solarwinds

WHITEPAPER

Zero Trust Security:
Getting to “Zero” Requires a Secure Foundation

Zero Trust Security: Getting to "Zero" Requires a Secure Foundation

It's safe to say today that cybercrime is as robust and evolving a tech industry as its IT security equivalents. Attacks are more frequent, more sophisticated, and more successful, requiring organizations today to shift security strategies to more secure models that take the most restrictive of stances when it comes to providing access.

It's one of the reasons the Zero Trust IT security model has seen such growth over the last few years. What started as a conceptual framework by analyst firm Forrester in 2010, has grown in interest and complexity to bring about a definition of entire sets of core services—and even a formal extended ecosystem to augment the capabilities of a Zero Trust network.

Zero Trust grew out of the need for a security model that was safer than the traditionally accepted "trust, but verify" method. Many organizations have utilized least privilege principles in conjunction with "trust, but verify" thinking as a way to limit access, but still allow the trusted credential to always utilize the access granted. In this way, least privilege feels more like an academic exercise around "what's the minimum access that can be provided while still allowing the user to do their job," rather than the answer to providing ongoing restrictive security. What's needed is less a conceptual security stance (like that found in least privilege) and more a practical living security model that actively protects the organization.

Enter Zero Trust.

What Is Zero Trust Security?

Zero Trust security is an IT security model that takes a holistic approach to network security using several different principles and technologies.

With Zero Trust, the dynamics change entirely. In least privilege, the assumption is once you've assigned the correct limiting permissions, it's safe to trust the user to utilize those permissions. In Zero Trust it's completely the opposite; even after roles and permissions are assigned, the default position is "never trust, always verify." Think of passport checks when entering a country—you've been issued a passport that presumably gives you the "permission" to enter the country, but what happens at the passport control booth? The officer doesn't trust you just because you have the needed "permission;" instead, they ask questions, check the validity of the passport, make sure it matches the owner (you), etc. In essence, they are verifying it's actually you to be certain you are allowed into the country.

Same thing goes with Zero Trust as a security model, the difference being the verification is based on credentials, time of day, whether you’re inside or outside the network, what resource you’re trying to access, whether all of this is predictably “normal” for your user account, and more. In short, Zero Trust security helps address both insider and external threats by never making the assumption that a) you are who you say you are, and b) the access you want is a given.

Understanding Zero Trust is the beginning; laying its foundation is the next step.

The Real Challenge of Zero Trust

The greatest barrier to truly getting an environment to a state of Zero Trust isn’t the whole “are you who you say you are” part. Instead, it’s actually the work of ensuring the access that identity provides remains consistent with internal security policy over time. In other words, is the access Zero Trust is protecting correct? For example, should someone make a change to permissions that, say, overprovision the access needed—by either granting too many rights or rights to too many users, all those security solutions that revolve around identity are simply going to blindly allow the overprovisioned access without having any idea it’s even in place.

The strength of the Zero Trust model is based on an assumption that the underlying foundational security is sound. And, as with any foundation, if it’s weak, anything built on top of it crumbles.

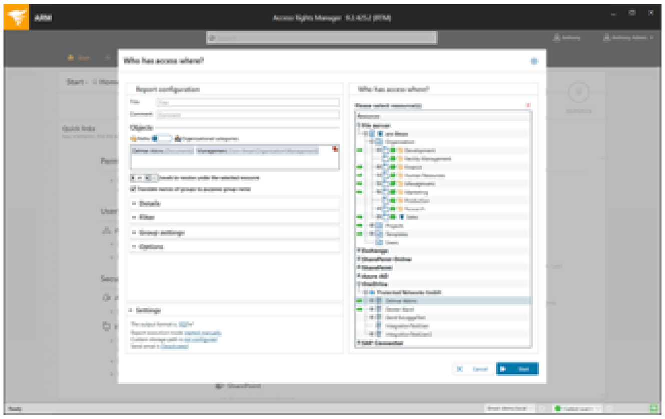
> ### Ensuring a Secure Foundation for Zero Trust: SolarWinds
>
> Any security model requires every aspect be as restrictive as possible to minimize the threat surface and the risk of successful attack. Organizations looking to implement Zero Trust eventually realize this same requirement exists, compelling a deeper look into and management of the underlying security that upholds Zero Trust.
>
> SolarWinds solutions help organizations seeking to implement Zero Trust ensure every underlying part of the environment remains safe in an effort to reach a true state of Zero Trust.
>
> **Look for insights from SolarWinds throughout this whitepaper!**

In this paper, we’ll focus on why you need to first focus on foundational security, what’s entailed, and how the monitoring of events and the management of permissions—as tactical as they sound—are critical to properly underpin a strong and effective Zero Trust security model.

SolarWinds Insights: Zero Trust Requires Visibility

The challenge of "getting to zero" has a lot to do with an organization's inability to see every last security detail that defines what a given account can access— and how that changes over time. Without visibility into every part of the network on which Zero Trust sits, the harsh reality is organizations are nowhere near "zero."

SolarWinds® Access Rights Manager (ARM) (shown below) provides organizations with visibility into permissions across a wide range of platforms and applications, including Active Directory®, Azure® AD, Exchange™, NTFS file systems, OneDrive®, SharePoint®, and more.



Establishing a Zero Trust Foundation

Much of the emphasis today with Zero Trust is heavily placed on the management of identity and authentication. After all, this is where the digital equivalent of "passport control" resides, right? But there's a problem with solely focusing on the point of authentication: The whole point of Zero Trust is to protect internal resources from inappropriate access. So what happens if the access a given account is granted is inappropriate to begin with? If an account has more permissions than intended, the whole purpose of "never trusting" anyone with any kind of access is completely missed.

To avoid this scenario, it's necessary to focus on building a secure foundation to Zero Trust. Functionally speaking, you should be thinking about the access granted to user accounts either directly or via groups in the form of permissions, as well as the management of that access. This includes any resource protected by Zero Trust.

What's involved in building a strong foundation for a Zero Trust security model?

There are three basic steps to building and maintaining a secure foundation:

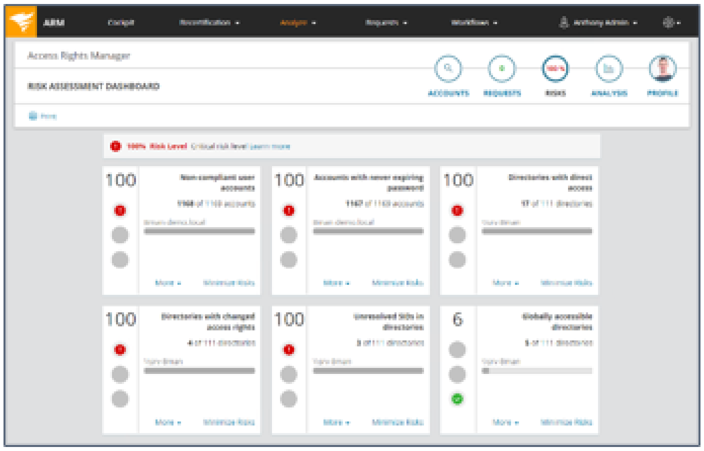
1. **Assessing Risk** – The first step is to determine whether the network environment that Zero Trust rests on has the most secure configuration possible. In everyday terms, this includes an assessment of configuration and permission assignments of every service, system, application, and data set that is eventually protected by solutions that are a part of your Zero Trust initiative.

   The work involves performing a detailed inspection of all things related to assigning access, including permissions, which accounts have been granted access, and group memberships. The goal is to do the work intended by least privilege principles but with the understanding of how the business operates when passed through the lens of Zero Trust.

SolarWinds Insights: Risk Is a Multifaceted Problem

The work of assessing how much of your environment creates a risk for your Zero Trust implementation is complicated at best. There are so many sources of risk within a given security configuration, it would take weeks to filter through every account, group membership, permission, etc.

SolarWinds Access Rights Manager (ARM) simplifies this work through the use of risk dashboards (shown below) and robust reporting to help automate the work of determining what parts of the environment are not properly secured.



Access Rights Manager

RISK ASSESSMENT DASHBOARD

100% Risk Level Critical risk level Learn more

100 Non-compliant user accounts
1168 of 1169 accounts
tenant.demo.local

100 Accounts with never expiring password
1167 of 1169 accounts
tenant.demo.local

100 Directories with direct access
17 of 111 directories

100 Directories with changed access rights
4 of 111 directories

100 Unresolved SIDs in directories
3 of 111 directories

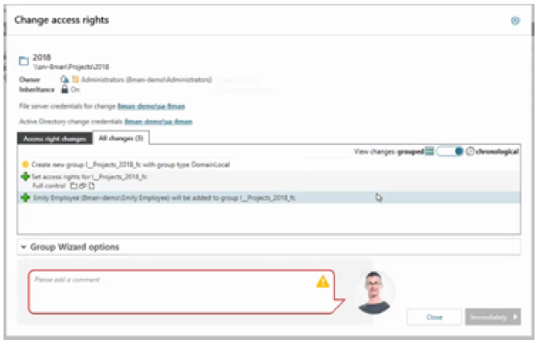
6 Globally accessible directories
5 of 111 directories

2. **Managing Risk** – The security assessment will, no doubt, unearth a number of misconfigurations, gaps, and vulnerabilities based on the way the environment is currently configured. These will need to be corrected to facilitate a security baseline that defines exactly who should have what access—which Zero Trust will enforce.

SolarWinds Insights: Risk Management Needs to Be Automated

Truthfully, one of the reasons organizations find themselves in a state of less-than-perfect security is all of the manual changes and mistakes made over time. Zero Trust doesn't permit those same mistakes; instead it demands as close to perfection as is possible—and that means you're going to need a way to ensure a consistent outcome to any and all management.

SolarWinds Access Rights Manager (ARM) utilizes intuitive automation (shown below) to define and perform management tasks that need to be conform to the needs of Zero Trust.



Change access rights

2018
\\srv-8man\Projects\2018

Owner: Administrators (8man-demo\Administrators)
Inheritance: On

File server credentials for change: 8man-demo\sa-8man

Active Directory change credentials: 8man-demo\sa-8man

- Create new group l_Projects_2018_fc with group type DomainLocal
- Set access rights for l_Projects_2018_fc
  Full control
- Emily Employee (8man-demo\Emily Employee) will be added to group l_Projects_2018_fc

1.

3. **Containing Risk** – Any deviation from the established baseline can impact the organization's ability to maintain a state of Zero Trust and introduce risk. So it's imperative to have a means by which to monitor any and all changes made to any part of the baseline, so that it may be reviewed and responded to as needed. There are two types of changes that introduce risk and, therefore, need to be monitored:

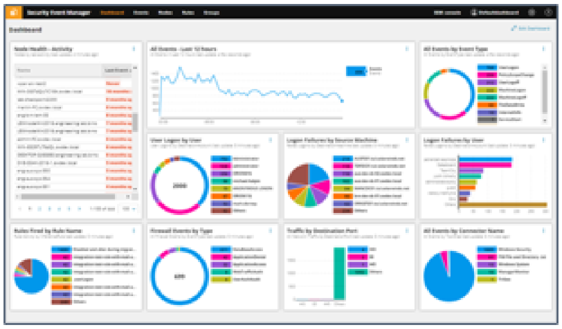
   - **Administrative changes** occur because business needs also change over time. Take the simple example of a group account in Active Directory that serves as the basis for access to cloud-based application via your Zero Trust infrastructure. Should that group be repurposed and given access to additional resources without first checking to see who is a member, the action results in users being overprivileged. The same could be true in circumstances where permissions assignments are modified accounts.

   - **Malicious changes** are also possible in cases of external attackers seeking to establish persistence and access by modifying Active Directory or resource-specific permissions lists.

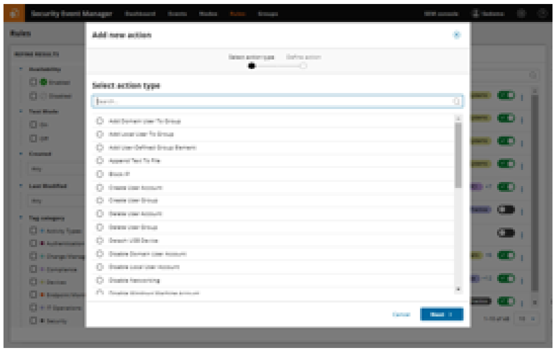
SolarWinds Insights: Risk Containment Requires Monitoring and Response

The ongoing work of containing risk in Zero Trust is as much about remediating a raised concern when it happens as it is to see the concerning action taken in the first place.

SolarWinds Security Event Manager (SEM) centralizes log and event data into a single view, providing insight into the current security state of the environment.



With an ability to see network-wide activity in real time, SEM can take action based on defined conditions to quickly contain risks.



Getting to "Zero"

At its core, Zero Trust actually puts significant trust in the assumption that every aspect of your security—that defines who has what access—is current. For most organizations, this isn't the case. Years of unaddressed changes to user and group accounts in Active Directory, modifications to resource permissions across so many disparate applications, systems, and platforms all result in the true state of your security being unknown and insecure.

The work of getting to Zero Trust requires a practical re-evaluation of the foundational security everyone assumes is already correct. By following the three steps outlined in this paper, you'll help your organization understand whether the assumption is warranted, be able to identify weak points in security, and utilize genuine, ongoing visibility over time into whether the security Zero Trust assumes is in place is correct, up-to-date, and appropriate.

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-prem, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.