

Reducing the Risk Surface

A Holistic Approach to Security

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 (IaaS).

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, Centrify'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.

"As a result, data breaches continued for a long time and it culminated in the summer of 2015 with the OPM breach," Cranley said. "And in actuality the breach had been going on for several years."

Following this initiative, was 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 what 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.”

“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.

Continuous Diagnostics and Mitigation

Cranley said the top challenge as it relates to CDM is what feels like additional compliance or governance regulations. “You talk to 10 agencies, you get 10 answers,” he said. He also noted there has been a concerted effort to understand the regulations through focus groups attended by industry, Blanket Purchase Agreement holders, and government. Ultimately, understanding CDM is a “big, big, big endeavor” where things likely won’t get accomplished in short order.

CDM regulation is now into OSI levels 3, 4 and 5 which includes the actual access control. This is where Centrify can help — particularly in functional areas 8 and 9. “We actually address very completely the authentication and authorization requirements as required by the CDM Phase request,” according to Cranley.

“Because Centrify works across the entire attack surface, we provide the ability for people to take that one identity, which is in Active Directory, provide the ability to access that identity through multi-factor authentication like a PIV card, CAC card, smartcard, derived credential, whatever it is, and then when you get there we can clearly define in a very granular manner exactly what privileges people have.”

The capability can go so far as to say on what days and time ranges someone can have access to specific resources. It can be very certain and precise on the actual access and authorization that’s provided. “There’s no other organization that does it better,” Cranley said. “This is what we do. Centrify’s dedication is proving out that we are the de-facto standard when it comes to Zero Trust Privilege.”

As for what lies ahead, Cranley says CDM is currently in Phase 2 with an eye toward mobility in the future. “Because of the cloud-first initiative for the government, they will come out with a Phase 3 that’s probably going to be a little bit more focused on cloud,”

he said. “Maybe the infrastructure-as-a-service because a lot of people are moving to that where they ‘buy compute’ as opposed to buying servers and building up square footage.”

Identity as a Perimeter

The security perimeter used to be the firewall, but now it’s the user’s identity. “A lot of organizations still spend a lot of time and effort fortifying their firewall, which is good; you need to do that,” according to Cranley. However, now privileged users include everybody, not just a select few, and those people work with different devices, many of which are mobile, and are “out” of the building as Cranley said “and not behind the firewall.”

Companies have studied this and Cranley said concluded that 100% of all data breaches are because of compromised identities. “Identity is the perimeter,” he said. “That identity is going to provide access to a lot of assets within your organization that are valuable.”

And it’s not limited to people who are solely focused on the most sensitive information. “Once I get in, and I get behind the firewall, I get through the VPN...you can get access to everything if you a good hacker,” Cranley said. “And if you’re a savvy hacker, you’ll figure your way around the place pretty quickly.”

There are many third parties, researchers and other groups that do business with the government and have access. For example, “CMS has people that audit their (Medicaid) claims, and there are hundreds and hundreds of groups from across the country that go into CMS and pull people’s healthcare information out,” Cranley said. “If a bad guy gets a hold of those identities, then it’s a free for all.”

Centrify’s solution provides an auditing capability that does three things:

1. Catch those looking to steal information or do harm;
2. Serve as a great training tool;
3. The ability to review the privileges people in a specific role hold by auditing their sessions for two weeks and review the commands they utilized during their session through data analysis system. The actual use of commands will allow you to determine what privileges workers use on a regular basis and what they didn’t use.

Cranley said as long as everyone can do their jobs and not feel curtailed, Centrify can right-size the role to the privileges they need, which leads to better security and compliance.

Following a “People, Assets, and Rules” philosophy, Cranley said it’s important to provide people with the access they need, but only what they need. Knowing that the identity is the perimeter and eliminating the password in favor of a credential or a right in the associates profile lends itself to more productivity. That also allows organizations to assign one identity to each person, rather than multiple identities per person and expanding the risk surface.

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 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:



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.



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.

Our mission is to stop the leading cause of breaches – privileged access abuse. Centrifly empowers our customers with a cloud-ready Zero Trust Privilege approach to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise attack surfaces. To learn more, visit www.centrifly.com.

Centrifly is a registered trademark of Centrifly Corporation. Other trademarks mentioned herein are the property of their respective owners.

©2019 Centrifly Corporation. All Rights Reserved.

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@centrifly.com



www.centrifly.com