Booz Allen | District Defend®

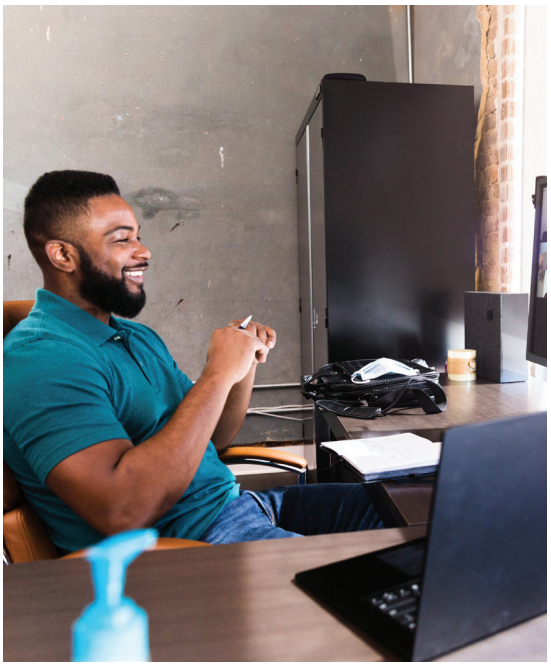
DISTRICT DEFEND®

GO MOBILE. STAY SECURE.

THE SECURE MOBILITY CHALLENGE:

Organizations today understand the need to embrace mobility, but doing so comes with inherent risk. Every day, malicious actors are plotting new ways to exploit enterprise networks and data. To stay a step ahead, security leaders must be forward-thinking and proactive about how they defend against these ever-evolving threats.

ORGANIZATIONS FACE A WIDE RANGE OF SECURITY THREATS, WHETHER USERS ARE WORKING WITHIN ENTERPRISE NETWORKS OR REMOTELY.



INSIDER THREATS:

An insider threat is the theft or misuse of organizational trade secrets or intellectual property by employees. Since employees often have elevated access to sensitive data and networks, there are fewer protections between them and an organization's most proprietary information.

EXTERNAL ATTACKS:

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

HUMAN ERROR:

People make mistakes. Whether an employee downloads unauthorized content, accesses an unsecure network, does not use the Virtual Private Network (VPN), has a weak password, or loses their computer, these mistakes can expose organizations to data breaches or hacks.

MEET OUR SOLUTION:

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.

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

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

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

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.

PROTECT DATA, NETWORKS, AND ENDPOINTS WITH DISTRICT DEFEND.

Looking for a security solution for your agency or organization?
Go mobile and stay secure with District Defend.
Contact us today at DistrictDefend@bah.com to learn more.

"District Defend is unquestionably the best geo-fencing security solution we've evaluated."

- Intelligence Community Customer

PROACTIVE PROTECTION

Situation: Enterprise security threats are continuously evolving, and data protections must be able to keep up. Forward thinking organizations are no longer relying on user training and manual precautions to protect their networks and data. These practices leave organizations exposed to breaches resulting from human error, the most common and most expensive threat to enterprise networks and data.

Organizations can stay ahead of changing threats by deploying tools that automate the endpoint security process to ensure that devices conform with enterprise policies, regardless of user role, location and time-bound permissions – even when powered off.

How District Enables the Mission:

- Automated Policy Validation
- Pre-Boot System Health Checks
- Enhanced Data Security
- Dynamic Command & Control

ZERO TRUST ACCESS

Situation: The future of work is here, and users are working wherever, whenever, and however works best for them. Organizations have been slow to catch-up and are resorting to traditional security mechanisms to protect data and networks in an environment that is anything but traditional. Too many organizations view traditional security mechanisms like VPNs as a silver bullet – they assume they can simply have users install VPNs and their enterprise will stay safe from attackers.

Instead, organizations should employ a solution that leverages the strengths of traditional security tools to create a true 'Zero Trust' environment that does not relay on the user to consciously comply.

How District Enables the Mission:

- Risk Management and Notification
- Analytical Insights & Control
- Simple Administrator Interface
- Inventory Management

UNMATCHED ASSET MANAGEMENT

Situation: Security administrators must continuously track how many devices are in their facilities, where they are, who owns them, and how they behave. When users connect remotely, administrators lose visibility and control to endpoints, adding risk for the organization. The challenge is heightened since various organizations may have their own policies that impact device usage based on location, user rank and clearance level.

Administrators need a tool that will automatically update endpoints to facility approved security settings and provide monitoring of devices to allow for advanced analytics that inform device behavior and actions.

How District Enables the Mission:

- Comply-to-connect enforcement
- Isolated User Work Environments
- Configurable User Access Controls
- Seamless Infrastructure assimilation

EVERYWHERE YOU DO BUSINESS

Situation: As today's missions become increasingly globalized, users demand the ability to access the right data at the right time, wherever work takes them. For some, this means countless hours spent in airport terminals and hotel rooms. For others, it can mean moving from the office to a classified environment or accessing data from the mission's edge in an aircraft or ground vehicle.

Time spent outside of traditional office spaces equals increased risk of data loss. Organizations need to ensure that devices automatically sense and respond to changes in user or environmental conditions – even outside of enterprise-managed facilities.

How District Enables the Mission:

- Safeguard Enterprise Spaces
- Remotely Deliver on Sensitive Missions
- Adaptive Security
- Locked-in-transit secure transport

CONTACT DISTRICTDEFEND@BAH.COM TO LEARN MORE ABOUT THIS OFFERING TODAY!