Reducing the Risk Surface

A holistic approach to security – HSPD-12

Too many users, too many passwords, too much access! That is the issue the IT security world is struggling with today, including those at the executive level, who are focused on the entire environment. Executives look for solutions to meet the compliance across all disciplines within the organization, including mobile, data center, cloud, applications, or even infrastructure-as-a-service.

Because of this, a ubiquitous, across-the-board solution is needed. This allows organizations to impose the correct compliance measures because each component has its own limiting factors. On the user side, if an organization is using various tools, each will be accessed securely in a unique way adding to too many passwords.

WTOP and Federal News Radio have partnered with Centrify to create this industry briefing to explore deeper the following concepts: HSPD-12, continuous diagnostics and mitigation, and identity as a perimeter.

Joining the discussion will be Greg Cranley, Centify's vice president federal and US public sector sales. Cranley will offer context as well as Centrify's solutions to these complex issues.

HSPD-12

The Homeland Security Presidential Directive 12 was put into law back in 2005 by President George W. Bush. At the time, the administration saw an opportunity to curtail the access to government data, equipment and facilities by using an electronic card instead of a user ID and password. The card would be coupled with a PIN, usually 4 or 6 digits long. The idea was to get away from the easily compromised user ID and password, which is the cause of many data breaches or compromised identities.

"The intent was that people would have something they have and something they know," said Cranley. "And to separate the two would be difficult for someone to hack in to."

According to Cranley, some people embraced it very quickly and, some didn't embrace it at all. Some people that felt that they weren't really "dot gov employees" and that their contractor status provided them immunity from compliance.

"So data breaches continued for a long time, and then as we saw, it culminated in the summer 2015 with the OPM breach," Cranley said. "And in actuality the breach had been going on for several years."

This initiative was followed by the cyber sprint initiative of federal CIO Tony Scott, who wanted to see two-factor authentication throughout government.

Cranley noted the balance between complying with the rules and being secure. The sprint started with an emphasis on getting privileged users to start using two-factor authentication, and then looked to incorporate the rest of the agency. He said one issue is that people interpret the rules differently.

"They think if they use their PIV/CAC card on laptop or desktop, they are secure," Cranley said. "But it's a problem when they go to other resources in the organization and still use a user ID/password. So the approach is not holistic or across-the-board in terms of how privileges are accessed.

"Having too many identities, too much access, too much privilege really denigrates the purpose of the security policy," according to Cranley. And in today's working environments, more people have access to more than ever before.

"It was the data center people; it was the technologists that had access to that," Cranley said. "Regular workers didn't have access to the important information." He says years ago information was written down, but now it's mostly stored electronically on phones and tablets. "Things don't need to be memorized anymore," he added.

Workers today have access to information about their companies that wasn't available to them 20 years ago. "It's there to do your job," Cranley said. "They want to take this technology and make you productive from it. But with that there are inherent risks and it gets you on the inside to where the data is stored. And while you may not in your role have access to certain things, you're connected to people that do. And if I can get in through your identity and I'm in the network, then who knows what damage I can cause or the data I can steal if I can find a power user or someone who runs the data center…Once I'm in, it's just a matter of scoping around."

But there is progress being made to get away from user names and passwords. Companies and agencies are embracing PIV and CAC cards, and Centrify is well-positioned to help meet the needs of HSPD-12.

Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure access to infrastructure, DevOps, IaaS, containers, Big Data and other modern government attack surfaces," states Cranley. "As traditional network perimeters dissolve, organizations must discard the old model of 'trust but verify' which relied on well-defined boundaries. Zero Trust mandates a 'never trust, always verify, enforce least privilege' approach to privileged access, from inside or outside the network. Centrify Zero Trust Privilege helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Centrify minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity and costs for the modern, hybrid government."

"Agencies may consider approaching Privileged Access Management by solely implementing password vaults, leaving gaps that can easily be exploited. Centrify Zero Trust Privilege combines password vaulting with brokering of identities, multi-factor authentication enforcement and "just enough" privilege, all while securing remote access and monitoring of all privileged sessions," he concluded.

Conclusion

Ultimately organizations must take the time to look for a holistic solution that's going to cover their entire problem. They must use modern technology instead of trying to fit things into what was developed in security policies more than a decade ago.

"The idea is you want to reduce the risk surface and by having spot tools you're only going to put pinholes in your risk surface," Cranley said. "Having a holistic tool is going to cover your data center and your cloud in concert with some other tools you already have in place, will really minimize your risk surface to nothing."

This paper was created in partnership with:

FEDERAL NEWS NETWORK

About Federal News Radio

Federal News Radio 1500 AM and FederalNewsRadio.com comprise the key source of breaking news, information and analysis for the individuals responsible for carrying out and supporting the missions of federal agencies. Federal News Radio addresses federal agency managers, policy makers and contractors.

Federal News Radio's coverage is non-partisan, non-political and is designed to help executives more clearly understand and make better decisions about issues affecting their agencies and their companies.

Federal News Radio broadcasts live on 1500 AM throughout the Greater Metropolitan Washington area. FederalNewsRadio.com distributes government-to-government and business-to-government news and information worldwide.

wtop | 103.5 FM WTOP.COM

About WTOP

WTOP is the news leader in the Nation's Capital. In Washington, that also makes us the community service leader, because a radio station can offer no greater service than to provide accurate news and information 24 hours a day. With commuter times leading the country, our WTOP "traffic every 10 minutes on the 8's" is invaluable to listeners.

We are the news source for Washingtonians, whether it's severe weather information, the latest on international developments, or useful, everyday information such as sports and business news.

In addition, we make it possible for any citizen to ask questions of elected officials and community leaders through our WTOP award-winning programs such as "Ask the Mayor," "Ask the Governor," and "Ask the Chief." Our consumer advocacy program, "Call for Action," offers opportunities for those who have been wronged to share their experiences and seek resolution.

In addition, we sponsor many community events each year — from the Marine Corps Marathon, to the Race for the Cure, to providing free flu shots and stroke screenings.

With these and many more WTOP outreach efforts, we serve the community more than 24 hours a day.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com

Centrify
ZERO TRUST PRIVILEGE