THE SECURE MOBILITY CHALLENGE

Organizations today face the twin challenge of leveraging mobile technology to meet **demands of a changing global landscape** while securing said technology from an **increasing number of threat vectors.**

Securely enable the post-COVID acceleration toward remote and decentralized enterprise workforces.

Allow accessibility of classified and sensitive information where it is needed beyond offices and hardened facilities.

Position organizations for resilience against the risk of natural, man-made, and adversarial events.

Booz Allen built District Defend® to:

Manage devices and maintain security postures at scale within and outside of the office environment.

Allow leaders to consume classified information from automatically configured reader tablets.

Use mobile technology at the tactical edge without risking data exposure through device theft or loss.

Dynamically leverage the optimal thick / thin data operating modes or securely wipe missing devices.

THE CURRENT APPROACH: A LACK OF END-TO-END SOLUTIONING HAS PRODUCED GAPS AND SILOS IN THE PROTECTION OF ENDPOINT DEVICES

VPN

VPN offers the ability to rapidly deploy to end users and reuse existing hardware components.

VDI

VDI reduces the risk of sensitive data being stored on devices, leading to potential offline compromises. Additionally, VDI leverages backend resources that can be monitored for key work functions.

Zero/Thin Clients

Thin clients minimize the attack footprint on an endpoint and limit the users' ability to interact with the underlying device and download harmful content.

While many technologies focus solely on endpoint hardening, **District Defend®** integrates the strengths of existing solutions to provide proactive, adaptive device security and response.

As an end-to-end solution, District Defend offers central oversight to internal and external threats, giving organizations the ability to manage and protect their devices using a dynamic approach.

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

Availability on most Windows 10+ compatible devices

Built by Booz Allen, District Defend® is a software-based, security platform that keeps organizations' data, devices, and networks secure with automated and intelligent safeguards tailored to enterprise security rules. From proactively protecting and managing enterprise assets to zero-trust enforcement, District Defend dynamically adapts to changing threat environments, defending organizations against insider threats and advanced endpoint attacks.

Zero Trust at the Edge

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

Dynamic Hardening & Endpoint Protection

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

Commercial Solution for Classified (CSfC) Compliance & Enforcement

Executes against CSfC standards to provide your organization with unmatched data-at-rest, locked-in-transit, and data-in-transit capabilities.

Enables Remote & Hybrid Classified Workforces

Location and context responsive controls ensure your devices and data are secure wherever employees and deployed users need to perform their mission.

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

ZERO TRUST AT THE EDGE

Ensures enterprise devices can only be powered on in approved locations and can automatically power off devices that are moved outside of approved locations. Enforces remote data wipes if devices are lost or stolen. Prevents access to sensitive data and networks until device compliance has been validated.

Comply to Connect & Comply to Decrypt

Ensures endpoint devices are compliant with enterprise policies prior to enabling access to vulnerable networked resources or encrypted information; persistent monitoring ensures ongoing compliance and safeguarding of data.

Isolated User Work Environments

Prevents unauthorized applications and data from being stored on endpoints—limiting attack vectors on the endpoint and reducing potential compromises of sensitive enterprise data, while simplifying the user experience through a kiosk-mode interface.

Configurable User Access Controls

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

Seamless Infrastructure Integration

Integrates with existing security and management solutions, augmenting existing capabilities and filling key security gaps without rearchitecting complex infrastructure components (i.e., works with established VDI, VPN, patching, and cloud solutions).

PROACTIVELY PROTECT AND CONTROL YOUR ASSETS WITH DISTRICT DEFEND

Device Wipe & Device Disablement

Powerful automation that can work without connections to enterprise networks to lock user access or wipe hard drives (via cryptographically sanitization of the TPM and ATA Secure Erase)—mitigating risk from lost, stolen, or compromised devices.

Enhanced Data Security & Device Hardening

Dynamically adjusts hardware and firmware configurations based on location, environmental conditions, and user behavior in real time to comply with organizational rules without relying on end-user action or manual intervention.

Automated Policy Validation

Ensures that devices comply with organizational rules, have the requisite security mechanisms in place, and that vulnerable hardware is disabled before allowing user access to the operating system, networks, or data—reducing compromises for both endpoint systems and sensitive infrastructure resources.

Pre-Boot System Security Checks

Pre-boot security enhances the Secure Boot process by preventing unauthorized boot order manipulation and forced health checks to ensure a device is compliant and in an approved location before the hard drive is decrypted, Windows loaded, and that users can access data.

DYNAMIC HARDENING & ENDPOINT PROTECTION

Intelligent controls automatically enable or disable device features and check security settings before decryption. Dynamic security policies adjust configurations as users move through different environments. Lost, stolen, or otherwise compromised devices can be cryptographically sanitized and erased on-demand or based on automated triggers.

ENFORCE NSA CSFC STANDARDS WITH THE HELP OF DISTRICT DEFEND

COMMERCIAL SOLUTION FOR CLASSIFIED (CSFC) COMPLIANCE & ENFORCEMENT

Integrates by enforcing the NSA CSfC Data-at-Rest and Mobile Access Capability Packages. Provides additional enhancements including comply-to-decrypt, comply-to-connect, and location-based security controls beyond minimum thresholds.

Locked-in-Transit Secure Transport

Provides the ability to force encryption and prevent decryption of devices as the device is shipped, carried, or transported from one location to another—preventing tampering, unauthorized access, or other malicious actions by attackers who gain physical control of endpoints.

Automated Data-at-Rest Encryption Enforcement

Eliminates costly hardware-based encryption drives by automatically powering off non-compliant devices or disabling devices that are outside of approved spaces, thereby enforcing CSfC-compliant Data-at-Rest disk encryption.

Automated Dual and Nested VPN Management

Streamlined network management tools automate device configurations (and certificate updates) to ensure the appropriate VPN or Dual VPN Tunnels are used to protect data in transit.

Data Operating Modes

Complete control over on-device data through dynamic and automatic management of operating modes can pivot from disconnected or VPN-enabled computing (data-full) to cloud or VDI (data-less) configurations to reduce risk exposure.

WHEREVER YOUR WORKFORCE IS LOCATED, PROTECT THEM WITH DISTRICT DEFEND

Location-Based Security Controls

Dynamically configures hardware settings and endpoint controls based on physical location and continues to adapt in real time based on predefined policies to remain compliant without human action.

Remote Delivery from the Field

Automatically establishes CSfC-compliant mobile access connectivity to classified environments, ensuring agents have access to the right data at the right time—with confidence that data is secured on the edge when outside of enterprise-managed facilities and in hostile environments.

Secure Enterprise Telework

Helps employees work from anywhere and allows organizations to maintain device, data, and network security as if everyone is at the office. Powerful controls will configure firmware settings, whitelist specific SSIDs, and control access to applications and files based on location, environmental, and user conditions.

High-Value Asset Tracking

Provides organizations and IT administrators with unmatched insight into device inventory, location, behavior, and risk exposure with a single administrator tool including real-time context of devices in use, device counts in each location, and devices outside of authorized facilities (including absence duration).

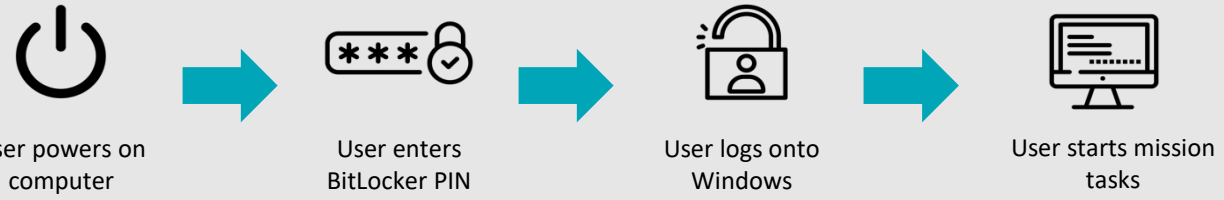
Enables Remote & Hybrid Classified Workforces

Enhances and complements existing security tools to provide stronger end-to-end solutions. Custom scripting and location-based device controls meet existing security protocols and CSfC requirements without infrastructure overhaul. Integrates with VDIs to allow provisioning by IT administrators possible in minutes instead of hours—cutting down on costs and operational disruption.

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

USER EXPERIENCE

District Defend balances security and simplicity.



DISTRICT DEFEND SOFTWARE

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

PRODUCT FEATURES

BOOT & PRE-OS SECURITY

- Confirms permission to boot
- Validates proper boot order
- Enforces policy compliance
- Monitors for changes & takes necessary security actions

CUSTOM POLICIES

- Supports a custom policy script engine using PowerShell
- Intuitive custom policy & device group management interface
- Wired & wireless provisioning
- Seamless security administration

DYNAMIC SECURITY

- Location-based security controls
- Automated VPN & VDI management
- Comply-to-connect
- Comply-to-decrypt
- Data-at-rest encryption enforcement

LOCK, WIPE, & DISABLE

- High-value asset tracking
- Device locked-in-transit controls
- Lost hardware disablement
- Cryptographic wipe & sanitization
- Irreversible secure disk erasure

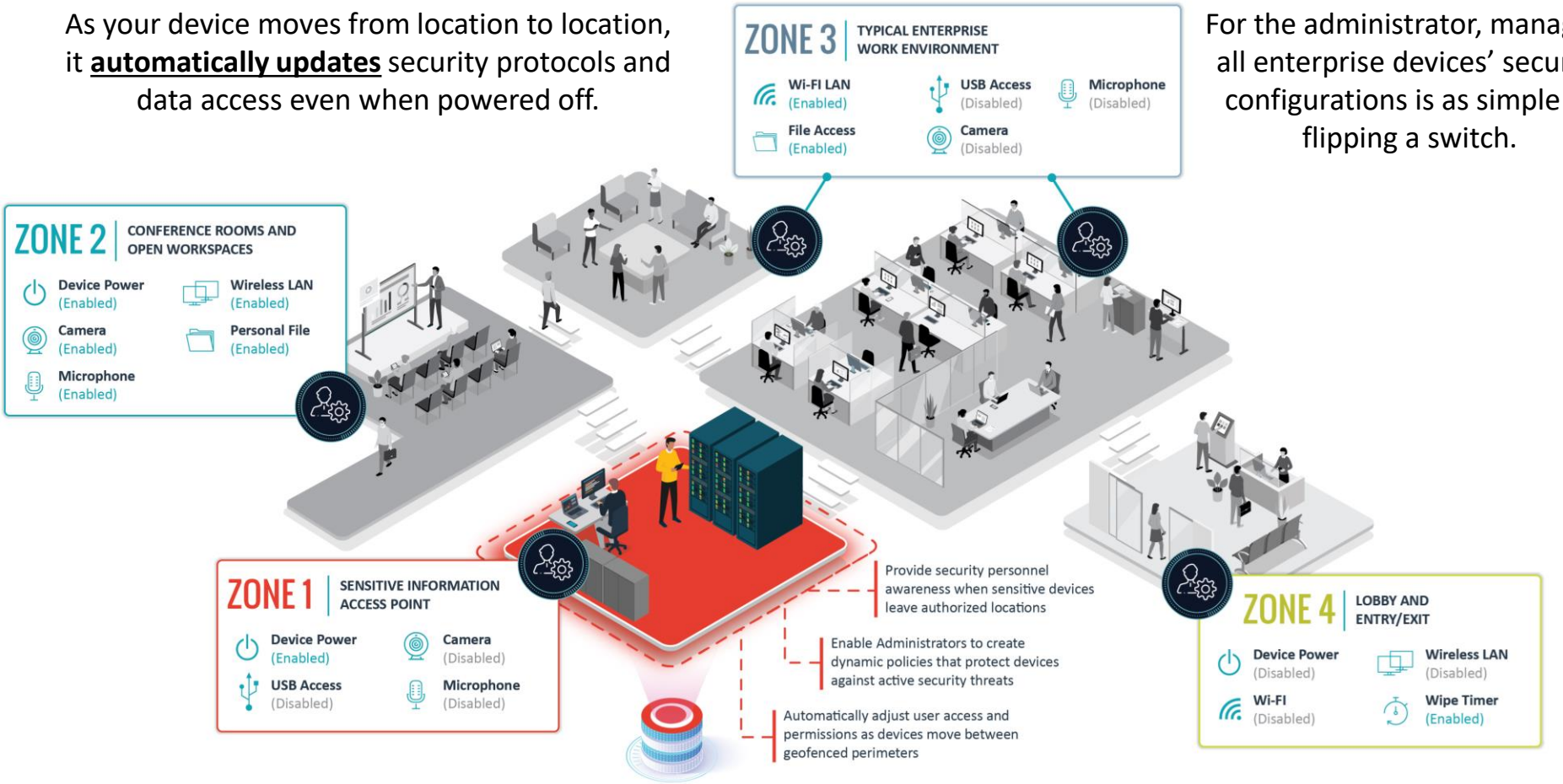
ZONE-BASED SECURITY ALLOWS USERS TO BE TRULY MOBILE, USING ONE DEVICE ANYWHERE WITHOUT SACRIFICING DATA INTEGRITY

DYNAMICALLY UPDATES SECURITY PROTOCOLS

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

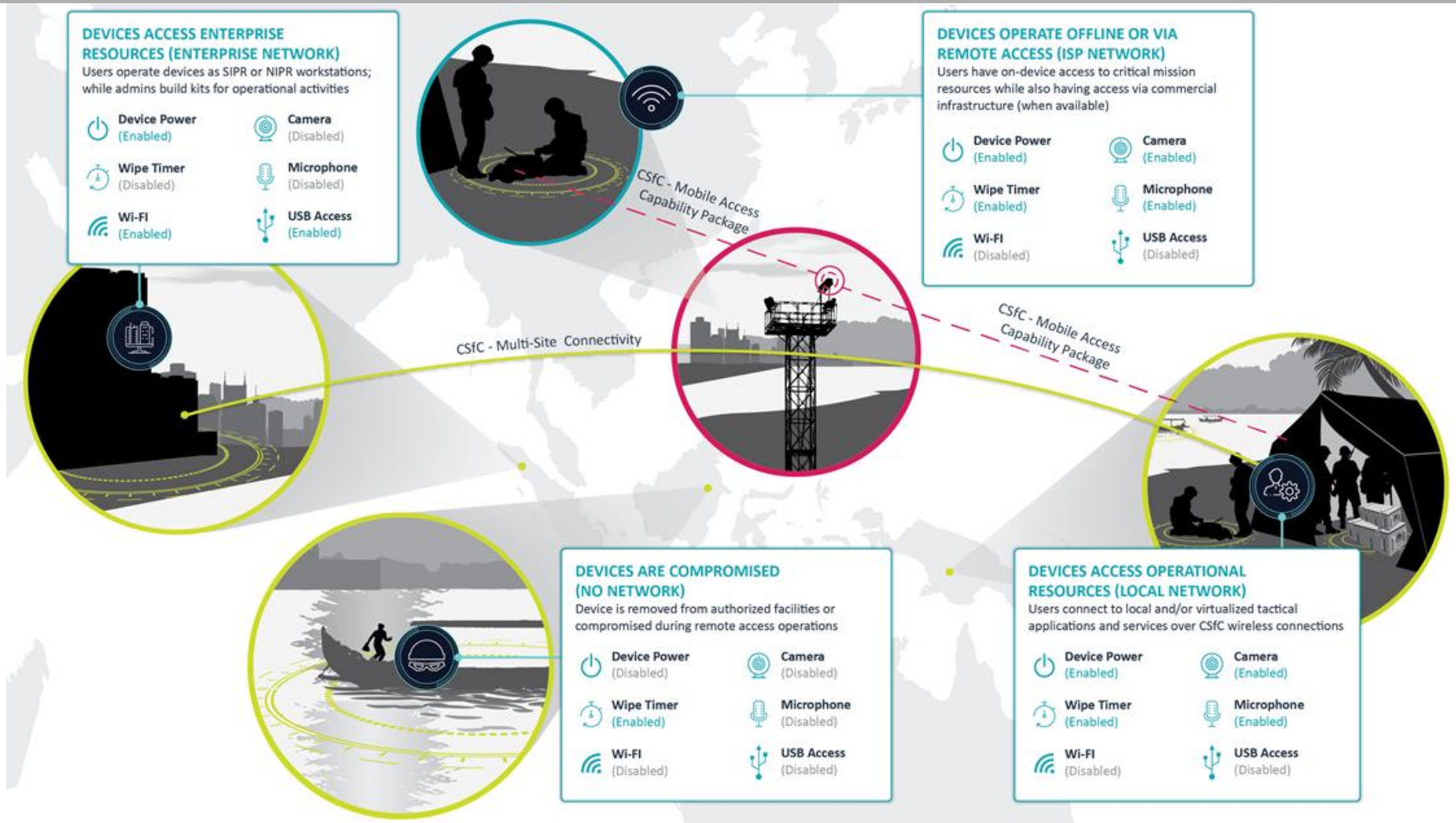
SEAMLESS MANAGEMENT

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

USE CASE: TACTICAL DEPLOYMENTS FOR CLASSIFIED OPERATIONS



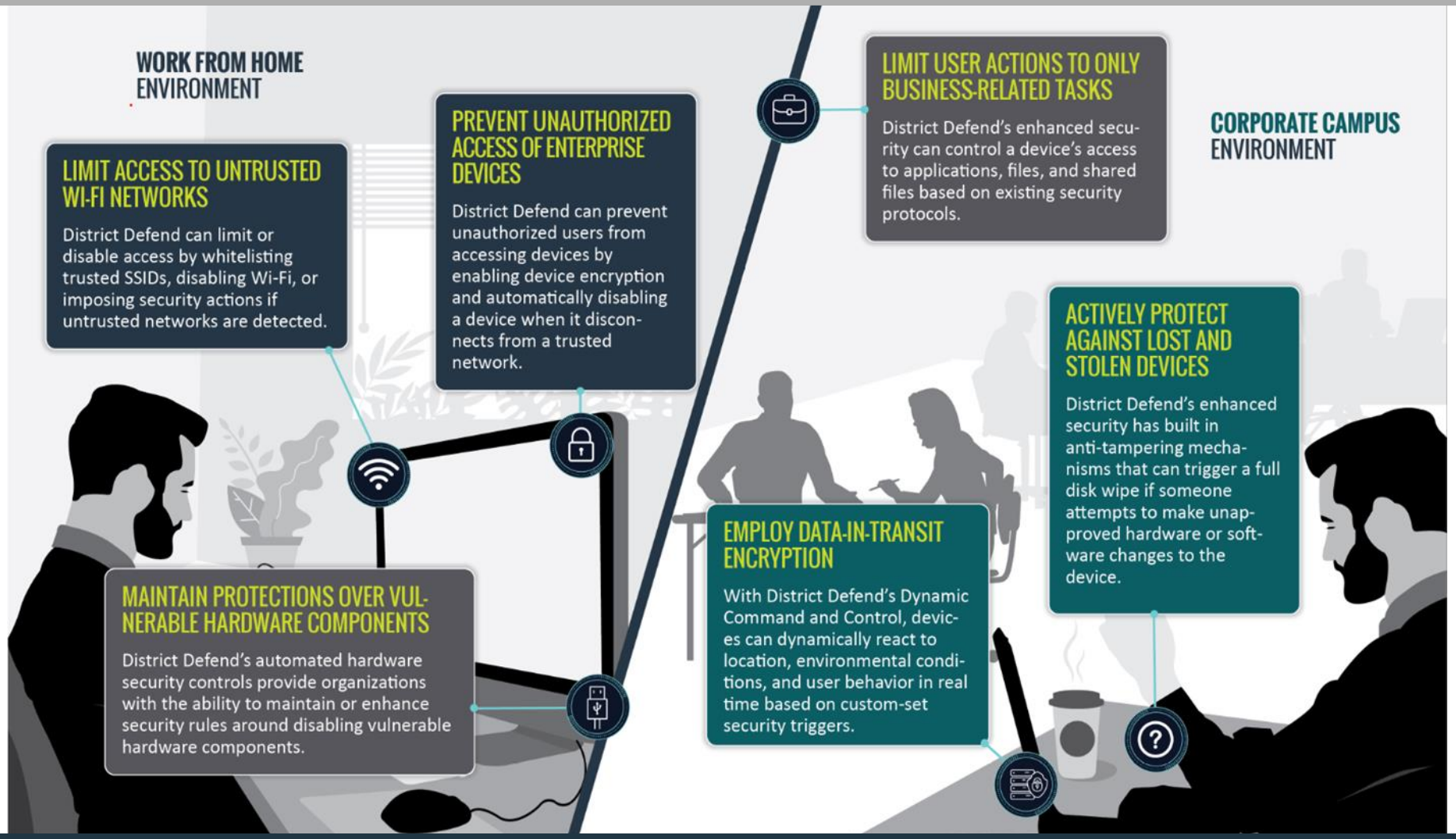
USE CASE:

Provide operators with wireless classified access world-wide, in cooperation with foreign partners, while delivering enhanced protections to overcome lack of physical defenses common in vehicles, tactical centers, and other austere environments.

DISTRICT VALUE:

- Locked-in-transit provides the ability to prevent tampering while devices are shipped globally
- Customize endpoint controls can be based on user groups, behavior, and physical location
- Hardware controls can disable vulnerable devices in unauthorized locations and/or conditions
- Forensically sound data wipes can sanitize devices in case of loss, overrun, or at the end of exercises

USE CASE: SECURE REMOTE TELEWORK & REMOTE CLASSIFIED ACCESS



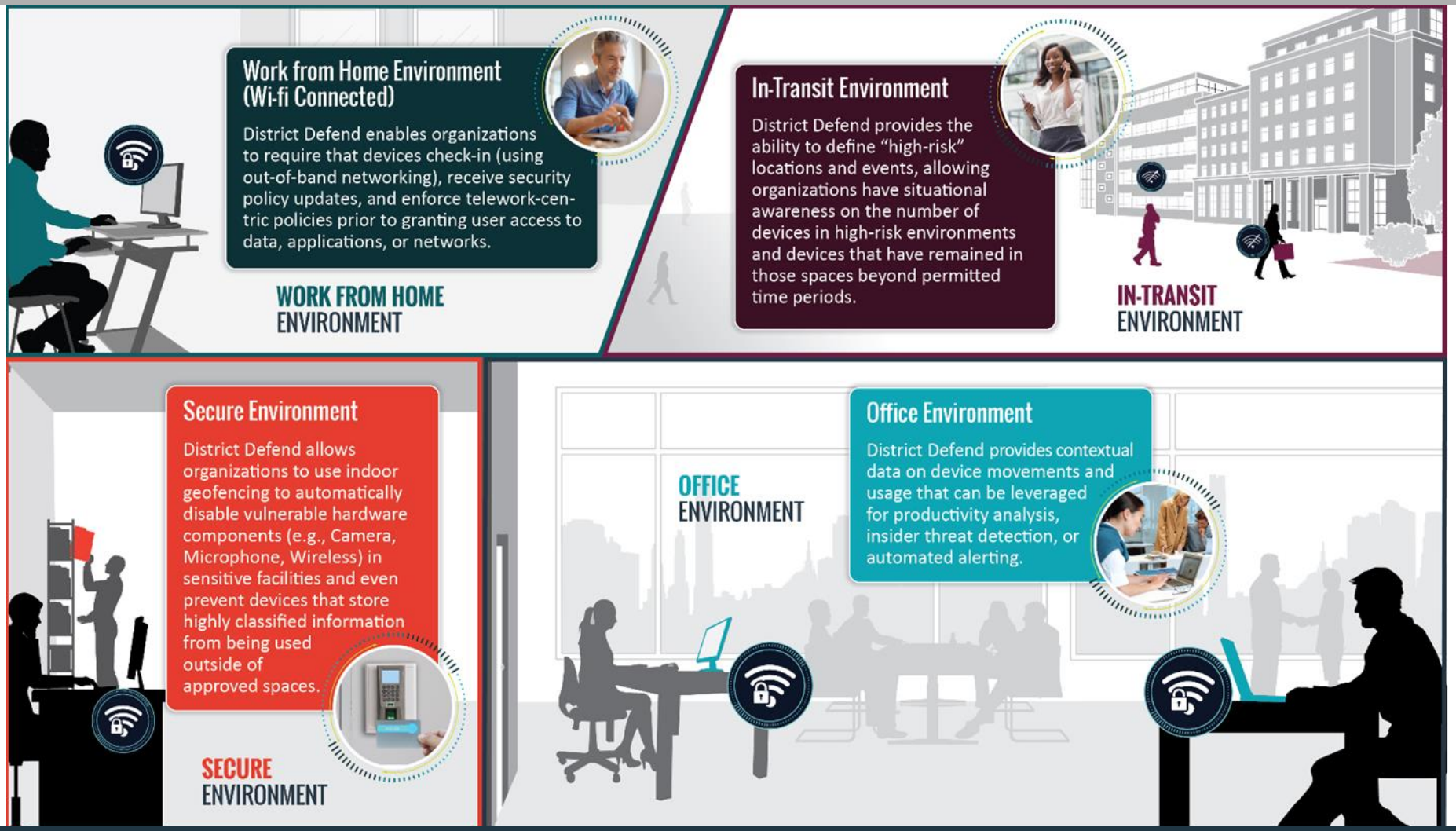
USE CASE:

Provide users of classified data with remote access to resources by securing endpoints while outside of organizationally controlled facilities. Protect classified, sensitive, personnel, operational, health, or financial data as if a device is being used onsite.

DISTRICT VALUE:

- Comply-to-decrypt & comply-to-connect provide zero-trust solutions to safeguard classified resources
- Custom scripts monitor user behavior for unauthorized actions (even when offline)
- Time-to-live triggers ensure that devices check in on time, while offering admins situational awareness
- Power-on disablement and automated wipes protect against lost/stolen devices in high-risk environments

USE CASE: ENTERPRISE OPERATIONS & ENDPOINT DEVICE MANAGEMENT



USE CASE:

Enable IT administrator to leverage zero trust principles and to safeguard critical organizational data (e.g., PII, HIPPA, financials) at enterprise scale by automatically enforcing customized policies for both on-premises and teleworking employees.

DISTRICT VALUE:

- Proactively and automatically adjusts network & data operating modes for on-premises & telework
- Controls firmware settings based on a device's location, both within a facility or when brought offsite
- Whitelists specific network SSIDs to allow remote work from known sites but avoid high-risk locations
- Prepares for contingencies by limiting access or initiating device wipe after a loss of network event

USE CASE: LEADERSHIP BRIEFING BOOKS & CLASSIFIED WORKSTATIONS

USE CASE:

Automatically configure devices to enable executive leaders to use a single endpoint to consume curated briefing material in specific conference rooms and/or provide full SIPR workstation capability within approved leadership offices or spaces.

DISTRICT VALUE:

- Detects environmental changes and dynamically controls device behavior and network/data access
- Configures network and data operating modes for executives moving between facilities
- Enhanced endpoint hardening protects high-value personnel from targeted attacks
- Devices removed from authorized spaces are disabled and ultimately wiped if lost/stolen

CONNECT WITH OUR TEAM TO LEARN MORE

Beau Oliver

Senior Vice President

Oliver_Beau@bah.com

Jason Myers

Technical Director

Myers_Jason@bah.com

Questions? Contact us today at DistrictDefend@bah.com and visit DistrictDefend.com to learn more.