District Defend

Powerful, zone-based security for sensitive data on mobile devices

DELL EMC

Booz | Allen | Hamilton
In the federal government and commercial enterprises, theft and inappropriate access to confidential information can compromise national security, damage a company’s viability and reputation, and put individuals at risk. Today’s data protection measures often restrict user productivity to achieve an acceptable level of security. Booz Allen Hamilton, a leading problem-solver for government and private-sector customers for over 100 years, has created District Defend™ to ensure device usability and information security so that you can harness the power of modern technology without opening the door to security gaps. This white paper provides an overview of how District Defend solves some of your most pressing security concerns and empowers organizations to proactively manage cyber threats.

Costs and consequences of data breaches mount while security measures lag

U.S. federal agencies, large banks, healthcare providers and retailers top the list of the entities that face an elevated risk of cyber attacks. In the public sector as well as in commercial industries, data theft and threats to intellectual property and software systems challenge security, IT and operations managers to stay ahead of ubiquitous cyber threats. The measurable costs and tangible consequences of such data breaches are enormous.

$7.01M  
Average cost of a data breach in 2016

4X  
Worldwide increase of cyber crime costs from 2013 to 2015

2X  
Projected worldwide increase of cyber crime costs from 2015 to 2019

Malicious actors employ various techniques to attack your systems, including spoofing wireless networks, cleverly disguised phishing attempts, and sophisticated hardware and firmware exploits. For example, cyber attackers sometimes set up fraudulent resources that look like a legitimate network, or they spoof WiFi, GPS or Bluetooth technologies to compel users to provide inadvertent access to their devices. Frequently, they exploit particularly vulnerable boot-up periods during which not all security tools and policies are fully activated.
Resourceful hackers interested in the informational or monetary value of confidential data routinely work around multifactor protocols, password security and software-based solutions, which tend to leave glaring vulnerabilities that they can exploit in a couple of hours. These threats are dynamic, requiring organizations to constantly play catchup to protect network integrity. Companies often rely on employees to actively avoid cyber threats, leaving organizations at the mercy of human error.

A common, often successful attack: The rubber ducky

In this scenario, USB drives with malicious code are planted in an organization’s parking lot for employees to find and insert into their device. Multiple studies find that close to half the people finding a USB drive do exactly that.

Employees remain highly vulnerable to threats posed by cyber criminals and may, unwittingly or intentionally, expose sensitive data and applications to attack. This may happen when administrators have ill-advised privileges on a device, given that these privileges are often associated with the ability to easily disable security functionality, thereby potentially creating an insider threat. Attempts by users to circumvent seemingly tedious security protocols to enhance device functionality and productivity are even more prevalent. Adding to these challenges, executives and senior managers often obtain waivers that enable them to use their mobile devices without being slowed by security measures. User intervention in information security protocols has proven to be a significant source of organizational friction between employers and employees.

Widespread struggles with security and usability concessions

The federal government and commercial enterprises make significant investments in data-protection technologies and take steps to protect their data assets from theft and unauthorized access. However, it tends to be difficult to achieve effective security while you also aim to enable mobile employees to take advantage of all the features of high-end laptops and tablets.

In the federal space, security is often favored over usability, restricting the use and movements of laptops and tablets, or disabling functionality to mitigate risks posed by frequently targeted mobile devices. Providing employees with partly disabled or older, less technologically advanced devices is detrimental to recruiting talent and building the workforce of the future. In commercial environments, organizations often favor productivity-enhancing devices and err on the side of compromising the integrity of organizational information security.

Clearly, every organization has to make trade-offs between security and productivity. No matter what approach companies and government agencies take to provide mobile security, the risk of attack will persist. Nonetheless, they all must work to create and maintain an active defense against these threats.
Booz Allen District Defend: A location-based, policy-compliant security solution

Booz Allen Hamilton is at the forefront of technological innovation, collaborating with its clients, academic institutions and the business community to address urgent information security and other challenges. Working with Dell EMC, Intel and Microsoft, Booz Allen Hamilton created District Defend, a new security solution to keep mobile devices in public-sector and commercial environments functional and secure. The company’s computer forensic experts have been engaged in offensive and defensive cyber capabilities surrounding the nation’s most sensitive data. That means they know firsthand which data and application-protection solutions are most effective, and how to render them ineffective. Drawing on this expertise, Booz Allen Hamilton engineers developed District Defend, a new way to protect mobile devices without sacrificing either device security or employee productivity.

Security districts and dynamic policy enforcement

Booz Allen District Defend uses physical security zones, known as districts, that are associated with configurable security policies set by administrators (see the government office use case example). As mobile devices move through districts, policies are automatically pushed through an out-of-band sensor network so that the devices dynamically conform to the security rules associated with their current environment.
Booz Allen Hamilton and Dell injected District Defend software into the boot sequence and firmware, allowing the solution to receive out-of-band policy messages, control power states, dynamically disable hardware, dump keys in TPM and trigger forensic disk wipes. This firmware disablement doesn’t just prevent access to the operating system, it shuts down power to the physical ports, allowing you to render WiFi, Bluetooth, USB, MicroSD, SIM and other hardware components inoperable. This security protocol deployment is functional even when devices are turned off, leaving end users no role in policy enforcement.

Taking advantage of security-enabling features in hardware, processor and operating system

District Defend currently runs on Dell Latitude 5285 2-in-1 devices, which can serve as both laptops and tablets and will eventually extend to the full range of Dell mobile computers. An excellent fit for demanding security requirements, Latitude 5285 devices incorporate several advanced data-protection capabilities:

- Smartcard reader that complies with Federal Information Processing Standard (FIPS) 140-2 and is certified for FIPS 201 and Trusted Computing Group Trusted Platform Module (TPM) 2.0
- Touch fingerprint reader
- Near-field communications (NFC) functionality
- Self-encrypting drive
- Dell ControlVault to store and safeguard security credentials, passwords and biometric authentication
- Dell Endpoint Security Suite Enterprise and Secure Lifecycle to enable strong, yet manageable data protection
In addition, District Defend on the Latitude 5285 takes advantage of the performance and security features of the Intel® Core™ i7 processor and the multiple layers of security supported by Windows 10 Enterprise. District Defend meets the standards the National Security Agency (NSA) has set for Commercial Solutions for Classified Program.3

Easy, flexible security management after guided setup

With District Defend, security management becomes more flexible and efficient. Booz Allen Hamilton consultants work closely with you to prepare a site survey and determine organizational requirements for establishing districts and defining security policies across user classes.

After the initial setup, you can easily adjust and reconfigure districts, policies and devices in a web-based application. From that centralized console, administrators can create and disseminate policies anytime, without needing to collect and manually update devices with new policies. Security policies are highly customizable and can be deployed uniformly, by user class or for individual users, with the option to dynamically shift settings for short-term requirements.

District Defend even safeguards against data loss from device theft. You can configure settings in District Defend to remotely erase data from the device’s storage drive if the device does not check in within a certain timeframe. A disk wipe performed through District Defend is forensically sound; it does not leave a data image that can be recovered by somebody using specialized tools.

Contextually aware, multilayer security boosts information protection

District Defend devices are built as an integrated platform that uses hardware, firmware, operating systems and applications to cohesively harden and protect your most sensitive information. District Defend incorporates:

- Attestation checks to validate integrity of network components
- Watchdog timers to prevent tampering and enforce encryption
- Boot-order modifications to prevent shims or security bypass attempts
- Other defense-in-depth measures to maintain device security at the deepest levels

Specific security protocols apply to each of these device components. If one security protocol is compromised, the others continue to function and protect the device, and a digital intruder cannot hop from one component to another. The solution accomplishes this isolation of device elements by means of hypervisor software; you can work with Booz Allen Hamilton cyber experts to determine the appropriate hypervisor for each use case.

Because District Defend handles security protocols below the operating-system level, it can effectively protect devices from rootkits and other sophisticated cyber attacks. Federal government agencies impose stringent security measures on devices, such as safeguarding their key components with discrete protection solutions. District Defend complies with these federal standards.
District Defend multilayer encryption technology is highly customizable and pairs well with commercial and proprietary encryption solutions. Booz Allen Hamilton consultants collaborate with your organization’s security and technology managers to enable the strongest possible security for mobile devices.

**Productive users and proactive IT security management in action**

Booz Allen District Defend automates compliance with environment and user-specific security policies. With District Defend’s enhanced, dynamic security features, users no longer need to worry about their permissions and restrictions, and IT managers no longer need to worry about usability outweighing security. You gain full visibility and complete control of devices enabled with District Defend. This technology represents a shift from reactive practices that are limited to mitigating the influence of breaches after the fact and identifying stolen data, to proactive device policies that greatly reduce and even eliminate the impact of stolen devices and cyber attacks.

Users benefit from the enhanced mobility potential facilitated by District Defend. At work, at home or on the road, devices automatically assume the appropriate security setting and enable users to conduct their digital lives as unencumbered as their environment allows.

District Defend supports a variety of data-protection scenarios in federal and commercial settings. District Defend has broad applications that include but are not limited to:
Empowered executives. In many organizations, enabling leadership and key contributors to work effectively while protecting their data and devices is a top priority. Today, many federal agencies provide executives with secure devices to receive briefings on the go. These devices typically lack productivity-enhancing functionality — such as WiFi, cameras, speakers and USB ports — which limits their usefulness. District Defend secures the most sensitive data without permanently impeding device functionality.

Enterprise policy enforcement. Using District Defend, you can easily implement enterprise-wide updates to security policies and remotely deploy these policies from a centralized administrative console. Policies are deployed immediately, regardless of a device’s network connectivity. This is a more reliable and less labor-intensive way to ensure consistent policy enforcement for all mobile devices.

Organization-wide risk mitigation. By deploying District Defend to users who create or access confidential, mission-critical data, you can greatly reduce risk exposure and help maintain the inherent value of data. In the federal government, securing devices and information can be a matter of national security. In healthcare, protecting confidential patient data and implementing role-specific security can prevent identity theft and ensure appropriate patient care. In finance, safeguarding mobile devices and data can prevent market manipulations and other illegal activities. In research-driven businesses, the design, engineering and production of innovative products require data to be held extremely closely to ensure a company’s competitive edge.
Getting started with District Defend

Learn more about District Defend’s adaptable, powerful security platform. Take the next step:

- Contact Booz Allen Hamilton at District_Defend_Sales@bah.com
- Learn more about Dell EMC.
- Learn more about District Defend by watching a video and reviewing solution details and FAQ.
- See the options and features of Dell Latitude 5285 2-in-1 devices.

1. secureworks.com/blog/ten-reasons-average-data-breach-costs-7-million
3. nsa.gov/resources/everyone/csfc/ for more information on the NSA’s standards for Commercial Solutions for Classified Program.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, Intel® Core™ are trademarks or registered trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. This case study is for informational purposes only. Dell and EMC make no warranties — express or implied — in this document.