Booz | Allen | Hamilton

Booz Allen Launches District DefendTM, New Location-Aware Technology Enables Mobile Computing and Greater Collaboration in Secure Workplaces

September 27, 2018

District Defend-Enabled Devices Empower Employees with the Information They Need, Where and When They Need It Without Sacrificing Security

- Available on select Dell Latitudes, District's location-aware technology could transform and significantly increase worker efficiency for the U.S. government while lowering long-term costs by providing a single device that can navigate between secure and unsecure environments.
- New survey data finds that a major factor limiting the government's ability to rapidly adopt mobile technologies is the tension between mobility and necessary security standards: though 60 percent of respondents report stringent security controls that inhibit mobility, nearly 75 percent feel that mobility is very or extremely important for their organization.

MCLEAN, Va.--(BUSINESS WIRE)--Sep. 27, 2018-- Booz Allen Hamilton announced today the availability of new mobility technology —District Defend™ —that uses patented security protocols to make the management of mobile devices like tablets in highly sensitive and classified environments easier and less complex. District Defend™, available on select Dell computers, brings the benefits of mobile computing to the public sector, unlocking opportunities to better collaborate, work from more places, and handle different types of data while mitigating security threats that have traditionally hampered mobility adoption within government.

According to a new survey of federal decision-makers commissioned by Booz Allen, a major factor limiting the government's ability to rapidly adopt mobile technologies is the current tension between mobile workplace practices and stringent security standards. Nearly 6 out of 10 respondents note they have stringent security controls that inhibit mobility in the workplace. And yet, three-quarters of respondents (74%) feel it is very or extremely important for their organization to have mobility.

"Mobility traditionally comes at a cost for government users, restricting productivity and collaboration in favor of stricter security," said Dee Dee Helfenstein, a Booz Allen Senior Vice President and leader of the firm's Solutions Business. "District Defend empowers government users managing highly sensitive and classified environments to mitigate security breaches from human error, limit advanced attacks, increase enterprise mobility, and enable secure communication. Simply put, District opens a world of possibilities for agencies managing data across multiple locations."

District Defend technology combines RFID and military-grade security to dynamically create "Districts"—each a distinct physical location with varying levels of security access. For example, when a District Defend-enabled device crosses into the perimeter of a secure location, the technology automatically pushes the appropriate security protocols to the device —regardless of whether the device is powered on. These security rules can simultaneously enable access to sensitive networks as appropriate and disable firmware functions that could capture and transmit secure information like the capability to record, use USB ports and access fraudulent networks. When the device leaves the secure location, access to sensitive information is closed off and encrypted with full functionality automatically restored once the device re-enters an authorized location.

District Defend could significantly lower costs for the U.S. government while increasing the efficiency of government workers. Government employees regularly use a multitude of different devices and computers to manage information: unclassified devices that cannot enter a classified location and classified devices that require different levels of security based on the information being accessed. District Defend-enabled devices give government employees a single device they can bring back and forth between spaces while keeping sensitive information contained and secured—serving as leadership-briefing books, on the go computers, enterprise desktop replacements and more. District-enabled devices are ideal across a variety of scenarios, including:

- **Mixed Use Buildings**: Many buildings with classified spaces have rooms with different classifications, including controlled unclassified spaces (e.g., conference rooms), and common unclassified spaces (e.g., lobby or cafeteria). District Defend-enabled devices can dynamically adjust to their environments and enforce security policies for each space as the device is carried around the building.
- **Locked in Transit**: Devices in transit from manufacturing plant to end user are often at higher risk of compromise. District Defend allows for devices to be completely disabled and encrypted until they reach their desired destination, significantly reducing the risk of breaches.

"District Defend, currently on the Dell Latitude 5290 2-in-1 device, will eventually be available on the full range of our mobile computers," says Steve Harris, general manager and vice president of Dell EMC's federal business. "The pairing represents an ideal marriage of hardware, firmware, operating system and applications to create a tightly secured system."

In addition to the immediate application of District Defend to help protect classified government information, the technology is highly adaptable to the private sector. In the future, it could help secure personally identifiable information and protect intellectual property and proprietary information – a threat that costs U.S. businesses hundreds of billions of dollars annually.

To learn more about District Defend, visit: https://www.boozallen.com/s/product/district-defend.html.

To review the survey mentioned above, visit: https://boozallen.com/s/insight/publication/mobility-and-security.html.

BAHPR-CO

About Booz Allen Hamilton

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world.

We solve the most difficult management and technology problems through a combination of consulting, analytics, digital solutions, engineering, and cyber expertise. With global headquarters in McLean, Virginia, our firm employs approximately 24,600 people globally, and had revenue of $6.17 billion for the 12 months ended March 31, 2018. To learn more, visit www.boozallen.com. (NYSE: BAH)

View source version on businesswire.com: https://www.businesswire.com/news/home/20180927005466/en/

Source: Booz Allen Hamilton Holding Corporation

Booz Allen Hamilton
Media Relations:
Joseph Campbell, 703-377-4422
Campbell_Joseph@bah.com
or
Investor Relations:
Nick Veasey, 703-377-5332
Veasey_Nicholas@bah.com
or
Industry Analyst Relations
Katie Sheldon Hammler, 703-377-6727
SheldonHammler_Kathryn@bah.com