Booz Allen | District Defend®

DISTRICT DEFEND®

GO MOBILE. STAY SECURE.

CONSULTING | ANALYTICS | DIGITAL TRANSFORMATION | ENGINEERING | CYBER

EXECUTIVE SUMMARY

Where and how we work has changed. 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.

Booz Allen developed District Defend® to address gaps in the secure mobility space by bridging the intersection of proactive protection, asset management, Zero Trust access on existing devices, and availability everywhere users are approved to support their mission. District Defend leverages technology from the commercial sector, lessons learned from defending the U.S. Federal Government from nation-State actors, and novel concepts from some of the world's best innovators to establish a technology solution that meets client's most challenging endpoint security needs.

Read on to learn how District Defend, a software solution from Booz Allen Hamilton, builds on the strengths of existing solutions to address the remaining security gaps, providing truly proactive protection, asset management and Zero Trust access for wherever your enterprise workforce does business.

ORGANIZATIONS OFTEN MISTAKE COMMON CONNECTIVITY TOOLS FOR SECURITY SOLUTIONS

ADOPTING A ZERO TRUST FRAMEWORK CAN HELP ORGANIZATIONS STRENGTHEN THEIR CYBER-SECURITY POSTURE.

With the explosion of mobility across the technological landscape, users are no longer tied to one location or one network. Zero Trust enables mobility within enterprise spaces and beyond while also ensuring end-to-end security across a variety of business needs. Zero Trust is the framework upon which a security conscious organization should guide their security architecture, procurement, and installation.

Zero Trust helps prevent data breaches by treating any "trust" verification-based action as an inherent vulnerability. By embracing this mindset, organizations can transform their security posture to reap the full benefits of enterprise mobility. Unfortunately, some organizations simply decide to deploy a Virtual Private Network (VPN) or Virtual Desktop Infrastructure (VDI) as "good enough" solutions, leaving critical components unaddressed in their end-to-end architecture.

AMPLIFYING THE VALUE OF LEGACY SECURITY SOLUTIONS

A **Virtual Private Network (VPN)** creates a secure connection to another network over the internet through end-to-end encryption of a user's data. Organizations use VPNs to protect sensitive data transmission, to share data securely and quickly between separate networks, and for connecting mobile employees to centralized servers. Today, over 400 million businesses and consumers worldwide use some form of VPN due to its rapid deployment and interoperability with existing hardware solutions.

While VPNs enhance security, they're only effective when employees use them correctly and consistently. When users fail to engage them, whether deliberately or by accident, and instead browse open internet resources without enterprise awareness, they expose themselves, the device, company data, and core networks to outside threats.

Virtual Desktop Infrastructure (VDI) is a software solution used to create a virtualized desktop environment on a centralized server, which is then deployable to authorized end user devices. VDI segments the servers into various virtual desktops which the users can access remotely through their devices. Many organizations prefer to use VDI because they can leverage back end resources for monitoring key work functions, and the risk of locally stored data is neutralized.

While VDI products have become a popular security solution, they fail to address multiple endpoint vulnerabilities. Employees may still access their local USB drive or other hardware features (e.g., microphone, camera, etc.) that can introduce risk in a VDI environment. Malicious actors can also employ malware attacks (e.g., keyloggers, app hijacking, and screen scraping) to seize control of the device before delivering the user into the VDI environment.

THE PROTECTION THESE SOLUTIONS PROVIDE IS NOT ENOUGH

VPN and VDI are widely recognized across key industries as essential products for security conscious organizations, but they cannot be accurately labeled as truly "zero trust" because they still rely on end users to activate them. Unsurprisingly, the vast majority of data breaches trace back to the end user, whether it be through user error, negligence, or willful disregard of security policies. Organizations need a way to strengthen their legacy security solutions without significant capital investment, time to enterprise deployment, or infrastructure overhaul.

Adopting a Zero Trust mentality even when devices are outside of their physical control, eliminating reliance on the end user, and automatically monitoring and enforcing organizational security rules in real time will help organizations enhance their overall security posture.

MEET DISTRICT DEFEND: A SECURITY SOLUTION THAT TRANSFORMS THE SECURE MOBILITY PARADIGM FOR WORKFORCES

Whether your employees are working at a secure facility, from their home office, or any other work environment, District Defend proactively protects and enforces secure, Zero Trust access to your networks and data. By transforming existing Windows 10 compatible devices to fit the "Zero Trust" framework, District Defend mitigates vulnerabilities that lead to malicious data breaches or spillage.

Installed under the operating system, District Defend proactively monitors and safeguards enterprise data, networks, and devices of employees. Real time security policy and software updates are pushed to user devices to ensure on-site security standards are upheld and enforced – enabling limited authorized access to sensitive networks and information, as desired. Organizations no longer need to "trust" users are performing enterprise-related work, conducting only authorized activities, and properly safeguarding material – they can continuously monitor and enforce these policies in real-time.

MAIN PRODUCT FEATURES

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

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.

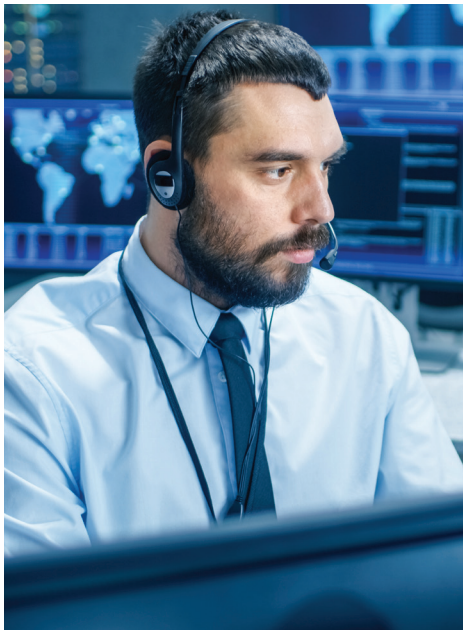
Unmatched Asset Management: District Defend gives organizations critical insights into their device inventory, location and behavior with a single administrator tool.

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.

WHERE IT PROTECTS

In the office: The way endpoints are used within enterprise spaces is changing, and data protections must be able to keep up. In certain industries, it is common for users to regularly move between spaces of differing sensitivity or classification levels, accessing varying types of information in the process. Enabling them to move between these spaces using a single device, instead of being tethered to a desktop or forced to rely on paper notes, allows them to stay productive without compromise. In addition, 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, external attacks, and insider threats.

Organizations can experience the advantages of mobility and stay ahead of changing threats by deploying District Defend to automate the endpoint security process. This will ensure devices conform with organizational policies, regardless of user role, enterprise location and time-bound permissions – even when powered off.



Outside the office: 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 means moving from the office to a classified environment or accessing data at 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.

District Defend enables the mission by using features such as adaptive security enforcement and locked-in-transit secure transport to ensure that only authorized users can access networks and data, regardless of where they connect from.

HOW IT WORKS

District Defend strikes a critical balance between advanced security processes and seamless user experience – delivering automated intelligence that is invisible to the user. This elegant design ensures a straightforward user experience while limiting attack vectors and upholding endpoint se-curity operations.

Once the user initiates device power-up, the District Defend security software confirms the device is permitted to boot up in its current environment. This confirmation is based on predefined organizational policies, as configured in the District Defend administrator interface. The software then validates the proper boot order sequence and prompts the user to enter their Bitlocker Pin.

If the device is authorized for use, District Defend launches into the Pre-User Operating System. In this stage, District Defend ensures that the device is configured based on organizational policies (e.g. USB disabled) to ensure policy compliance. Additionally, it monitors for contextual triggers that may cause the device to take a predefined security action (e.g. disable camera and microphone if device boots in a sensitive space). With the device configuration appropriately set, the user can login to their Windows OS.

Once logged into Windows, additional controls may be enforced based on organizational policies. For example, this could mean that a user is forced into a VPN or VDI connection. At this point, the user can begin normal business operations, and the District Defend security management software will continue to monitor for new policy updates. It will also continuously run custom policy scripts (as desired) to monitor for unauthorized user behavior or external environmental triggers, and perform corresponding defensive actions (e.g., disabling networking, disabling USB ports, shutting down device).

In addition to the endpoint components, the District Defend solution comes with a back-end policy management service that allows organizations to register new devices, identify the status of devices, update security policies, and even export audit data for further analysis.

Organizations manage a wide range of cyber risks that generally fall into three main categories: external attacks, insider threats (including human error), and organizational inefficiencies. District Defend can help organizations mitigate these risks without requiring an overhaul of current infrastructure or policy.

REDUCING THE RISK OF EXTERNAL ATTACKS FOR ENTERPRISES

District Defend can help enterprises reduce vulnerability to malware, keyloggers, air-gap-jumpers, man-in-the-middle, and other types of attacks by:

Pre-Boot System Health Checks: Prevents low-level attacks against the endpoint and enables organizations to disable devices without being connected to enterprise networks – mitigating access to enterprise certificates/keys and reducing ability to inject persistent threats when devices are physically compromised.

Isolated User Work Environments: Optional custom OS that 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.

Remotely Deliver on Sensitive Missions: Establishes CSfC-compliant mobile access solutions to wirelessly connect devices with classified environments, ensuring users have access to the right data at the right time – with confidence data is secured to the edge even outside of Enterprise-managed facilities.

"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.

Analytical Insights and Control: Provides endpoint device/server usage data and critical counterintelligence data, allowing administrators to leverage Splunk analytics to understand device movement/usage, high risk behaviors, and insider threats.

Enhanced Data Security: Automatically powers off devices outside approved spaces and enforces CSfC-compliant data-at-rest encryption; as well as offering remote data wipes if devices are stolen or left outside secure spaces beyond defined thresholds.

MONITORING USER BEHAVIOR TO IDENTIFY INSIDER THREATS

District Defend can help enterprises monitor user behavior to identify the misuse of company assets, such as devices or intellectual property.

Adaptive Security Enforcement: Automatically senses and responds to changes in user or environmental conditions to enforce organizationally-defined defensive actions – reducing the potential and impact of risky user behaviors or unauthorized access attempts.

Automated Policy Validation: Ensures devices comply with organizational rules, have the requisite security mechanisms in place, and 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.

Risk Management and Notification: Role-based access to management interface with situational awareness on number of devices in high-risk environments, devices that have been wiped due to potential compromise, and overall system health.

Locked-In-Transit Secure Transport: Provides the ability to encrypt and power-off devices (blocking subsequent power-on attempts) while a device is being shipped, carried, or transported from one location to the other – preventing tampering, unauthorized access, or other malicious actions by attackers who gain physical control of endpoints.

Dynamic Command & Control: Leverages pre-boot and run-time validation and enforcement to support automated or manual configuration of endpoint security settings (e.g., hardware disablement, wipe, application access) based on organizational policies, user role, location, and time-bound permissions

MITIGATING ORGANIZATIONAL INEFFICIENCIES

District Defend can help enterprises quickly deploy software by seamlessly integrating with existing infrastructure.

Safeguard Enterprise Spaces: Organizations can customize their devices to dynamically react to location, environmental conditions and user behavior in real time based on custom-set security triggers in a wide variety of enterprise spaces, from office space, to classified environments, to aircraft and ground vehicles in the field.

Seamless Infrastructure Assimilation: 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, and cloud solutions).

Inventory Management: Provides real-time context of how many devices are in use, device counts in each location, and knowledge of when devices leave authorized facilities (and the duration of absence).

Simple Administrator Interface: Controls the configurations of all enterprise devices across numerous user groups and approved locations without requiring physical access to the endpoint device or manual processes.

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.

SOLUTION DETAILS

SIMPLIFIED IMPLEMENTATION TO KEEP YOUR WORKFORCE FOCUSED ON THE MISSION

District Defend works with any Windows 10 compatible device and is installed beneath the OS to add to an organization's "defense in depth" strategy. Custom scripting capabilities empower organizations to customize device behavior to meet existing security protocols and adapt to changing requirements without infrastructure overhaul.

District Defend operates as a security enhancing software, compounding on the strengths of existing tools to provide a more secure end-to-end solution. Strategic partnerships and thoughtful architecture design ensure District Defend can be integrated with leading VDI solutions, including AWS, Google Cloud, Citrix, VMWare, and Microsoft Azure. In addition, devices can be provisioned by IT Administrators in minutes, not hours, cutting down on costs and operational disruption.

WHY BOOZ ALLEN?

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision.

SUMMARY

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.

With the help of industry leading technology partners, Booz Allen Hamilton developed District Defend to be differentiated in the endpoint security space. District Defend exists at the intersection of proactive protection, asset management, zero trust access on existing devices, and availability anywhere users do business. It allows organizations to monitor and manage data and networks today, while establishing the infrastructure to respond to the unknown threats of tomorrow.

IN SHORT:

With District Defend, be confident that your organization can go mobile, and stay secure.

Take the Next Step

Talk to a team member about options for deploying District Defend in your enterprise.

About Booz Allen Hamilton

Booz Allen Hamilton is at the forefront of technological innovation, collaborating with clients, academic institutions, and the business community to address urgent information security challenges. Having been engaged in offensive and defensive cyber capabilities surrounding the nation's most sensitive data, Booz Allen's computer forensic experts know firsthand which data and application-protection solutions are most effective, and how to render them ineffective. Drawing on this expertise, Booz Allen's engineers developed District Defend, a software solution to protect data, networks, and endpoints in the defense, IC, civil, health, and commercial sectors without sacrificing either device security or employee productivity.

For more information, please contact:

DistrictDefend@bah.com
