Reducing the Risk Surface

A Holistic Approach to Security Part III

Too many users, too many passwords, too much access! These are the issues many in the IT security world are facing, 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 resulting in too many passwords.

WTOP and Federal News Radio have partnered with Centrify to create this industry briefing to explore deeper the following concepts: big data, federal mobile standards and Cloud computing.

Joining the discussion will be Greg Cranley, Centrify's senior director of federal sales. Cranley will offer context as well as Centrify's solutions to these complex issues.

Big Data

With the big data market expected to grow to more than $50 billion by 2020, there are plenty of opportunities and challenges. There are also key elements organizations must pay attention to. To explain, Cranley established the concept of shadow IT, which he described as people who are not in the IT department, but who are data scientists. They have a clear understanding on how the data should be manipulated and what the key points are that need to be put into that data so that the right information can be extracted.

They're responsible for showing the actual users how to leverage the data, what to do with it and where to put it.

"They see the value in putting all of this data together in a very searchable, findable way to leverage that data for the betterment of the organization," according to Cranley. "However, being shadow IT, they often run the risk of not doing the primary things that you need to do to ensure security and to ensure that the architecture is correct and things follow the right order."

As it relates to opportunities, Cranley sees several, particularly in government.

"On the government side, we interact as citizens with the government so often: tax; Social Security; we have an overwhelming number of veterans that are in the system, Veterans Affairs; CMS, Medicaid, Medicare, Treasury, the Postal Service," Cranley said. "So if they can take the data and know for good reasons where people are positioned, where they are in life, what would be beneficial to them, what things the government could bring to them because they fit a certain demographic or they're in a socioeconomic position, they could be educated more. Instead of knowing how to get that benefit from the government, it gets pushed a little more naturally."

But challenges remain, particularly by increasing the risk surface. "You're going to be gathering in one spot all this very valuable information," Cranley said. "It's going to be leveraged for the good of the organization but that can always be turned around. If stolen or compromised, it can be turned around for the bad of the organization and then you have a data breach.

> "The elimination of user IDs and passwords and replacing them with smartcards and multi-factor authentication reduces the risk surface significantly."

"So it's important that they get security in place initially so that they are not behind the eight ball and then have something that never gets out of testing and never gets into production because it is not secure. And then there's a lot of cycles and money spent re-architecting the system with the right security measures."

Cranley added it's important to get security right from the beginning and tie all access back to the individual. "Anonymous users are no good," he said. "Being the root password or the super user or your local administrator has been the cause of many breaches and lacks the security of controlled access. The elimination of user IDs and passwords and replacing them with

smartcards and multi-factor authentication reduces the risk surface significantly. Full uncontrolled access like root or local administrator is extremely dangerous."

The Centrify solution can help eliminate the identity-related risks as companies and government agencies develop and refine their big data strategies.

"The concept is, we leverage one single data storage for identities," according to Cranley. "We find that 99.99% of every organization we work with has active directory. It's the best LDAP you can have. It utilizes very standard yet key protocols like group policies and Kerberos ticketing. Through our software we can extend that to everything, even if it's not a Windows asset, and make it look like a Windows asset. The desired result is to have three datasets in the active directory — all people, all the assets/resources and all the rules. An organization can then group the rules together to create roles, assign people to those roles and assign those roles to resources. The result would be the ability to provide granular access rights to certain people on certain resources."

Cranley concluded by explaining that access rules would be given to each user in the organization that specifically match the user needs based on their role.

"And by using the Centrify software we'd have the correct access to resources resource's such as cloud and on premise applications, servers of every type in the data center or in the cloud, Hadoop platforms — even the Windows machines to provide access rules much more granular than Local Administrator, all controlled by Active Directory. " he said. "So having the assets, people and rules in one identity store allows the organization take the rules and create, and group the rules in sets that represent roles. So administrative Level 2 would have these 25 privileges they could use. These are the rules. So that becomes a role. And then all I have to do is take all the people that I want to be administrative Level 2s and assign them to that role. And then I take that role and assign it to the right machines that they would work on."

Federal Mobile Standards

The use of mobile devices in government continues to rise and that only figures to increase in the years ahead. But questions remain about who's device should be used — the individual or the agency — and how much privacy can be expected. Security also plays a large role in the conversation.

"Mobility, it's kind of in an odd position," Cranley said. "There's a lot of discussion on federal equipment being pushed out there or do we want to use our own devices and have a Bring Your Own Device policy (BYOD). So there's a yin and a yang between the associates and the administration thinking, 'if I bring my own device, then you're going to be able to look at what I'm doing and I don't want any part of that.' And the agency is concerned about cost and security 'but we don't want to go out and buy phones for $400 for everybody and then have to pay the bill but we want to ensure security.'"

Cranley goes on to address the actual security piece. "So NIST has gone to great lengths and have written some BYOD security requirements but unfortunately they can't keep pace with the versions of the phones that come out," he said. "Android and Apple are doing a great job and Windows is doing a good job of keeping the versions rolling. And every time they do that it's like, 'wait a second, we have to evaluate that phone.' So to be able to get a catch all requirement set that they can judge against is a moving target and difficult."

Physical security also has a place in the discussion, as it's become commonplace for people to misplace phones or even have them stolen. Cranley addressed that in the context of application security and the concept of containerization.

"A secured container makes it better," Cranley said. "But you need to have a way to access that phone that's not a PIN or my user ID/password. The same thing about me wanting to go to Office 365. If I'm a user, I can't be logging in with my thumbs trying to get into any number of apps like Office 365 on my iPhone. That would just drive you crazy. People wouldn't use the apps as and that makes the investment in those apps a waste. Not using apps takes away from the productivity that these applications are supposed to provide.

"So the key is to give both the user and agency what they desire. Make it easy to use for the end user with confidence that the agency isn't looking at their personal data, make secure enough for the agency with a credential that is derived from their PIV or CAC card. The ability to gain access to your phone and the apps on that device then use a digital representation of the user to gain access to the app wherever it's located would appease everyone. Single sign-on, using that credential makes the user happy. The organization is happy because it's a derived credential; it comes off their PIV or CAC card. You can also have additional authentication pieces where you can get phone calls or texts or e mails on other devices to ensure you are who you say you are. The thinking is, 'if these two things are together, that's a security probability.' You can lose your phone but the chance of you losing two or three devices is not likely. So as long as they're together, and we do things like geo-spacing, if we get a request from a phone in California but their iPad is in New York, somethings wrong. So you don't grant access."

"So the key is to give both the user and agency what they desire.

Single sign-on, using that credential makes the user happy."

Despite questions about device management, ownership and security, the benefits are clear. There are countless easy-to-use applications designed to increase productivity and also tie into the Cloud First initiative.

But tying everything back to identity-as-the-perimeter concept is enough to do what you can to secure that device and the access. Cranley worries about mobility access. Who has access to what and how much?

"They become super users because now I have access to applications that has government data," he said. "That I'm anywhere I can be because the perimeter is where anybody's identity is. It's not behind a firewall anymore. And to that end, if I'm going to allow you to do that, I have to have a security policy on it. And then what does the government say, what does NIST say the security policy is and how serious do I take it or am I just looking to be compliant?"

The Centrify solution is uniquely positioned to answer these questions, Cranley believes.

"We've worked out a way use CAC/PIV credentials to access applications on mobile devices called derived credentials," he said. "It is exactly what it says. They are credentials and derived from a certificate that they already have, from a certificate authority they already have, which can be the same one that they have tied to them on their PIV or CAC card.

"That credential is an electronic or digital representation of their CAC/PIV card is because nobody's going to put a card reader on their iPhone or their iPad. The form factor doesn't work. It doesn't go well with it.

"So the derived credential is what NIST is looking to do in regards to mobile device use for federal employees. They have standards out for mobile device use but because of the technologies in the phone and their ability to do some of the things that they weren't able to do in the past, now they have to get rid of some requirements that don't apply any longer."

Cranley says the federal government is still at the drawing board when it comes to standards around mobility.

"I think that the GSA is working hard on trying to work with NIST to come up with standards and requirement for mobile use." he said. "There are some very good mobile experts out there that GSA is utilizing, that we're working with to ensure Centrify's capabilities match what is needed from a standards and ease of use. They are looking at our derived credential design now that could work for what they are going to do, for how they would do derived credentials and what they would derive.

"It's fairly technical but, once I get the certificate on the phone, how do I hide it? If I was going to steal your phone and if I was able to unlock it, if I could get that credential, how is it embedded in the phone so that nobody can see it and then how is that leveraged at the same time when I want to use that to go out to Office 365 or some other application that's going to be looking for my identity and needing that representation of me?

"There's a lot of work being done. There's a lot of discussion on the use of mobile and how the promises of the great advantages smart device offer and still remain secure. There's a desire because the Cloud First initiative is exactly that. It's the use of applications, rented compute capability for cost savings and productivity. And where do you use applications the most? You use them on your desktop but you also want to use them on your mobile device."

Cranley acknowledged people would prefer having only one device for business and personal use, but want assurances that those activities can be separated on the device.

"There's got to be a way to demonstrate to the users that we can separate business from personal applications and use, that big brother is not going to be watching their personal stuff, that they can carry one device," Cranley said. "Because even carrying two devices, it's not only expensive but it's a hassle. Another thing you have to keep track of is the passwords for each.

"So I think if we can leverage the CAC/PIV card and the credential and containerization on these devices for the business side and demonstrate that to the user, provide them a little bit more self service like being able to lock their own phone, reset their own phone, kill their own phone in case they lose it without having to call anybody, that's a productivity saver.

"And if the government doesn't have to go out and buy equipment, then that's a big savings as well. And then everybody can have the phone that they like. And if they separate, they can always keep their number. And once they get out of the application that Centrify provides, nothing changes on their personal side. All of their pictures are there, all of their music is there, and their personal e mail is there, everything."

Ultimately, Cranley believes standards around security are essential to making mobility work in the federal government.

"I think you need to figure out a way that you're going to have a standard security policy, that the phone can't be opened without using some type of credential," according to Cranley. "If you're a commercially based company and you want to use a four digit thing, that's fine. If you want to use an RSA token, if you want to use a UBI key, which has become very prevalent in the commercial space.

"In fact, Centrify will be using them as well. Everybody typically has a certificate of authority of some sort in their organization that they can leverage to tie identities to and tie it back to the active directory that this UBI key credential belongs to this person.

"The other thing is, when you're doing applications, you want to have a way where you can provide people rights to access. You want to leverage technology. You want to leverage things like SAML tokening or things of that nature.

"You also want to make sure that your information as an organization stays behind your firewall or the protected assets you rent, that there's only one identity. No directory synchronization of your active directory or identity stores. There's no replication of your users identity into somebody else's Cloud infrastructure. Everything is seamless. That one architecture is leveraged not having to use one tool to do Cloud applications and then another tool to do on premise applications and yet a third tool to do applications because there's always going to be a mix of solutions to get the job done.

"You also want to make sure that your information as an organization stays behind your firewall or the protected assets you rent, that there's only one identity."

"And the user, quite frankly, doesn't care where solutions resides. What they really don't want is the need for multiple user ID/password to get to their work tools. They want to click on a ICON that represents that application. They want to get authenticated by whatever single identity an organization decides. And then they want to get logged in and do their job

"So I think using known technologies like SAML tokening and things of that nature will provide that security. And, again, when you're just granting rights to people and not giving them user ID passwords, you reduce your risk surface tremendously. And by reducing your risk surface tremendously, your security posture goes up significantly.

"Abuse also goes down. If I don't know the user ID password, I can't share it with you. I can't lose it. And I can't have it stolen."

Cloud

Cranley noted two key Cloud components: renting computing power rather than owning servers and hardware, and then the applications that live in the cloud represent great opportunities.

"Since we don't have any infrastructure or we're going to minimize infrastructure, why do I want to worry about customizing software?" he said. "Why do I want to worry about making it when I can have a service provider give me the functionality of the software that I need, get my requirement, and make it so? And then I just pay for it as I use it.

"Both of them represent that we're going to be putting our data in the Cloud, which the federal government is usually resistant to," Cranley said. "So that becomes a stumbling block. The organizations have all tried very hard to explain the security piece of it. And I think that while there's reasonable amounts of effort put on the security piece, I think some of the architecture, some of the applications — typically you buy people accounts on Salesforce or BOX, they're going to get a user ID/password and you're going to have it, your company's going to have it, and the application owner will have it. And they will have a little data store in the Cloud with that information. So, again, we going to run the risk of increasing the risk surface greatly by now having all of these applications and account, which makes everyone a super users. Because now they have access tall these applications and systems, like citizen data or financial data, mission data, etc."

Centrify's solution has taken some of the concepts used on the data center side and incorporated them into application management in the Cloud. "We can grant rights and not hand out user ID/passwords," Cranley said. "We can also get away from things like directory synchronization where they're going to have to take their active directory and synchronize it into the Cloud.

"Centrify's solution has taken some of the concepts used on the data center side and incorporated them into application management in the Cloud."

"Everybody keeps their data inside. We use technology to send representations of people's credentials based on the fact that we've checked in real-time that they're still a member in that group and that they are allowed access to that application.

"There's nothing to hack. There's nothing to steal. It's a very secure way of passing that credential and that identity information."

Cranley also detailed the evolution of companies renting services instead of purchasing servers and data centers. He says this concept takes away a lot of the maintenance and gives users the opportunity to have the most up-to-date technology.

"You get the best versions. You get all the bugs out of it and people get to use it and I'm only going to pay for what I use," he added.

From a security perspective, Cranley says Centrify has it covered as well.

"Based on our Cloud brokerage we have a very secure Cloud connector that allows you to get rid of VPNs and it allows users on the outside to come through that Cloud connector, which is not a proxy, not a VPN," according to Cranley. "It's a direct connection back to the resource you want to get to that can be behind your firewall or in the cloud".

"When you're on the outside, on your iPad, your iPhone, or your laptop and you want to get to Office 365, you'll be able to make that request and that request goes through the agency's tenet in our cloud, which basically is a traffic cop, identifies the fact that, oh, you're from NOAA.gov for example and sends it down through that Cloud connector, it goes directly behind your firewall at NOAA.gov, goes to the certificate authority, takes the request, goes to active directory and says: Is Greg still a member of this organization and can he get access to Office 365?

"When a user requests access to a resource and your still active and in the active directory the organization can grant rights assigned to me and others in my same position. Basically, once a request is made to gain access an electronic certificate, a token, some type of digital representation of my rights and it will pass it directly to Office 365 to where NOAA email resides and it will look at it and say: That's Greg; let him into his mailbox. So we're leveraging their active directory inside. We don't have to leverage a second or replicated directory stored elsewhere."

"I think having a holistic approach to it where you can leverage existing technologies like active directory, group policies; that will lead you to the best success you can have very quickly."

Cranley ultimately sees Cloud, particularly in government, as a great opportunity for cost savings and productivity.

"I think the government has it right that it can be extremely productive and cost effective," he said. "I think organizations need to look for a holistic solution instead of spot tools to ensure that they're buying few fewer tools, get the best breed as opposed to having a bunch of stove pipes because it just keeps adding to the frustration.

"I think having a holistic approach to it where you can leverage existing technologies like active directory, group policies; that will lead you to the best success you can have very quickly."

Shared Account Password Management

In a response to the OPM breach and Federal CIO Tony Scott's 30-day cyber sprint, many agencies invested in a Shared Account Password Management (SAPM) solution to manage their privileged users. Unfortunately, this does not meet HSPD-12 and multi-factor authentication requirements and CDM authentication and credential requirements.

SAPM solutions only cover 5% to 10% of the problem. The need for a true Super User Privileged Management (SUPM) tool is the only way to ensure everyone in the organization is using a smart card (CAC/PIV) and a PIN plus a third level of authentication to access all resources.

SAPM tools are used by a select few on a select number of assets. This leaves the majority of the organization's associates and assets open to a breach. This is very dangerous since every organization has a diverse number of heterogeneous resources that the entire organization uses to accomplish the mission. The result is risky behavior that has led to the breaches seen in the past.

This is where a single architecture platform that leverages a single already existing repository of roles to access every resource in the organization will increase productivity. It will do so in the most secure, compliant manner using multi-factor authentication everywhere in a cost effective manner.

In order for an organization to achieve true accountability of who is accessing what resources, the agency associates must access those resources themselves, not as "admin" or root. In today's environment anonymous access increases an agency's risk surface tremendously. Having the ability to leverage a SUPM solution using a PIV or CAC card and a PIN plus a third factor of authentication to support HSPD-12, multi-factor authentication everywhere and CDM authentication and credential requirement will meet the mark. Employing just a SAPM tool will not suffice. It's essential for federal government leaders to understand and implement this.

Having 5% of an agency's associates leveraging a root password vault solution to check out passwords is not enough to protect their risk surface area. Government leaders must embrace the need to ensure all agency associates leverage their PIV or CAC card, a PIN to employ a "something you have and something you know" access process coupled with a third method of authentication to assure they are who they say they are. This will reduce the cyber data breach threat that has cost millions of dollars and threatened the security of millions of people.

It's time to dismiss the myth that Shared Account Password Management solutions are the answer to our cyber security problems.

Conclusion

Ultimately organizations must take the time to look for a holistic solution that's going to cover their entire problem. They must use 2016 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, your cloud and cloud applications, and your mobile devices, 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 RADIO.COM 1500 AM

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.

Centrify

Centrify strengthens enterprise security by securing identities from cyberthreats. Centrify uniquely unifies identity for privileged and end users across cloud, mobile and data center. Centrify improves security, compliance, agility and productivity for over 5000 customers, including over half of the Fortune 50 and over 80 federal agencies. www.centrify.com.

SANTA CLARA, CALIFORNIA	+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
EMAIL	sales@centrify.com
WEB	www.centrify.com