevents data to be stored on the endpoint.

aws

vmware CITRIX

USER EXPERIENCE

District Defend balances security and simplicity by enforcing two-factor authentication.



DISTRICT DEFEND SOFTWARE

All behind-the-scenes content happens without customer intervention.

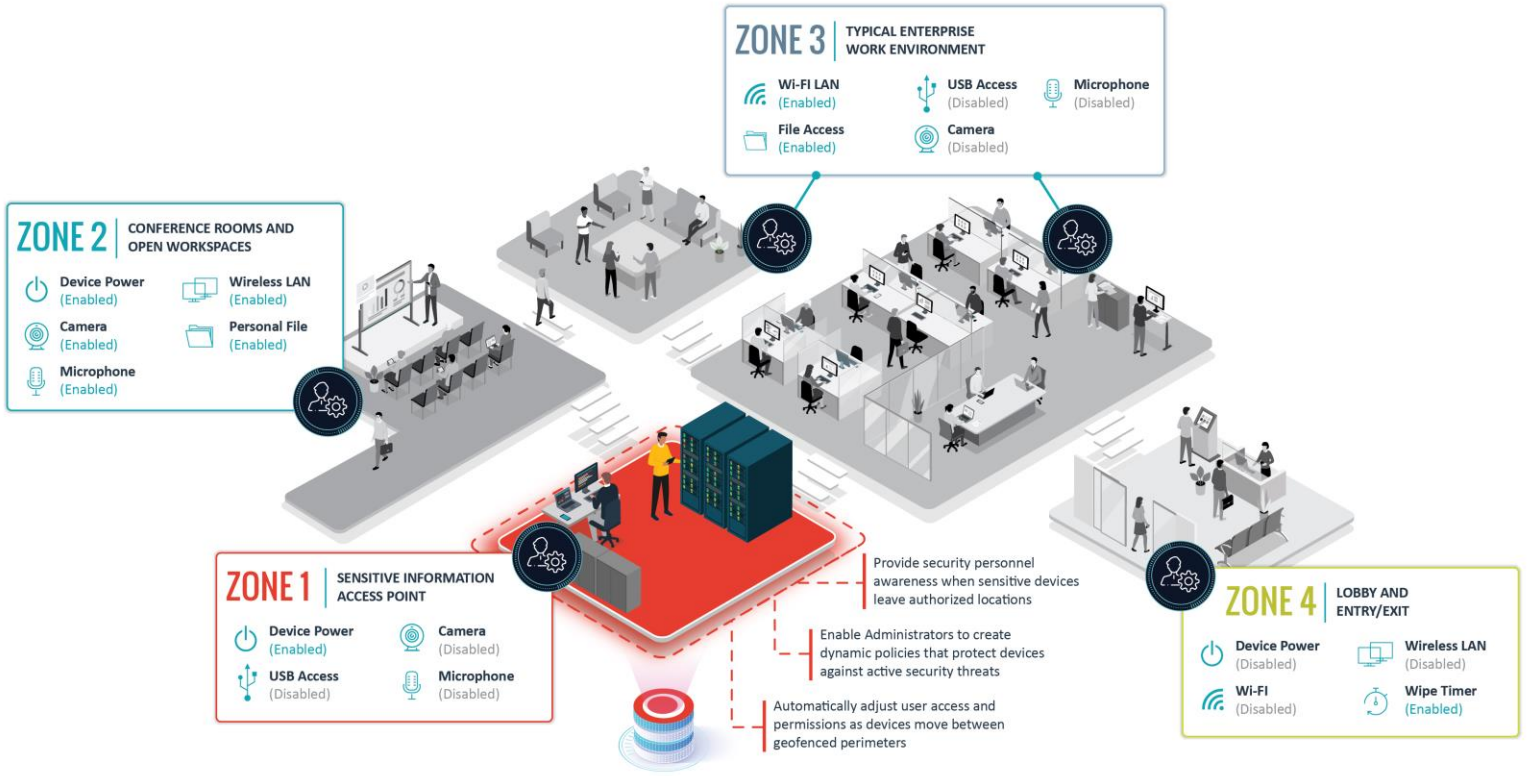
ZONE-BASED SECURITY ALLOWS USERS TO BE TRULY MOBILE, USING ONE DEVICE ANYWHERE WITHOUT SACRIFICING DATA INTEGRITY

DYNAMICALLY UPDATES SECURITY PROTOCOLS

As your device moves from location to location ("District" to "District"), it **automatically updates** security protocols and data access even when powered off.

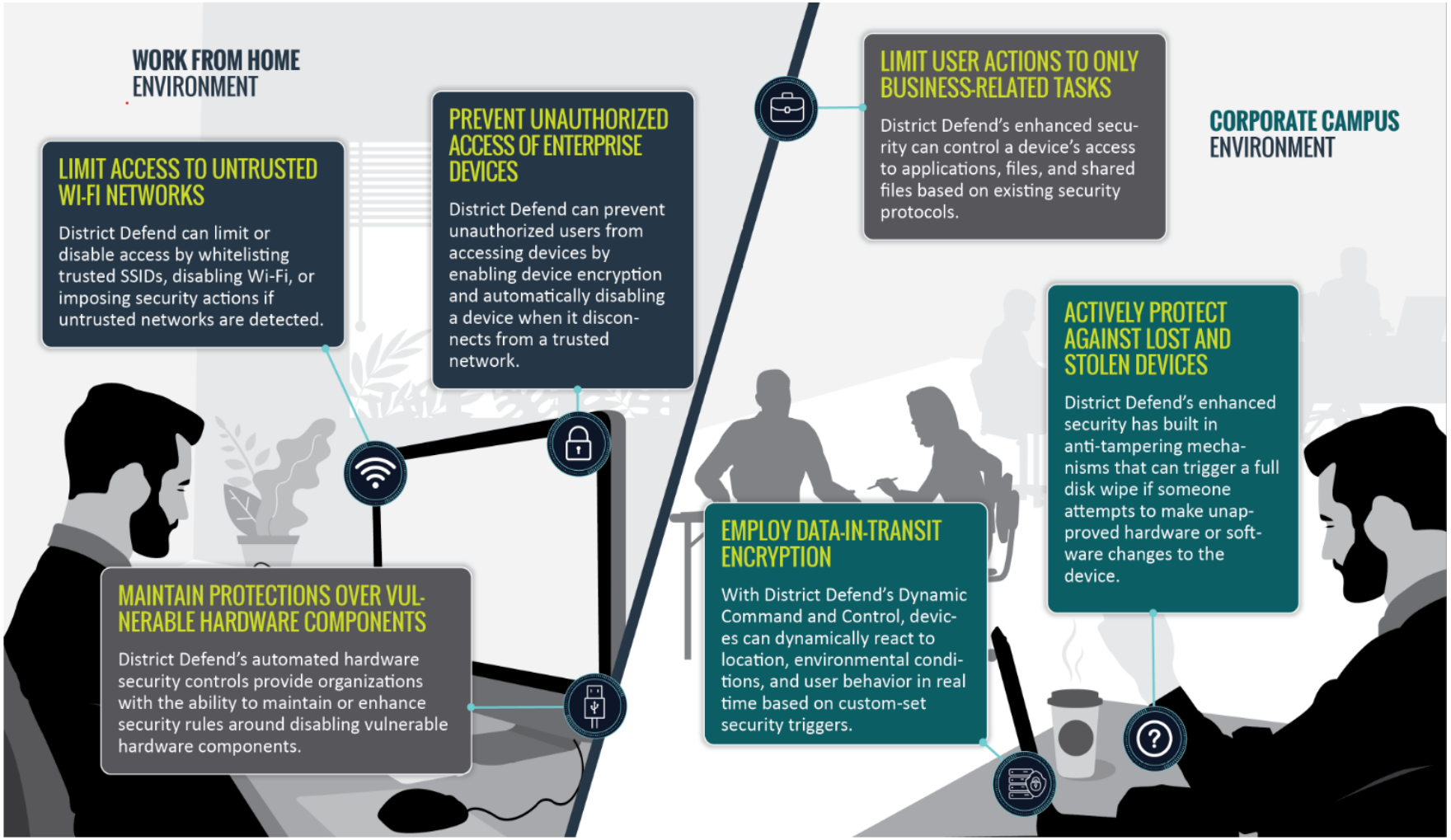
SEAMLESS MANAGEMENT

For the administrator, managing all enterprise devices' security configurations is as simple as flipping a switch.



SECURITY THAT AUTOMATICALLY KNOWS WHERE YOU ARE, AND HOW TO ADAPT

SECURE REMOTE TELEWORK



Risk Vectors:
- Distributed Workforces
- Lost or Stolen Devices
- Suspicious Behavior and Insider Threat
- User Uncertainty or Indifference to Policies

USE CASE: SECURE REMOTE TELEWORK

The Challenge:

A mission critical employee is forced to work from home and needs to access secure information from a single device, while maintaining strict security protocols regarding network access. It is essential for organizations to be able to quickly transition to a contingent remote workforce, ensuring continuity of day-to-day operations.

As the world embraces mobility, enterprises face an increasingly dynamic threat landscape. Common tools like Virtual Private Networks (VPN) and Virtual Desktop Infrastructure (VDI) might be seen as adequate security solutions, but these alone are not enough to effectively protect organizations and mitigate threats. To combat this, many organizations are considering solutions that automate security controls while monitoring and managing end user behavior, making it dramatically more difficult for attackers to exploit data and networks.

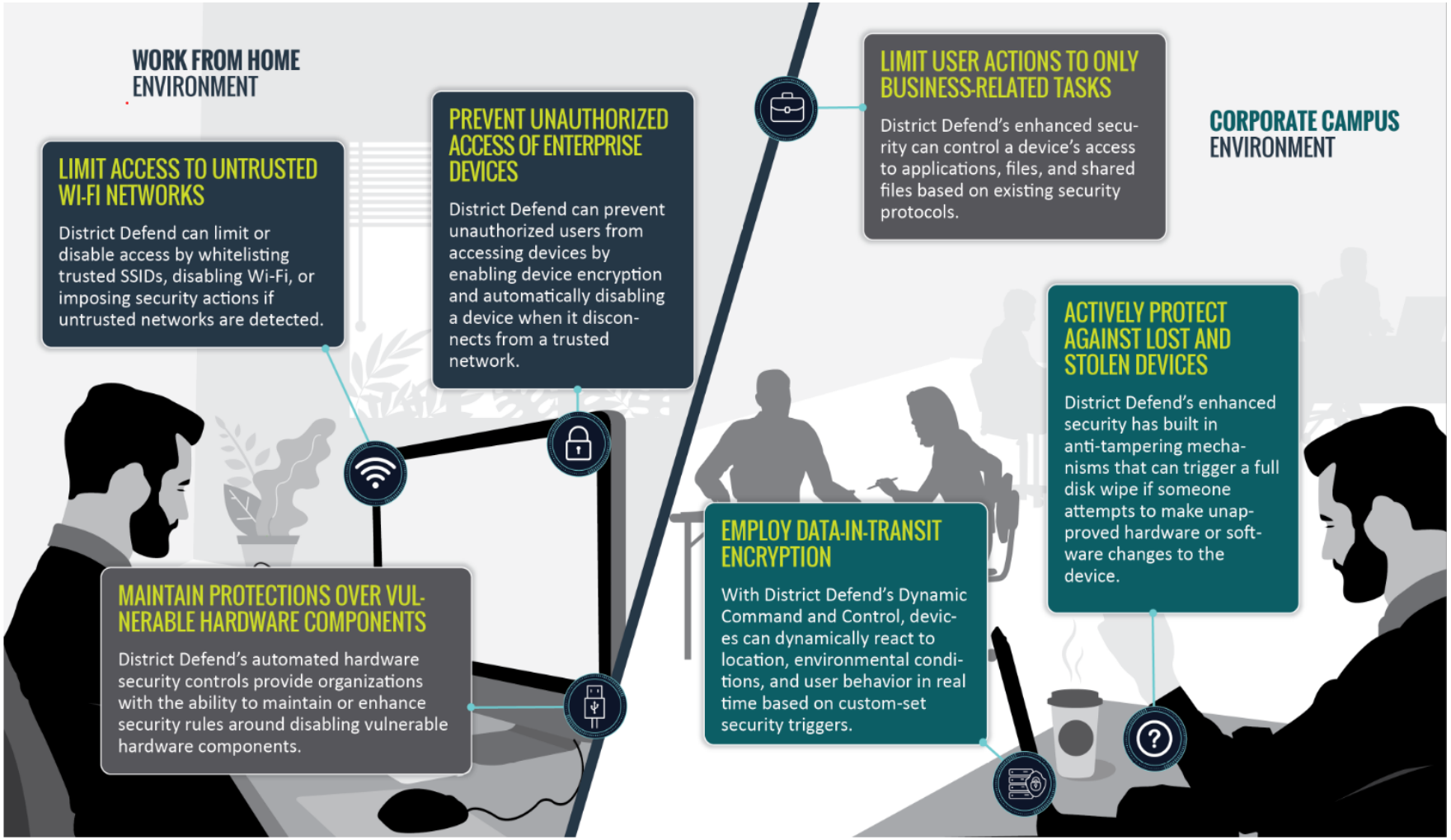
How District Defend enables the mission.
District Defend help employees work from anywhere and IT teams maintain control of the devices and network as if everyone's at the office. District Defend-enabled devices allow organizations to completely customize how their end user devices react to environmental, contextual and user conditions. IT administrators can control firmware settings, whitelist specific SSIDs, and control access to applications and files to ensure the right usershave access to the right data, in the right place at the right time.

How District Defend can help:

Endpoint security platform that proactively protects and enforces secure, zero trust access to networks and data, everywhere the mission needs

- Advanced Analytics with Splunk
- Monitors and Safeguards Data
- Geofencing Security Enforcement
- Automated Policy Validation
- Remote Hardware Disablement

SECURE REMOTE TELEWORK



Risk Vectors:
- Lost or Stolen Devices
- Suspicious Behavior and Insider Threat
- User Uncertainty or Indifference to Policies

USE CASE: REMOTE MONITORING AND MANAGEMENT OF ENTERPRISE ASSETS

The Challenge:
Security administrators are faced with the challenge of continuously tracking how many devices are in the facility, where they are, who owns them, and how they behave. Devices frequently move between enterprise locations, and these devices are often limited in where and how they work due to the nature of data that must be accessed on them. There is additional complexity since each organization has its own policies that impact device usage based on location, user role, and clearance level.

Administrators need a tool that will enable users to bring their organizationally approved devices into various enterprise spaces, automatically update them to facility-approved security settings, and provide real-time monitoring to support advanced analytics on device behavior and counterintelligence trends.

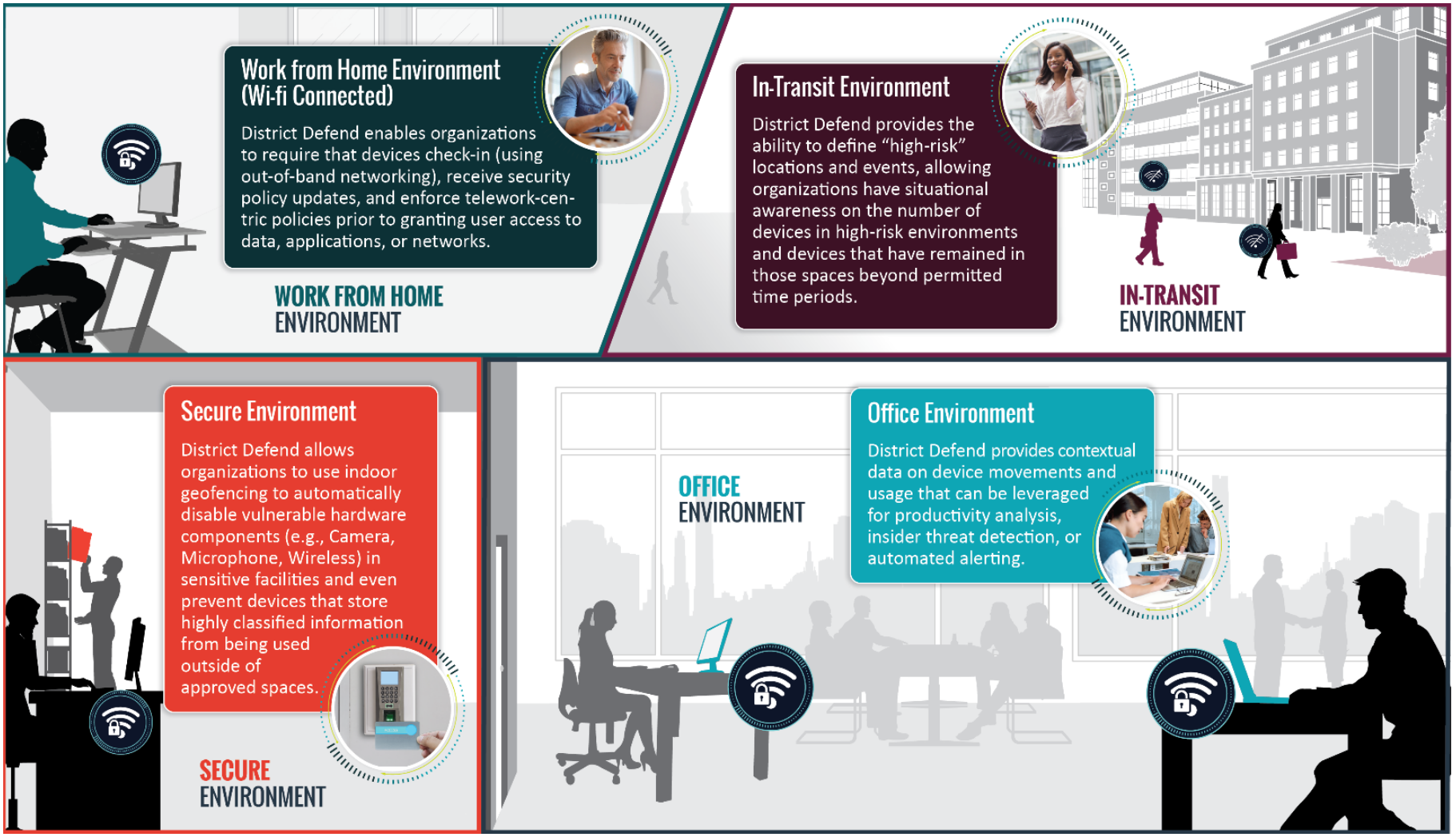
How District Defend enables the mission.
District Defend enables security administrators to establish 'Districts' for each organization, with policies that determine how devices behave based on organization, physical location, and user role/permissions. Administrators gain access to valuable pattern-of-life data, allowing them to perform advanced threat analytics with tools, such as Splunk, to identify insider threats and other counterintelligence risks.

How District Defend can help:

Endpoint security platform that proactively protects and enforces secure, zero trust access to networks and data, everywhere the mission needs

- Advanced Analytics with Splunk
- Monitors and Safeguards Data
- Geofencing Security Enforcement
- Automated Policy Validation
- Remote Hardware Disablement

REMOTE MONITORING AND MANAGEMENT OF ENTERPRISE ASSETS



Risk Vectors:
- Reliance on User Security Actions
- Compromised Mission Intelligence
- Man-in-the-Middle Attacks

USE CASE: REMOTE ACCESS OF CLASSIFIED RESOURCES

The Challenge:
United States government agents working abroad in the field are required to access sensitive and classified intelligence information to execute their mission. This creates complexities and inefficiencies as agents must be within embassy walls to access this data. The personal safety risks to agents are heightened in unstable environments when they are forced to travel with a device to an embassy to be able to access mission data.

Foreign agents need to be able to access classified information from a home environment, or wherever the mission takes them, but need to ensure that sensitive information is kept secure in the process.

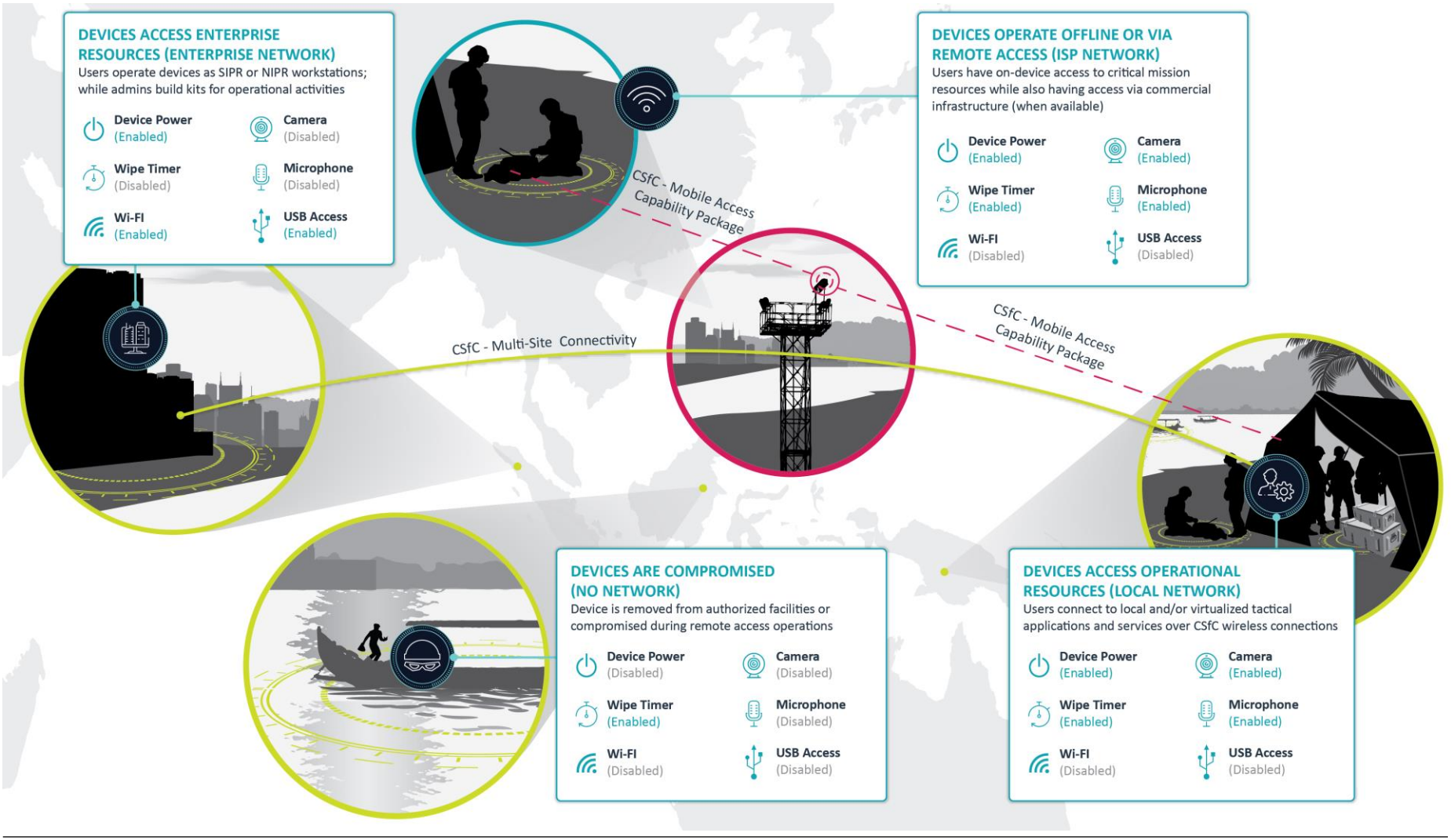
How District Defend enables the mission.
Deploying District Defend, in tandem with an AWS cloud migration, will enable agents to utilize hardwire connections at an agent's home, or mobile jet packs while on the go, to provide foreign service agents with added protections and underlying security to facilitate information flow and maintain personal safety, even when operating in hostile environments.

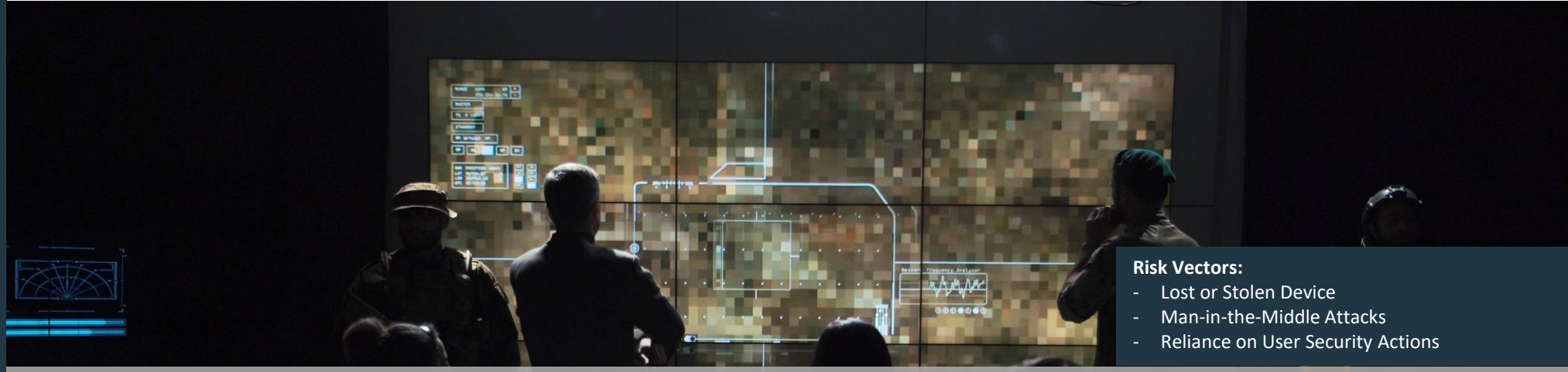
How District Defend can help:

Endpoint security platform that proactively protects and enforces secure, zero trust access to networks and data, everywhere the mission needs

- Secure Remote Disk Wipe
- Pre-Boot System Health Checks
- Behavioral Security Restrictions
- Automated Policy Validation
- Locked-In-Transit Secure Transport

REMOTE ACCESS OF CLASSIFIED RESOURCES





Risk Vectors:
- Lost or Stolen Device
- Man-in-the-Middle Attacks
- Reliance on User Security Actions

USE CASE: LEADERSHIP BRIEFING BOOKS AND EXECUTIVE CLASSIFIED WORKSTATIONS

The Challenge:
Today's government leaders are often forced to consume complex, multi-dimensional mission and intelligence data in static, text-based formats. Briefings can be conducted in a variety of environments with different security rules and requirements, as well as network accesses. Leaders need hardened devices that can safely store and secure classified data locally, while also connecting to approved networks when available. Unfortunately, local storage of highly classified data introduces risks as devices are moved frequently between facility spaces.

Additionally, many leaders are forced to switch between multiple devices for different use cases, scenarios, and operating environments. This requires managing and maintaining numerous endpoints and complicates their ability to take notes, respond quickly, and consume all necessary information for critical decisions.

How District Defend enables the mission.
District Defend enables leaders to use classified endpoints to consume and collaborate on valuable mission data without the need to worry about manually safeguarding actions. District Defend automatically conforms devices to each environment (enabling/disabling components as appropriate) and provides the ability to lock and/or shut down devices if removed by unauthorized personnel.

How District Defend can help:

Endpoint security platform that proactively protects and enforces secure, zero trust access to networks and data, everywhere the mission needs

- Adaptive Security Enforcement
- Location-Based Contextual Security
- Secure Remote Disk Wipe
- Automated Policy Validation
- Kiosk-Mode Application Locking

LEADERSHIP BRIEFING BOOKS AND EXECUTIVE CLASSIFIED WORKSTATIONS

LEARN MORE: CONNECT WITH OUR TEAM TO LEARN MORE.

Beau Oliver

Vice President

Oliver_Beau@bah.com

Jason Myers

Technical Director

Myers_Jason@bah.com

Questions? Reach out to the team at DistrictDefend@bah.com today.