Conversational

Next Gen Access: Mobile Management and Trusted Endpoints

A ConversationalGeek® Book

Sponsored by Centrify® ZERO TRUST SECURITY

Learn about:

- Establish a system of trust and management for mobile devices and applications
- Use device identity for access control purposes.

MINI Edition

By Brien Posey
(Microsoft MVP, Commercial Scientist-Astronaut Candidate)

Sponsored by Centrify

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a-Service (IDaaS), Enterprise Mobility Management (EMM) and Privileged Access Management (PAM). Over 5,000 organizations worldwide, including more than half of the Fortune 100, trust Centrify to proactively secure their businesses.

www.centrify.com

Conversational Next Gen Access: Mobile Management and Trusted Endpoints (Mini Edition)

by Brien M. Posey

ConversationalGeek

Conversational Next Gen Access: Mobile Management and Trusted Endpoints (Mini Edition)

Published by Conversational Geek Inc.
www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Brien M. Posey
Project Editor:	Emily Downs
Copy Editor:	Steven Zimmerman
Content Reviewer:	J. Peter Bruzzese

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books, both through cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

Ensuring Trusted Devices

Nearly a decade ago, the so-called Bring Your Own Device revolution began to take hold. Prior to that, access to corporate networks was almost exclusively confined to domain-joined, tightly controlled PCs. However, the proliferation of consumer electronic devices such as tablets (most notably the iPad) and smartphones made it nearly impossible for IT pros to ignore the demands, made by users and executives alike, to use personal devices for work.

As users reveled in their newfound freedom to work from whatever fancy new device happened to be cool at the moment (perhaps occasionally even using "but I need it for work" as an excuse to buy such a device), IT pros found themselves having to answer a difficult question; *how can you secure a device that you neither own nor control?*

Initial efforts at securing mobile devices centered around things like securing VPN access or applying ActiveSync policies to the devices. Ultimately, however, such efforts were inadequate. Perhaps more importantly, these efforts resulted in the creation of management and security siloes.

The "per-device type" security model is unsustainable. There are simply too many different device types and operating systems out there. This approach to security just does not scale. Besides, taking a siloed approach to security overlooks the most fundamental aspect of security – *trust*.

The bottom line is that, in almost any organization, there will be a mixture of company-owned and user-owned devices, and desktop and mobile operating

systems. Furthermore, the list of devices used to access corporate resources is anything but static.

According to some studies, the average person owns four devices (https://bit.ly/2oLj7Bj), and new devices are being introduced all the time. As such, the best way to secure all of these devices isn't to try to understand the configuration nuances of every conceivable device type, but rather to establish trust. After all, if a device is going to be used to access confidential corporate resources, then the device needs to be proven to be trustworthy before that access is granted.

Devices are gateways to company data and resources, *but how do you know if they can be trusted?* According to the latest Verizon DBIR, "95% of phishing attacks that led to a breach were followed by some form of malware installation." – Verizon DBIR 2017

I'm not trying to say that device-level security is unimportant; devices have to be secured. It's just that device-level security alone isn't enough. It's better to follow the long-standing best practice of defense in depth.

Device and Application Management

If an organization is to secure the devices that are being used by its users, then it is necessary to begin by understanding the risks that are posed by those devices. On the surface, this probably seems like a daunting task. After all, there are potentially thousands of different factors that could result in a security vulnerability. Even so, the vast majority of security breaches can be grouped into some really basic categories, such as privilege and ID. While it may be tempting to think of the concepts of privilege and ID as pertaining exclusively to user accounts, these same concepts can also be applied to devices.

If an organization truly wants to enforce secure access, then it must have a means of determining whether an endpoint should be trusted. The first step in doing so is being able to positively identify each individual device through the use of certificates. Once devices are registered in this way, then it becomes possible to ensure that access requests are coming from known devices.

It's important to remember that an organization likely supports a variety of device types, including Windows, Macs, and other devices. Although non-Windows devices cannot be natively joined to the Active Directory, a good device management platform should ideally be able to *bridge* non-Windows machines to the Active Directory.

Of course, device and application management is about more than just being able to identify devices. The device identification should be able to be used as a means for establishing access control. An IT pro might, for example, group certain devices together and create a policy stating that only the devices within a specific group will be able to access a particular resource or application.

Another key step in the process is to create a policy that defines what it means for a device to be secure. Such a policy can be enforced by using hundreds of individual security settings that can be fine-tuned to meet the organization's specific needs. When a user onboards a new device, an identity can be established for the device automatically, and any applicable security settings can then be applied to the device, as defined by the policy.

Perhaps the most important reason behind establishing device identity is that doing so makes it possible to create conditional access policies that are based not only on the user's rights, but also on the identity of the device. For example, if a user is attempting to access data that is subject to GDPR, then access should only be allowed if the user is working from a trusted device that is known to be secure.

The bottom line is that it is no longer sufficient for an organization to focus most of its security efforts around protecting user accounts. If an organization is to truly achieve zero-trust security, then devices must be identified and secured. Furthermore, resource or application access requests should only

be approved if the device's identity can be validated, and if existing policies allow access from the device.

Device Context and Security Posture

Now that both the devices and the apps are identified and managed, and the proper controls are in place, the next part of verifying the device is to dynamically and automatically assess the security posture of the device for each access request. Here, assessment includes understanding if the device is actively managed, as well as the current security risks and security posture state. These context feeds can come from Centrify and other endpoint security providers.

Checking the security posture state could mean:

- Does the endpoint have a password (i.e. min of 8 characters)
- Does the device lock after 5 min of inactivity?
- Does it have the latest AV or Wi-Fi Settings?
- Can you enforce passcode on a mobile phone?

These are ways that you can understand if a device is in a "healthy/trusted" security posture and, based on this information, create a combination of policies that define the circumstances to grant access based on identity assurance and device posture.

Endpoint Privilege Management

In the world of IT, privilege can mean a lot of different things. If we are talking about devices though, then privilege can be roughly defined as the things that a user is allowed to do on the device. Someone who has full-blown Root or Admin privileges on a device, for example, can do pretty much anything that they want to the device, while someone who has been assigned a restrictive set of privileges might be able to use the device but might not be able to interact with certain parts of the device's operating system. *So why is this important?* Well, there are several reasons, but let me give you a couple of examples.

If you were to ask the average person, *who is not an IT pro*, what the most pressing threat to IT security is today, they would probably tell you that it is ransomware. Even though ransomware remains a

huge threat to security, there are limits to the damage that it can do. This holds true for almost every type of malware that is out there. The reason why these limits exist is that the malware is bound by the privileges that have been extended to the user who was unfortunate enough to have contracted the infection. Hence, if the user has unlimited privileges, then the malware *also* has unlimited privileges. On the flip side, if the user has very few privileges, then the malware will also have few privileges and won't be able to do nearly as much damage as might be possible if it had unrestricted access to the entire system.

Ransomware has gotten a huge amount of attention over the last few years, both in news stories, and in late night TV commercials for cut-rate PC security products. Even though a lot of people do not seem to really understand what ransomware is, almost everyone has at least heard of it and perceives it to be one of the most pressing threats to the security of their data.

Malware prevention is not the only reason why it is so important to examine end user privilege. After all, you also don't want end users to be able to do anything that will compromise the security or the

stability of the operating system. Once again, let me give you an example.

Suppose, for a moment, that a user has been issued a laptop that they use in the office, at home, and while traveling. Because the laptop is used outside of work, there are certain configuration tasks that the user needs to be able to perform. At the very least, for example, the user would need to be able to connect the laptop to the Wi-Fi network in their home. They would probably also need to be able to connect the laptop to a printer, or perhaps to a Miracast-enabled display.

At the same time, there are certain configuration changes that the user *should not* be allowed to make. You probably would not want the user to be able to disable the Windows firewall, change the User Account Control settings, or install an application that the user downloaded from the Internet. Privileges allow you to define the scope of things that a user is and is not allowed to do.

Back in the early 90s, I worked as a network administrator for a large company. At the time, there really wasn't a good way to restrict a user's permissions on a PC. As such, users could do almost anything that they wanted. Most of the helpdesk calls that the organization received were due to a user either changing settings or installing unauthorized software. In other words, there was a direct relationship between privilege (or lack thereof) and helpdesk costs.

IT pros are often conditioned to think of privilege as something that is assigned to users, but it is also possible to dynamically assign privileges based on the endpoint device that a user is working from. To do this, a couple of things must happen.

First, you have to be able to positively identify the device. This is usually accomplished through a device enrollment process in which the user authenticates themselves into an enrollment portal, accepts the device usage terms, and then has the device provisioned for corporate use. This provisioning process typically installs a certificate onto the device, allowing it to be identified.

Then, even after a device has been positively identified, the system has to determine whether it

should extend any sort of privileges to the device. There are many ways of doing this, but typically the decision comes down to evaluating the device's health. In other words, does the device comply with the organization's basic security requirements? Does the device require a password? Has the operating system been jailbroken? There are many security factors that can be considered.

The important thing is to take a zero-trust approach to device management. Just because a user is connecting to the network using a good set of credentials and a known device does not automatically mean that they should be fully trusted. *How do you know that the device wasn't stolen?*

From a security standpoint, it is far more effective to base the assignment of privileges not just on user and device identification, but also on behavior-based analytics, where the user is never automatically given any privileges whatsoever. When the user attempts a privileged operation, the system uses a machine learning algorithm to determine if the operation is normal behavior for the user. If it is, and the user is operating from a known, healthy device,

then the system may extend the required privileges to the user, but for a very limited period of time. If the user's behavior is determined, by the system, to be abnormal or risky, then the system may challenge the user to reauthenticate in an effort to confirm the user's identity.

The Big Takeaways

Device management poses a huge challenge to the security of our organizations because of the sheer number and variety of devices that are in use. Even so, it *is possible* to use those devices to our advantage and treat the device itself as a second authentication factor. Furthermore, user access can be limited if such a device is found to violate any of the organization's security requirements. The trick to making it all work is to find a solution that provides unified device identification regardless of device type (PC, Mac, mobile, etc.) and ties the device identity to a zero-trust identity management system.

To accomplish this, it is necessary to validate every device using a mobile device management system; that way, you can enforce security policies in a way that ensures that only trusted devices are allowed access to resources. One way to accomplish this is by leveraging certificates on the device to positively identify the device.

The zero-trust approach to device management also requires ensuring that apps are managed and locked

down appropriately for the user on that device. Apps should be installed on an as-needed basis, rather than simply being installed by default. When a user's access is removed because of a role change, or because of a departure from the company, those applications and data can be automatically uninstalled from the device.

Additionally, access to company data should be limited by policy rules that define the circumstances under which the user and the device are allowed to use the data.

Finally, endpoint privilege management should ultimately give you more confidence about the applications that are being installed on the validated endpoint. The IT department needs to be able to push trusted applications to the device and, at the same time, the user's privileges need to be limited to avoid allowing the user to install potentially malicious apps that may pose a threat to the organization.

NOTES

NOTES

More and more employees are working remotely these days, but how do you keep your network safe if you aren't sure they are who they say they are. In this book I will discuss critical considerations to successfully manage those mobile endpoints and users.

About Brien Posey

Brien Posey is currently in his 4th year of training as a commercial Scientist-Astronaut Candidate, and is preparing for a mission to study polar mesospheric clouds from space. In addition, Posey is a 17 time Microsoft MVP and an internationally published author and conference speaker, with over two decades of information technology experience. You can learn more about Posey's spaceflight training by visiting his Website at www.BrienPosey.com/space.

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.