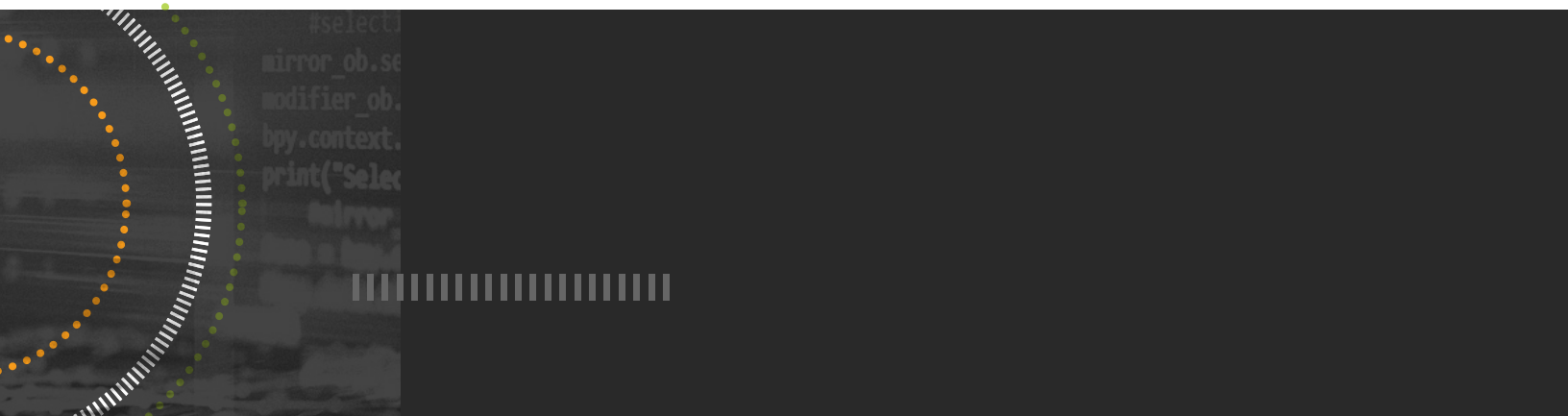
solarwinds

WHITEPAPER

Achieving an Assume Breach Culture Within Your Organization

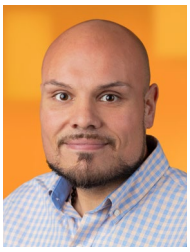
A Complete Guide From Adoption to Implementation

By Humberto Amador, Tim Brown, and Chris Day



Meet the Authors

Dr. Humberto Amador, *Senior Director of IT, SolarWinds*



Dr. Amador spent ten years as a systems engineer focused on virtualization and storage systems. He holds a bachelor's in forensic science with a focus on cybercriminal investigations and counterterrorism, has an MBA in IT project management, and received his Doctor of Information Technology degree from Capella University. His goal is to help businesses achieve high performance through internal alignment.

Tim Brown, *SolarWinds CISO and VP, Security*

Tim Brown is at the front line of the most vexing challenge facing organizations today: IT security. Tim is currently the Chief Information Security Office and VP of security for SolarWinds with responsibility spanning internal IT security, product security, and security strategy. As a former Dell Fellow, CTO, chief product officer, chief architect, distinguished engineer, and director of security strategy, Tim deeply understands the challenges and aspirations of the person responsible for driving digital innovation and change. Tim has over 20 years of experience developing and implementing security technology, including identity and access management, vulnerability assessment, security compliance, threat research, vulnerability management, encryption, managed security services, and cloud security.

Chris Day, *Chief Information Officer and Group Vice President*

Chris Day is CIO at SolarWinds, an IT infrastructure management company headquartered in Austin, Texas, with more than 30 offices and 3,200 employees worldwide. With over 30 years of technology experience ranging in IT to product research and development (R&D), Day assumed the role as SolarWinds CIO after having led the SolarWinds SaaS DevOps and site reliability engineering (SRE) global divisions. He has held other executive IT positions with BioGen Idec, PegaSystems, and Level(3) Information Services where he also served as CIO. Day holds a Bachelor of Science in computer science from Bentley University.

Achieving an Assume Breach Culture Within Your Organization

A Complete Guide From Adoption to Implementation

Do a quick internet search for enterprise security strategy, and you'll likely come across the term "zero-trust" with varying definitions from some of the biggest names in the tech game. Enterprise security means different things to different people, as the many definitions show us. But key to adopting an effective security strategy is determining a way to effectively reduce the attack aperture and risk—taking a step outside of a standard enterprise security term.

At SolarWinds, instead of adopting only zero-trust, we decided to take reducing the attack aperture and risk a step further. We work from an assume breach mindset to secure our enterprise because we understand the importance of taking as many measures as possible to insulate your environment from security threats. We have built our assume breach mindset into our overarching Secure by Design approach.

Assume breach means we start with assuming something has been breached (a user or asset), look at the possible result, and determine how to limit the exposure. By using the guiding principles of Secure by Design, we aim to eliminate implicit trust in applications and services and assume users aren't secure and are most likely already compromised regardless of authentication practices. In our everyday practices, we're moving toward single-pane-of-glass observability insights with integrated artificial intelligence (AI), machine learning (ML), and AIOps to speed issue discovery, decrease manual errors, and modernize our digital performance.

Does adopting an assume breach mindset makes sense for your business? This whitepaper discusses the current state of breaches, critical considerations for building a security strategy, and what we've learned in our journey of adopting an assume breach mindset with observability.

Single-Pane-of-Glass

In our everyday practices, we're moving toward single-pane-of-glass observability insights with integrated artificial intelligence (AI), machine learning (ML), and AIOps to speed issue discovery, decrease manual errors, and modernize our digital performance.

WHAT IS ASSUME BREACH?

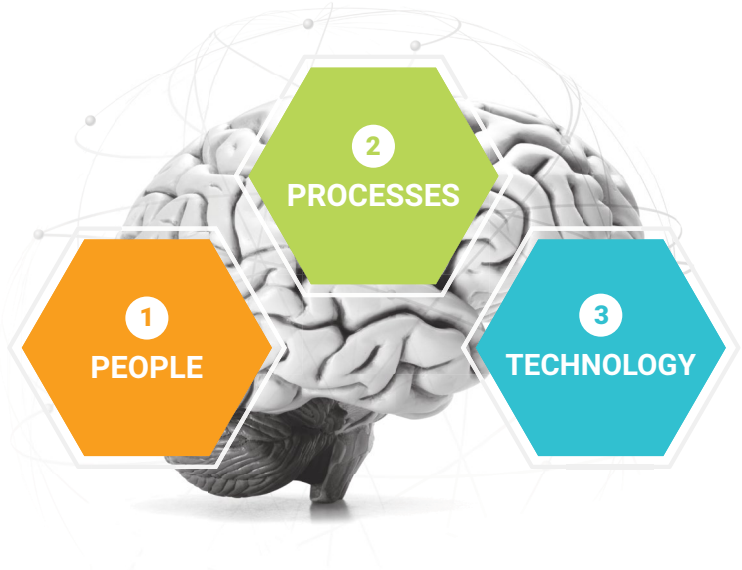
Assume breach is a mindset guiding operational security practices and investments. It's generally considered part of a zero-trust maturity model in which the organization eliminates implicit trust, relying on AI and analytics to continuously validate connections between users, data, and resources through identity and access management (IAM), multi-factor authentication (MFA), and other measures.

> With assume breach, an organization can ascertain if a compromise was caused by an application, user, or asset.

An assume breach mindset forces organizations to verify that their protection, detection, and response mechanisms are correctly implemented. This goes a long way toward preventing "knowledgeable attackers" who try to use legitimate assets, such as compromised accounts and machines unknown to the organization. Specific controls need to be implemented to ensure someone with access rights can't abuse these rights, such as requiring two people to make a change. Other controls include immediately generating logs and alerts to be sent to a security operations center when rogue commands are run or when access by someone or something is inappropriately attempted.

Coupled with observability, organizations can gain single-pane-of-glass visibility into the entire environment, allowing organizations to proactively identify issues, including potential breaches. The assume breach model needs accurate information to mitigate risks, an essential element observability can improve. With observability, your teams can have clarity on your assets and how they fit into the ecosystem while gaining data about the infrastructure and indicators to help protect the most important assets.

Given the complexity of modern environments, adopting an assume breach mindset can be even more critical depending on the types of customers an organization serves and as the organization expands products, services, or revenue. Assuming a breach will happen and protecting yourself by embracing this new model—which continuously evolves to mitigate the ongoing risks of sophisticated threat actors—can help organizations protect against vulnerabilities before they're exploited. Adopting an assume breach mindset can also be a crucial component of your overall security posture as it relates to security regulations that your organization may need to comply with.



ADOPTING AN ASSUME BREACH MINDSET

To implement an assume breach mentality, organizations must focus on building a strategy to address three core elements: **people**, **processes**, and **technology**. Since assume breach looks across applications, services, user identities, and networks, all three elements must work together to achieve the assume breach mindset. Even when you can't stop a breach, correct processes can help limit the harm done by a bad actor.

1 PEOPLE: Your first line of defense

The device is no longer your weakest point; now, the user poses additional threats to your environment. Assuming a threat actor can target, socially engage, and potentially phish any user poses a new challenge to modern-day security experts. It puzzles them with the following thought: "How do I protect users from themselves, and how do I protect the organization's assets and data from users?"

Reevaluating how you approach remote work, team dynamics, and continuing education can aid in mitigating as many risks as possible to help ensure the highest levels of security.

Address remote work security

Though it's convenient, remote work adds another layer of risk to the organization. The IBM® 2022 Cost of a Data Breach Report found that 45% of breaches were cloud-based. An assume breach security strategy can help organizations increase cyber resiliency and manage risks in remote work environments. The approach supports securely connecting the right users to the right data at the right time under the right conditions.

Organizations may implement a robust identity management program to reduce their overall threat vector, proactively monitor workstations, and complete routine auditing to push out suspicious activities in the network. They can also implement best practices to prevent, mitigate, and manage future incidents.

Build the team you need

Finding the right talent to support your security operations and information security teams can be critical to cybersecurity. Organizations don't just need knowledgeable leaders—you must also work with existing employees to adapt their knowledge around what it means to secure the environment. Since assume breach is a mindset change, partnering with your people technology or HR department is crucial in developing a robust internal frame of mind.

Given the complexity of some environments and the level of data sensitivity, more organizations are becoming targets for threat actors. These threat actors are developing sophisticated approaches to gain access to the environment—approaches your teams should be knowledgeable about to protect your applications, services, user identities, and networks.

Prioritize security training and continued education

With an assume breach mindset, the organization acts to ensure proper protection of its data and most critical assets. This concept requires continuous training and education at the organizational level to ensure the concepts are exercised, and new employees are acclimated to the environment.

Leveraging a learning management system (LMS) or other corporate resources for training can provide formal training to the organization's users on key cybersecurity awareness concepts. This approach can also help organizations spot the signs of a cyberattack attempt, like phishing. Internal phishing campaigns can be leveraged to identify vulnerable users and provide them with more active and monitored training. Operating a "think before you click" campaign can also help educate the staff on how easy it is to compromise a user or device. In extremely sensitive environments where data is critical, keeping active logs of user activity is also highly recommended.

These ideas can be formalized by a corporate-sponsored training program to require each user to undergo annual training. Security awareness training must be mandatory in some environments, as it's tied to many regulatory compliance entities. In more mature environments, security training should also be standard practice. It's important to remember you're only as secure as your users are educated, as threat actors are consistently finding creative ways to get in.

A Mindset Change

Organizations don't just need knowledgeable leaders—you must also work with existing employees to adapt their knowledge around what it means to secure the environment.

2 PROCESSES: Why policy is critical

Business process and policy management lie at the core of an assume breach mindset. Policy and business processes don't just affect the physical user—they also affect the technical environment. Like a user policy, a system policy provides a set of controls to an authoritative function (such as Active Directory®) to manage policy across multiple devices. Aligned with a strong firewall policy to manage incoming and outgoing traffic and a good network access controller to help ensure users meet proper conditions, you can manage and help demonstrate compliance for most devices.

However, since policy affects both the technical and non-technical aspects of the environment, how can organizations ensure the right policies are in place to allow the user to do their job in a controlled and secure manner?

Predict scenarios through modeling and situational awareness

One way to help ensure your business is prepared for a breach is to model breaches. Modeling potential attack vectors, determining where a breach could come from, and understanding how it can impact your environment provides valuable insight into how you can potentially mitigate the breach.

This is a practice we undergo often. We spend a great deal of time red teaming trying to infiltrate, attack, and impact our environment. By doing so, we gain knowledge about how these activities could be successful, learn where to put stops in place to limit success, and better understand how bad actors think when trying to infiltrate. In other words, our ability to mitigate these risks is improved by our attempts to think like the bad actor.

In addition, if you successfully infiltrate your environment posing as a bad actor, you can practice how your organization reacts and responds to a breach. Your organization can prepare a response plan for a breach by creating internal and external marketing assets, drafting official statements, and ensuring the appropriate stakeholders understand their responsibilities. By role-playing through different scenarios, your teams can develop a real-world feel for what would happen during a breach and be more prepared when it occurs.

Gain organizational alignment

As organizations evolve, processes must also evolve to meet corporate and market demands. Aligning your technical teams on approach, tools, and methodology can help you achieve the desired mindset.

From a security perspective, aligning with your organizational growth plans early on can provide an advantage in preparing for what's to come. If an organization is expected to expand geographically, understanding the regulatory compliance concerns and local privacy laws can help you establish the right business processes.

From an IT standpoint, standard policies should govern how the organization's users are expected to utilize its resources. Policies such as acceptable usage, bring your own device, data controls, and non-disclosures can all help protect the environment, user, and business from many risk factors.

As an organization, you must ensure these processes align with the desired user experience while maintaining adequate protection. Having an organizational change management (OCM) manager on hand to incorporate OCM concepts can help ensure successful changes to mitigate risk. Otherwise, users may be unhappy with the changes, making it increasingly challenging for organizations to adopt an assume breach mindset.

Limit and protect user access

Alongside user- and device-level policies are access control policies designed to be implemented at the network and physical levels. This is where the "principle of least privilege" comes into play, as access can be specific to a user type within the organization. One good example is a software engineer needing access to the build pipeline. Ideally, access would be extremely limited to the build pipeline in production, and there would be less restrictive access in staging. This allows the engineering team to access staging and openly perform code modifications without increased restriction.

However, this doesn't mean the software engineer can install any tool or service in staging, as policies would be in place only to allow the engineer to complete work with sanctioned or approved tools made available to the environment. The production build pipeline can be limited to only service account functions or users with privileged access. The build process can run automatically after a peer review is conducted on the final code output in staging. This is another excellent example of a policy-driven, access-controlled environment where the software engineer user type can perform their duty without knowing the restrictions set to protect the organization.

Policy-driven protection is also significant within software development environments. Presenting the right level of protection with flexibility enables engineering teams to produce code freely, ultimately making for a more secure product. By maintaining a multi-layered threat restriction approach with conditional access granted to one environment and restricted access to the other, organizations can retain enough flexibility to make proper testing and production of code possible and help to protect the organization from potential supply chain attacks.

Policy-Driven Protection

By maintaining a multi-layered threat restriction approach with conditional access granted to one environment and restricted access to the other, organizations can retain enough flexibility to make proper testing and production of code possible and help to protect the organization from potential supply chain attacks.

3 TECHNOLOGY: Reassess and protect

Technology can go a long way toward providing a barrier to intrusion and can go further if properly developed alongside an assume breach mindset. Without this mindset, the organization may have difficulty embracing the technology. When people and processes are aligned, organizations can assess and build technology to meet the needs of the business.

Start with the network

Adopting an assume breach mindset around technology begins with a paradigm shift in how we view the network and how our systems grow and work together. Traditionally, the network was thought of as an avocado. The most vulnerable part of the avocado, or network, is the seed. The traditional network firewall is the skin or the shell. Network and security engineers would take an empirical approach to managing security, looking for possible entry points and solidifying them with intrusion detection and prevention techniques. Exploits were mainly focused on gaining network access to cause disruption. As the sophistication of threat actors improved and the assets within an organization became more valuable, so did the approach used by the network and security engineers.

As digital transformations continue, the metaphor of the avocado must adapt. The old firewall model no longer suffices as a primary form of security for modern businesses. Because there are more possible entry points, we must now view the network as a pomegranate. Within the pomegranate, each application, user, or technology is a seed encased in the network shell. Each seed needs its own protective coating to protect it from other seeds within the network, all connected by a web holding each one in place. When observability is introduced, the webbing holding each seed together becomes fully visible, allowing organizations to view every seed and how each one interacts with the network and the tech stack as a whole.

Understanding risks in your environment

The specific components within a technical environment—such as servers, network devices, intelligent firewalls, applications, critical data, and code repositories—help determine the infrastructure to implement. Knowing how your services and components affect your risk exposure is critical when deciding how to best protect the environment.

Let's take critical assets as an example. Critical assets can cause an increase in risk exposure because they're vital to your network. When you manage them effectively, they can help you stay ahead of possible threats and vulnerabilities. One way an organization can gain insight into potential vulnerabilities and how to protect against them is by organizing and classifying critical assets based on their impact on the business.

Businesses should ask themselves the following questions:

Which of your critical assets pose the highest cost if breached?

Which assets can be easily breached based on their architecture?

Which assets are vulnerable because of the type of data they're exposed to?

Understanding how each critical asset is classified can drastically improve the approach used to protect them. If you don't know what assets comprise your network, you can't understand where the vulnerabilities lie—again, this is where adopting observability can significantly increase visibility and infrastructure management. The broad-sweeping and easily identifiable vulnerabilities are important to mitigate, but skilled threat actors often use hidden vulnerabilities to infiltrate and wreak havoc on your network.

Reevaluate user access management

In addition to helping users understand their roles in preventing breaches, you must reassess how you approach user identity and access to your environment. IBM reported 20% of breaches were caused by compromised credentials in 2022. Today, your users likely access your system from multiple devices across the globe. And though you may not be able to ensure their devices (like personal cell phones) are secure, you can take measures to require two-factor authentication or a different verification method to access company documents or applications.

However, more than user access management is needed to protect your environment. Threat actors can manipulate the system and make it think they're legitimate users by circumventing and intruding on the login/authentication process. Even in instances where multi-factor authentication exists, threat actors can circumvent the process and validate an SMS request from a remote location. Though user identification can help mitigate risk, it can't eliminate it.

Consider adopting identity management solutions to enforce a single identity, which can help mitigate risk associated with users. Because users can be misled and socially engineered to compromise themselves, organizations are often tasked with protecting business assets and data by putting controls in place to protect the environment from the user. By initiating a program like this, you can help ensure access to your network or company-specific applications isn't available to anyone, making it harder for a threat actor to infiltrate your system through user credentials.

Identity Management Solutions

Because users can be misled and socially engineered to compromise themselves, organizations are often tasked with protecting business assets and data by putting controls in place to protect the environment from the user.

BUILDING A ROADMAP TO ACHIEVE AN ASSUME BREACH MINDSET

Work with your team to build a roadmap based on how you want to operate within the assume breach mindset. Below are several key requirements to consider when building your roadmap to help make implementation faster and more successful.

Determine the destination

Whether you're following a zero-trust or an assume breach model, you must know what you're building toward and what you want to get out of the implementation. In some cases, meeting regulatory compliance is sufficient, but for more uncompromising organizations, establishing a plan with critical success factors and incrementally driven milestones can help them realize and maximize value.

Secure executive support

Given the significant investment often accompanying IT purchases, corporate and business executives typically cringe when IT pros walk in with a "bright new idea." But cybersecurity and threat mitigation are critical, and continuing to be part of the 79% of people identified in the IBM report who haven't adopted a strategy will cost far more in the long run to the organization's bottom line, customer perception, and reputation.

Implementing an assume breach mindset can't eliminate the risk of a breach or create a 100% secure environment.

> One hundred percent secure is never possible, but the assume breach mindset can help make an environment as secure as possible and support expedited breach discovery and resolution with the right tools and practices in place.

Select vendors and partners to help

A reputable third-party consultant can help you along the journey toward an assume breach mindset. Look specifically for vendors with experience responding to or actively working through incidents. You'll also want vendors who are well-connected with experts in the industry to provide reputable insight into the most effective way to approach and implement these concepts.

However, picking the wrong vendor or partner can leave you open to more vulnerabilities than before. This is because the fabric of assume breach is built around trusting no one and implementing just the right level of control so a user can be productive in the environment provided. Observability supports the ability to quickly identify access rights issues to help prevent vulnerabilities across your infrastructure.

SolarWinds isn't just a knowledgeable partner capable of supporting your assume breach mindset—we're also industry leaders in observability solutions. Wherever you are in your digital transformation journey, SolarWinds has solutions designed to scale with you and provide the features you need at every step.

Master data classification

Proper data classification is also key when rolling out new security measures. Proper data classification can lead to a better understanding of mission-critical business assets and how best to protect them.

Because it provides unified, extended visibility across your entire technology stack, observability is crucial in gaining a fuller picture of your total surface attack area. This helps you detect and prevent vulnerabilities before they occur and master data classification. Key elements of observability include performance metrics, gathering data, and log analysis. Because metrics are the number one way to measure success, ensuring your data is classified accurately is critical.

Key Elements of Observability

- ✓ Performance Metrics
- ✓ Gathering Data
- ✓ Log Analysis

OBSERVABILITY IS CRITICAL TO SECURITY

Though organizations have traditionally used multiple tools to monitor their environments proactively, managing multiple toolsets has resulted in a critical challenge many businesses face today. Using different tools can also create disconnected data points, which require a lot of manual intervention and increase the opportunity for manual error. Users are often left to consolidate data points on their own to present a summary of the overall environment.

Observability takes this approach and flips it upside down, focusing on establishing a baseline using a centralized solution designed to unify the data and provide intelligent reports. The value realized through reduced human labor, improved visibility, and improved mean time to resolution (MTTR) is usually self-sustaining.

Observability introduces an approach to monitoring and managing components across your infrastructure to help you improve your environment's overall health. It can also provide a general health score you can easily reference to improve, optimize, and mature your environment continuously. In practice, observability helps you address many aspects of the security life cycle by providing deep visibility into the environment to help enable a more proactive approach. All this is necessary for a fully implemented assume breach approach to cybersecurity.

From a security standpoint, it takes great effort to constantly observe environments for anomalies. In some cases, automation can allow for the detection and remediation of certain issues. These issues can then be documented and reported to the security team, which usually conducts a retrospective exercise to understand why it happened, what could have been done to better protect against it, and how they'll prevent it in the future.

In other cases, proactively patching the environment may be enough to stay ahead of new threats. Like a flu vaccine, the intention is to download the new virus definitions and instructions and update all the agents so the antivirus can quickly and effectively identify and quarantine the latest threats. Both practices require a deeper level of monitoring within the environment. Because observability is more than just monitoring, it can go deeper and provide the end-to-end visibility necessary to truly adopt an assume breach mindset.

Observability can increase assume breach benefits

Both SolarWinds® Hybrid Cloud Observability and SolarWinds Observability, our software as a service (SaaS)-based observability solution, integrate AI and ML to help expedite MTTR. Incorporating AI and ML also means fewer necessary manual tasks, saving time and money while reducing manual error.

As with many suggestions around security, people always think, "It won't happen to me" until it does. However, we know a breach will happen—it's simply a matter of time. Stakeholders should be aware of this and understand the longer the organization's environment goes unprotected, the higher the likelihood when a breach does happen, it will be costly and detrimental to the organization's reputation and bottom line.

SOLARWINDS OBSERVABILITY SOLUTIONS ARE BUILT TO SUPPORT YOUR BUSINESS

By prioritizing adopting an assume breach mindset, organizations can have the right processes, people, and technology in place to proactively observe their environments for anomalies and potential vulnerabilities.

Though no product can assume breach for you, SolarWinds products can provide the level of visibility needed to help enable proactive monitoring, rapid diagnosis, and quick time to resolution. SolarWinds observability solutions built on the SolarWinds Platform are designed to allow your business to grow into its needs. With the guided help of our customer success team, you can better understand the needs of your environment and establish a plan to help ensure success. Our products offer an array of value-added features and reports you can customize based on your environment and business needs.

SolarWinds can help by providing robust observability solutions, customer service, and internal support to help address your business needs now and in the future. To learn more about our guiding principles for how we approach security and cyber resiliency at SolarWinds, visit our Secure by Design resource center.

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of simple, powerful, and secure IT management software built to enable customers to accelerate their digital transformation. Our solutions provide organizations worldwide—regardless of type, size, or complexity—with a comprehensive and unified view of today's modern, distributed, and hybrid network environments. We continuously engage with technology professionals—IT service and operations professionals, DevOps and SecOps professionals, and database administrators (DBAs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures, applications, and environments. The insights we gain from them, in places like our THWACK® community, allow us to address customers' needs now, and in the future. Our focus on the user and our commitment to excellence in end-to-end hybrid IT management have established SolarWinds as a worldwide leader in solutions for observability, IT service management, application performance, and database management. Learn more today at www.solarwinds.com.

solarwinds

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

© 2023 SolarWinds Worldwide, LLC. All rights reserved. | 2302-EN

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

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.