Conversational
Next-Gen Access

A ConversationalGeek® Book

Sponsored by Centrify® ZERO TRUST SECURITY

Learn about:

- **Why traditional security is missing the mark**
- **How a Zero Trust approach improves organizational security**
- **The use of Next-Gen Access to power Zero Trust Security**

By Nick Cavalancia (Microsoft MVP and CEO of Conversational Geek)

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 behaviour 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 worldwide organizations, including over half the Fortune 100, trust Centrify to proactively secure their businesses.

www.centrify.com

Conversational Next-Gen Access

By Nick Cavalancia

ConversationalGeek®

Conversational Next-Gen Access

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 www.conversationalgeek.com

Publisher Acknowledgments

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

Author:	Nick Cavalancia
Project Editor:	Emily Downs
Copy Editor:	Pete Roythorne
Content Reviewer:	J. Peter Bruzzese

Note from the Author

Access has always been about getting the right user and the right resources connected. It's an idea that hasn't changed in years. The most we've really done with it is applied Least Privilege to it. But the concept of Next-Gen Access takes the basic concepts behind access (that is, the user and the resource), and takes a cold, hard look at what you're *really* trying to accomplish in *today's* world.

Ten years ago, giving someone permanent rights to a resource was fine. Today, we've got external attackers, hackers, data breaches, and more to worry about. *Today*, old school Access just won't cut it.

So, the question becomes, *what's it going to take to keep the environment secure while providing needed access*?

That is what Next-Gen Access is *all about*. In the coming pages, I'll talk about the next step in security models: *Zero Trust Security,* and take an introductory look at how Next-Gen Access makes it possible.

I hope you'll find it educational, and that it gets you thinking about how to better secure your environment.

Nick Cavalancia

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.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

"Geek in the Mirror" Boxes

We infuse humor into our books through both 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 or gut reaction and analysis, it might just be a sarcastic quip, but these "geek in the mirror" boxes are not to be skipped.

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

Moving from Traditional Security to Next-Gen Access

"Credentials, please."

When thinking about security, you need to plan and implement it by addressing *risk*. So, it makes sense to begin the conversation by asking *what is the organization's greatest risk that security can address?* The answer is clear today – it's *data breaches*.

No other single event has more impact on organizations. Incurred costs, loss of reputation, brand damage, loss in revenue, and more all plague businesses that become headlines due to data breaches. Let's take a look a just how painful a breach can be.

Ponemon estimates the average cost of a data breach is $3.62 Million[1], this includes the costs involved with "help desk

---

[1] Ponemon, *Cost of a Data Breach Report* (2017)

activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services, and regulatory interventions."

The business and its brand also take a hit. Stocks take an average hit of 5% when a breach is announced, 31% of customers discontinue their relationship[2], and 65% of customers lose trust in the business and the security of their personal data[2].

And the pain doesn't stop once the cleanup of a single data breach is complete; if your organization experiences a data breach, there is a 28% chance it will happen again within the next two years![1]

So, the goal for IT is to work towards avoiding and/or stopping breaches *from happening altogether*.

However, with two-thirds of organizations still being impacted by breaches not just once, but an average of *five or more times in the past two years*[3], it's evident that what organizations like yours are doing today simply isn't cutting it. The security placed around access to your most valuable data isn't keeping it from being stolen.

So, what's wrong with your current security strategy?

To get your organization to a place where access is truly secure, I want to propose a few perspectives that you need to buy into.

---

[2] Ponemon, *The Impact of Data Breaches on Reputation and Share Value* (2017)

[3] Forrester, *Stop The Breach: Reduce The Likelihood Of An Attack Through An IAM Maturity Model* (2017)

Traditional Security Isn't Getting It Done

You've spent years building up a structured defense, adding on layers of security in response to changes in attack methods, threat actors, and best practices.

But, we've shifted from a world where the attacker used to be "two guys in a garage" looking for bragging rights, to one where your adversaries are well-organized corporations with revenue targets, quarterly board meetings, and agile development processes. So, methods that may have been viable even a year or two ago are now likely to be somewhat suspect in their viability.

Let's walk through some of the parts of most organizations' security strategies, and see how traditional thinking no longer provides as strong a value:

- Perimeter Security — Network and application firewalls certainly have their place to keep bad traffic out and good traffic in. But the idea of an actual network perimeter no longer exists for most companies (yours included). The use of IoT sensor networks, edge computing, remote employees, and cloud applications have extended your "perimeter" so much that it's now practically non-existent.

- Endpoint Security — Endpoint-based antivirus and antimalware solutions have evolved over the past few years to include cutting-edge machine learning and artificial intelligence. But the bad guys are using evasive techniques more frequently (such as direct memory injection, where malware avoids detection by being loaded directly into memory being used by a known good process). As much as 86% of exploit kits

and payloads used in 2017 used evasive techniques[4] – and are looking for new ways to evade detection in order to fool endpoint security.

- The User — You should always consider the user a part of your defense. If properly trained, they should be able to spot abnormal emails that may be part of a phishing attack. With criminals getting exceedingly good at using leveraging social media, LinkedIn, and sites like data.com, their ability to social engineer a very credible email is at an all-time high.

One of the big reasons that traditional security isn't working is that it's focused on the *outside-in* — the belief that the attacker is trying to get in — and putting protective measures in place to stop that.

While important, the challenge with this thinking it that it doesn't take into account if the threat is already inside. How do you stop an external attacker that has made their way inside and now has a foothold within the organization? And don't forget the 28% of data breaches that are perpetrated by an actual insider5. Your security needs to go well beyond just "keeping the bad guys out" and take into account how to stop the bad guy should they get (or already be) inside.

Identity is the Key to a Successful Attack

Without a set of credentials with access to the data-to-be-breached, there simply won't be a breach. Use of stolen

---

[4] Minerva Labs, *Malware Year-in-Review Report* (2017)

[5] Verizon, *Data Breach Investigations Report* (2018)

credentials is the number one attack method used in successful data breaches[5].

Cybercriminals need to laterally move within your network, leveraging as many sets of credentials as they can to advance from one endpoint to the next. Techniques like retrieving password artifacts from memory stored as hashes, Kerberos tickets, and even clear text passwords are common.

And with nearly half of users sharing (yes, *sharing*) their credentials with a colleague, and almost one-quarter stating a colleague *always* has their credentials[6], the concept of a user protecting their network identity is laughable.

Those last two concepts (the retrieval of password artifacts and the sharing of passwords) should have you worried — it means the bad guys have that much more ammunition to continue their attack. So, if you don't have Identity under control (and, as you'll see, it's more than just having, say, MFA, in place), you're leaving the organization vulnerable.

Security Spend isn't Effective

Gartner predicts that 2018 worldwide IT spend on security will reach a staggering $96 Billion[7]. Most (a little over 90%) of the spend is found in three areas:

- Security Services
- Network Security Hardware
- Infrastructure Protection

---

[6] IS Decisions, *Insider Threat Manifesto*

[7] Gartner, "Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017"

While pretty broad categories, you can make some assumptions around what's entailed in each and see that this is probably pretty relevant. And yet, in 2018, we're seeing increases in security incidents, malicious and phishing URLs, new exploit malware, and more[8]. With spending overall up around 8% year over year[7], it begs the question *why isn't our security spend having a greater effect?*

You've Tried Least Privilege… and Failed?

Don't get me wrong, the principle of Least Privilege is a fantastic concept — the practice of restricting users, applications, services, etc. to only access the data, applications, and systems they require to perform the desired work. If you've gone through an assessment and implementation of Least Privilege, you know it's serious stuff. But the failure is found in the execution. Organizations establish Least Privilege once and don't have an ongoing means by which to monitor privileged and non-privileged access to ensure it's appropriate (and then make changes if it isn't). To fend off data breaches, Least Privilege needs to be a cultural shift where it's not just about limiting access, but also about making sure the approved user *is the only one using that access*.

Most organizations base Least Privilege solely on the user account being assigned limited permissions and then relying on their identity strategy (be it IAM, MFA, or just Active Directory) to validate who the person is. Remember, the bad guys leverage credentials 81% of the time in data breaches[9]. So, in essence, Least Privilege only limits what an attacker can do with the *current credential*. If the compromised credential already has access to valuable data, so does the attacker. And,

---

[8] McAfee, *Threat Report June (2018)*

[9] Verizon, *Data Breach Investigations Report (2017)*

if it doesn't, the attacker just waits patiently until they can get their hands on another credential with better access.

Another reason the implementation of Least Privilege isn't always effective is that the definition of "privileged" remains too high. Anyone with access to data that is valuable outside the organization should be considered "privileged".

Your Security is Missing the Mark

Add all these perspectives up and you quickly realize that the current way of doing security isn't providing organizations with a level of security that accomplishes the following:

1) Limits access to critical and valuable data;

2) Ensures only appropriate use of credentials;

3) Leverages more security layers than just identity to determine accessibility;

4) Enforces the same levels of security regardless of where the user, their endpoint, the application, or the data resides;

5) Is an efficient use of security budget (read: it actually stops data breaches!)

So, how do you accomplish all this? *With a Zero Trust Security approach.*

Defining Zero Trust Security

There's an old Russian proverb, "trust but verify". It's a simple truth that organizations should take to heart. You trust your employees, but you can't always be certain when someone is accessing valuable data that it's actually them. So, organizations leverage technologies and processes (the simplest being the logon) to verify the user.

The challenge today is that organizations see the "verify" part of the proverb occurring during logon only. Cybercriminals that have installed a remote access trojan (RAT) can perform tasks as the user without needing to interact with the desktop — meaning the "verified" user is now unwittingly part of an attack.

Zero Trust Security takes the concepts of "trust but verify" and Least Privilege and goes a few steps further. To paraphrase the proverb, Zero Trust Security is "*never* trust, *always* verify".

Zero Trust Security is like that guy who mans the passport control booth when you're entering a foreign country. His job is *to not trust anyone.* That guy looks you up and down, asks questions, checks to see if you're lying, etc. all in the name of *verifying* you so you can enter the country.

To better understand Zero Trust Security, let me cover three foundational mindsets that outline how you should approach security with zero trust.

Outsiders *and* Insiders are *Both* Untrustworthy

You already don't trust external attackers — their intent is clear, and they have no business on your network. But insiders shouldn't be trusted either. As previously mentioned, insiders are responsible for a material portion of data breaches and in a majority of cases, external actors compromise credentials to essentially make themselves appear like insiders.

So, in reality, to truly be secure, you *can't* implicitly trust either group.

Zero Trust Security Goes Beyond Just the User.

I previously pointed out that one of the mistakes with Least Privilege was that most organizations focus solely on the user. But in many cases, it's not the user that is the indicator of a breach. Take the example of an insider (we'll make them the head of Product Management) who decides to make a copy of some of the organization's intellectual property. They're using the permissions given them, perhaps leveraging their ability to logon from home to commit the theft. In this case, the only indicators of malice here are perhaps the day of the week, the time, and the remote access — the user wasn't an issue.

This is why Zero Trust Security takes the standpoint that *you don't trust anything* on your network… *ever* — that is, until it's verified.

In addition to users, the Zero Trust Security principal of "*never trust, always verify*" applies to endpoints, networks, servers, and applications. Each one needs to be verified before access is granted.

Verification is an On-Going Process

If you want to be able to hold to the "never trust" principle, each and *every* time access is requested, the default is to "verify". Note I didn't say "each time a user logs on", verification is a continual necessity — without it, there is no way to uphold the "never trust" principle.

So, verification should occur at logon, when connecting to another system, when opening an application, when copying data, etc. *Every* time resource access is requested, verification is necessary to maintain Zero Trust Security.

Zero Trust Security: One Goal, Four Actions

Since I've spent the last few pages talking about how important it is for your organization to achieve Zero Trust Security, let's spend a little time covering what it's comprised of in a practical sense. There are four actions that make up Zero Trust Security:

- Verify the User — Use SSO, to minimize the use and transmission of passwords, combined with MFA, to ensure the account's owner is the one utilizing the credentials.

- Validate the Device — Only allow known and trusted endpoints as a means of further verifying the user access is appropriate.

- Limit Access and Privilege — The intent is as much to limit access to resources (i.e., the principle of Least Privilege) as it is to limit lateral movement throughout the network. Also, think of this as more real-time and not "one-time", as is the case with most Least Privilege implementations.

- Learn and Adapt — Profiles for each user need to be built that contain what they do, which devices they use, what actions are taken, and which privileges are used. Because the profile changes over time, the only way to truly attain Zero Trust Security on a continual basis is to layer on artificial intelligence that learns on its own to decide whether an access request is appropriate or not.

To make this possible, IT organizations need to consider the concept of *Next-Gen Access*.

Next-Gen Access Powers Zero Trust Security

Next-Gen Access is a label for embracing a combination of modern access management layers working in concert to control access to resources. Think about the moving parts in the Zero Trust Security model — credentials, devices, access to systems, applications, and data, and the user's behavior once they access a resource. All these elements need to be monitored, managed, and policed — ideally, together.

In practical application, Next-Gen Access combines the use of several technologies — some, of which, you may already have in place — to create a Zero Trust Security environment.

The goal is to leverage all of these with the Zero Trust Security mantra of "never trust, always verify" in mind.

So, let me throw a few solution buzzwords at you so you have a better idea of whether you have some (or all) of the pieces in place:

- Single Sign-On (SSO) — Use this to provide controlled access to resources, systems, and applications.

- Multi-Factor Authentication (MFA) — Use this to ensure the user is who they say they are.

- Enterprise Mobility Management (EMM) — Use this to control mobile devices, securing their authentication to, and connection with, the network environment.

- Privileged Access Management (PAM) — Use this to secure privileged credentials within an encrypted vault, provide policy-based access to resources, and have users log in as themselves, only elevating their privilege level when required.

- User Behavior Analytics (UBA) — Use this to understand normal behavior for every user and identify when inappropriate or abnormal behavior occurs. This can include logon time/day/endpoint, location, application use, resource access, and more.

The goal is to leverage these solutions *in concert* so that you can achieve a few back-end goals:

- Share Relevant Data — Each of the solutions I've mentioned could benefit from details sourced from any one of the other solutions. The sharing of data can have a dramatic effect on the security you are able to provide. For example, if a user wanted access to a privileged account, your PAM solution should know whether the machine the user is on is approved, and whether the user themselves has been verified. Thus, in an ideal Zero Trust Security scenario, your SSO might talk to your PAM to let them know the user has been verified, etc.

So, using solutions that, by default, can leverage each other to make better security decisions *without you* is a step in the right direction towards Zero Trust Security.

- Reduce (or Eliminate) User Friction — Every decision around whether access should be permitted that needs to be made can add seconds of latency, frustrating users. You've experienced this yourself (albeit, perhaps not in the context of security) when you've attempted to visit a website and gave up after waiting even just 5-10 seconds.

  These friction points can exist when data needs to be passed from one solution to another in order to properly (and securely) provide access.

  Take the previous example of the user wanting to use privileged access, if this had to be done manually (by, say, using a manual approval by IT in the middle of the user request), it could take minutes to get the approval.

  Your goal is to provide a Zero Trust Security environment in such a way that there is minimal friction to the user.

- Reduce the burden on IT — the previous example is perfect: IT potentially had to get involved to approve a privileged account request manually. You want to avoid that as much as possible. With nearly every solution, IT is required to write lots of rules to establish policy around what is and isn't allowed. This is time-consuming, and usually requires a bit of expertise. The

end result for most organizations is one person actually understands it all.

Instead look for ways to integrate your solutions so that decision points can be data-driven and, hopefully, automated. Some solutions choose to leverage policies with exceptions, while others use machine learning and artificial intelligence to build profiles and adapt over time.

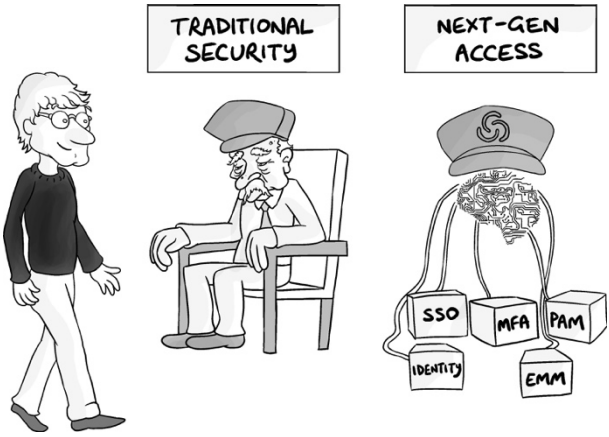
The Big Takeaways

Data breaches have seemingly become part of every organization's reality. *But they don't need to be*. It's the reduced state of security that allows attackers to be successful. Spend on traditional security methods, and the increase in successful external attacks, are only making the case that something needs to change.

The principles of Zero Trust Security reduce the ability for both insiders and external threat actors to make inappropriate use of credentials, devices, applications, and data. By making the access a default "nope", and working up from there, organizations implementing Zero Trust Security provide themselves with several checkpoints along the path to access where malicious actors will be stopped.

Using Next-Gen Access solutions in concert helps to establish and maintain a Zero Trust Security environment. By making SSO, MFA, EMM, PAM, and UBA work toward the same goals (rather than considering them as separate solutions each with a different purpose or for different silos of resources), you can dramatically improve the security of your environment, reducing risk, improving IT efficiency and accuracy, all while keeping users happy.

Vendor Sponsor Chapter — Centrify



Getting to Zero Trust Security's goal of pretty much never trusting anything on your network — and yet still providing access — will require some pretty close orchestration between systems and solutions that manage and provide access to user accounts, devices, and privileges.

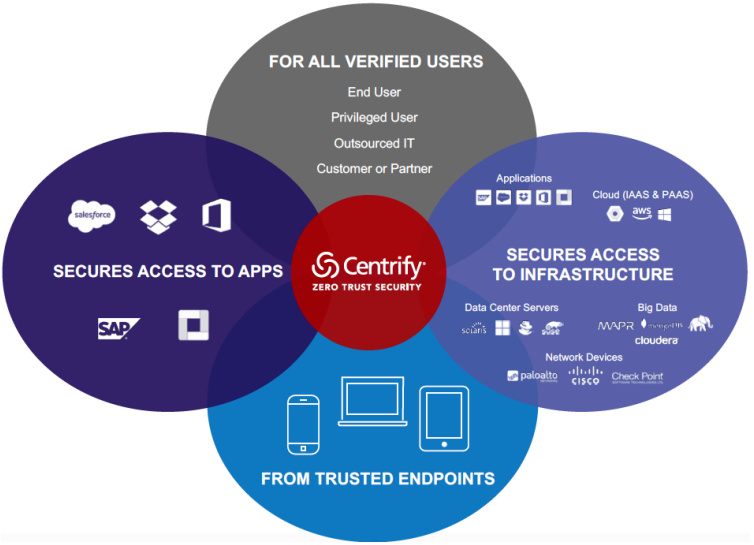
In the last chapter, I mentioned five solution types that together provide Next-Gen Access (SSO, MFA, EMM, PAM, and UBA). But, it's in the specific execution of the involved solutions that a successful implementation is found.

Now, it should be said that no one really *wants* to manage five disparate solutions and somehow configure them to become what *should be* a secure environment, right? If you were to start with a Zero Trust Security approach, providing access with separate solutions would be a complex process. It would involve manually aligning solution-specific policies and configurations in an effort to "define" when a certain user on a particular device, accessing a specific resource, under express conditions is allowed to do so. And you'd need to do this for every possible scenario.

Next-Gen Access sounds like it could be a lot of work.

Centrify Zero Trust Security with Next-Gen Access

Centrify starts with the premise that no users, endpoints, etc. should be allowed to access any of your apps or infrastructure. Their solutions verify every user, validate their endpoint(s), and ensure any access and privileges are limited in scope. They also leverage machine learning to scrutinize the various access request specifics to identify risk and take appropriate action without impacting the user experience.



Centrify's differentiator is the integration between its solutions, enabling them to *work together* in an effort to seamlessly and intelligently implement a Zero Trust Security environment while still providing every needed bit of access.

You'll recall the four actions that make up Zero Trust Security that I mentioned in the last chapter. I'd like to use those as a way to discuss how Centrify achieves Zero Trust Security through Next-Gen Access.

One of the common themes you'll see in the next few pages is how Centrify uses risk to determine access. Every aspect of the interaction between user and environment is measured and recorded, and then used to establish a baseline of "normal" activity for the user. Anything that lies outside this baseline indicates a level of risk that can be used to dynamically allow or deny access.

Verify the User

From logon to access, the best security is one where the access is verified throughout the process, all while the user remains unaware. To achieve Zero Trust Security *without user friction,* Centrify starts by using multi-factor authentication (MFA) to securely verify the user. But MFA on its own lacks ease of access to applications. So Centrify combines it with Single-Sign On (SSO) to seamlessly provide access to applications from a single portal. Log on once with MFA and access everything you need with SSO.

Behind the scenes, Centrify is busy working to determine whether access should be granted using a contextual set of rules (e.g., whether the user is on the corporate network, the request is made during business hours, and the user is on a validated device). Normally, this is a challenge for most organizations — rules are generally complex, scenario specific, and cause IT to always be playing catch-up to keep them up-to-date. Centrify simplifies this by combining access with User Behavior Analytics (UBA). They watch user access requests (and the specific conditions when requests are made) and use machine learning to establish what is "normal" for the user. Any access attempts that deviate from this norm present a certain level of risk. Each attempt is then dynamically

evaluated based on the risk, rather than on a generic set of static conditions.

This risk evaluation would be difficult without fully integrated behavior analytics — too much latency in a loose integration between the MFA/SSO systems and the UBA systems would frustrate users and possibly make it impossible to use in more automated environments where API calls are being used. But Centrify makes these technologies work together to help verify the user in real-time, to minimize latency, and improve the user's experience.

Finally, each attempted or successful access event is automatically fed back into a user profile to update their risk level.

Validate the Device

Security can't be just about verifying the user. If it is, all that's necessary to bypass security is to steal a user's password, spoof the user's phone for MFA, etc. Instead, if we can also only allow those devices we know — for example, a known laptop, identified by a unique certificate, registered to me, in a known state (e.g., not jailbroken, has policies applied, disk encryption, etc.) — to access the network, it's MUCH harder to get passed security.

So, even if an attacker can somehow spoof a user's phone for MFA, but do so on an unverified device, they still won't be able to gain access. This greatly reduces the attack surface.

Like user verification, Centrify leverages its solution integration to make sure access to devices is secure. A mixture of device policies, device identity (through a unique certificate assigned when the device is registered), MFA, and UBA (which can determine if the user is logging on from the device they normally use, whether they logon from the Starbucks free Wi-

Fi all the time, etc.) are used. And, as with the user, for every attempted or successful access, details around the device are fed back into a profile to determine its risk level in future access requests.

This use of multiple solutions in tandem reduces the attack surface — especially in scenarios where stolen property could be used against you.

Limit Access & Privilege

Even after layering on security to verify user/device, users still shouldn't have unfettered access. You want to reduce the user's ability to move laterally within the organization, as well as to the systems, applications, and data they need to do their job.

And by limiting access, I don't mean *Least Privilege* in the sense that you define and assign just the permissions they need in a steady state. I'm talking more along the lines of providing users with access in real-time *when they need to perform a task*. By doing so, you materially reduce the attack surface.

Centrify accomplishes this using a combination of solutions that, again, work in concert. *Shared Account Password Management* provides a secure vault to store passwords, making them accessible to users based on roles and policies. *Privilege Elevation* uses role-based access control and privilege self-service for on-demand access. And, lastly, *Secure Remote Access* provides proxied access to privileged sessions, which obfuscates the credentials used, while also recording the session to create a complete audit trail of all privileged activity. All activity is fed back via the UBA solution and incorporated into user profiles to determine risk for future requests.

Learn and Adapt

This last section has really already been covered in the previous three, but it needs to be pointed out. Security can't be static — users change locations, log on at different times, need to take care of emergencies, and change roles over time. By watching the interaction of users (and their devices) with the organization's data, applications, and systems, and plugging all that back into Centrify's UBA to identify potential risks, you enhance the other steps, making them more accurate and deliberate in providing or denying of access. This risk-based approach is also crucial to properly balance the security needs of the organization, the productivity of IT admins, and the ease-of-use for the end users.

Making Zero Trust Security a Reality with Centrify

Zero Trust as a *security model* is easy to achieve — just give no one rights to anything. It's making Zero Trust Security productive that takes work. Providing on-demand, real-time responsive access based on multiple factors is what makes Centrify's Next-Gen Access so powerful — especially in a Zero Trust Security environment.

By intelligently validating each aspect of a user's need for access, leveraging multiple solutions working together, Centrify finds the balance between security and productivity, while achieving a zero trust state.

Easily “converse” about Next-Gen Access in any setting.

No organization wants to experience a data breach. But traditional security methodologies only provide a limited blanket of protection, leaving gaps big enough for breaches to occur. In this book, I’ll explore the concept of Zero Trust Security as a way of minimizing risk and look at how it can be powered by Next-Gen Access.

About Nick Cavalancia

Nick Cavalancia is a technical evangelist and a 25+ year IT veteran who regularly speaks and writes for some of today’s more recognizable companies. Follow Nick on Twitter @nickcavalancia and @techvangelism.