The SolarWinds Silver Lining

Motivating the Move to Zero Trust

Synopsis

Effective implementation of a Zero Trust security strategy would likely have prevented what is plausibly the most damaging cyberattack in US history, the full impact of which is far from realized. This whitepaper explores how SolarWinds, or any one of the 18,000 companies compromised by the SolarWinds breach, could have leveraged Zero Trust principles to establish tripwires alerting to the attack in its earliest stages. Coupling these strategies with an effective/progressive prevention posture, the plausible result would have been early identification and eradication.

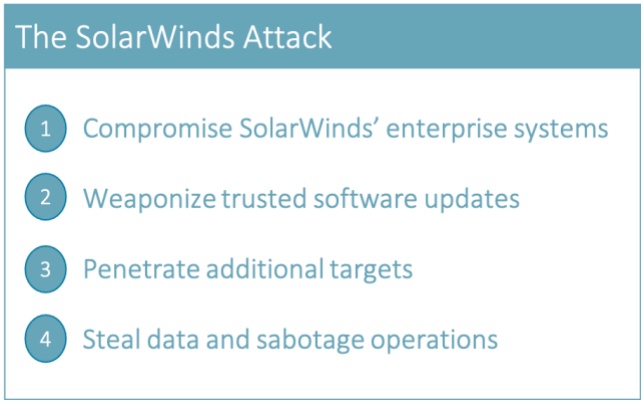
What is the Core Issue?

The SolarWinds breach generated a lot of commentary. How did it happen? How should the 18,000 impacted customers respond? What does it mean for national security? Most of the focus is on the impact of the attack rather than the root of the problem: the lack of detection and mitigation of anomalous behavior. What if SolarWinds could have detected abnormal behavior in its system as soon as it occurred? What if all of SolarWinds' customers had the capability to do the same?

The intent of this whitepaper is to advocate that organizations adopt a Zero Trust strategy to implement these protections.

What Happened?

There were a minimum of four attack waves executed over the last 18-24 months, designed to steal insight into how the US government thinks and operates. The massive scope of the impact and spread of the malware is still being uncovered. Current analysis is that, in the first wave, a nation-state actor compromised SolarWinds at an enterprise level. The second wave attacked the product development environment, inserting trojan code into the companies' popular and proprietary Orion software. In the third wave, the attackers attached the trojanized code to a product update patch, delivered to customers between March and June of 2020. Once installed, the attackers targeted authentication systems and gained access to global administrator accounts. In the fourth wave, using trusted credentials and back-door remote access, the attackers stole confidential data and disrupted business activities.



This highly-sophisticated, multi-phase attack is a wake up call, a red flag alert that current cyber-defense strateties are insufficient. The core theme, repeating in each wave, is that organizations lack effective monitoring at the granular level required to effectively detect threatening activity within their environments.

What is the Solution?

Traditionally, networks have relied on perimeter defense. Conventional solutions establish zones of inherent trust by focusing on broad, perimeter-based security. The impact of the SolarWinds breach-and costly predecessors like NotPetya and WannaCry—shows the vulnerability of these approaches to entities that can compromise credentials to gain persistent trust. Zero Trust directly addresses this issue. Pioneered on the belief that an organization should not

inherently trust anything inside or outside of its perimeters, a Zero Trust environment narrows access, **continuously verifying all connections** to its systems before authorizing the requested operations. Furthermore, effective Zero Trust is implemented enterprise-wide, extending beyond the bounds of IT and network security, evolving beyond traditional cybersecurity approaches.

What Does Zero Trust Really Mean?

Many organizations acknowledge that Zero Trust is an attractive alternative. But, amidst the marketing blitz from a cacophony of vendors touting Zero Trust products and services, choosing the right mix can be overwhelming, and implementations too often incomplete. It is not that the claims are misleading; most of these solutions provide value in moving towards Zero Trust. The challenge is that products alone do not address the Zero Trust tenants holistically at the enterprise level.

Zero Trust is not a product feature but a strategy founded on guiding principles that are continuously pursued and applied. The objective is not an ideal, utopian state, but a continuous process to develop and improve a Zero Trust posture. The goal is to remain dynamic, flexible and scalable, able to constantly adjust to the evolving threat landscape.

Eliminating inherent trust means every entity and action are treated as potentially hostile. Every interaction is vetted every time, and all verified credentials are good for at most a single session. This results in a far more granular approach than both perimeter-based security and defense-in-depth solutions.

For example, interaction between two internal smart devices, such as components of an HVAC system, would be vetted at inception, before data exchange was allowed. Access would be allowed only for that interaction and would expire when communication ceased. There would be no persistent "trusted" connection between devices. Over time, leveraging AI/ML technologies, verification can be tightened further, down to the level of individual commands or based on analysis of explicit historical behavioral patterns.

The problems tied to exploitation, hacking and breaches reside in the granular decisions of one user or device trusting another. Zero Trust addresses the root of this problem. Security controls are designed around the entities and interactions occurring in the system environment rather than network boundaries and layers. Access, action privileges and configurations are challenged regularly to authenticate and authorize all entities providing granular focus that brings cyber risk to the forefront.

Two additional core concepts of adopting Zero Trust are continuous monitoring and continuous verification. Continuous monitoring implies an ongoing behavioral analysis of the actors and actions in an effort to develop an understanding of normal patterns establishing the baselines used in continuous verification.

Continuous verification embraces the reality that some degree of risk exists with every interaction in a system. If you validate and verify every connection and user or device interaction, you lower risk. But, is that enough? In today's adversarial world where identities can be compromised and protocols can be cloned, as with SolarWinds, solutions need to look deeper. When the actors are valid and the actions are expected, having the ability to identify deltas at a granular/behavioral level such as timing, volume and frequency is the next step in identifying unauthorized activity. Continuous verification must leverage behavioral analysis at a granular level to differentiate between system actions within a normal behavioral range and anomalies. This normal behavioral range is established through continuous monitoring.

How Could a Zero Trust Strategy Have Mitigated the SolarWinds Breach?

How would applying a Zero Trust strategy through the implementation of Zero Trust principles have mitigated each wave of the attack?

The Lockheed Martin Kill Chain

Wave 1: A Zero Trust architecture that intercepted and validated every transaction against a comprehensive baseline would have identified and alerted unknown/unauthorized access in the enterprise environment. Leveraging behavioral analysis in the detection process would have alerted on anomalies even if the credentials of the actors and actions had been compromised.

Wave 2: Looking at the enterprise environment from a Zero Trust perspective would have identified the Orion Source/Patch code as a critical asset. In-depth validation would have identified an unauthorized change to patch code, forcing an investigation into where the unauthorized code originated.

Wave 3: SolarWinds customers' inherent trust in the Orion software patch led to disastrous consequences. For the impacted clients, applying Zero Trust principles to the patching and upgrade processes should have revealed variances in check sums and other controls. These deltas should have alerted that the patches received had been altered.

Wave 4: The SolarWinds attack was detected by an analyst at FireEye when a new/unknown device appeared on the network using his credentials. It wasn't until this device was analyzed that the real issue was identified. For the impacted clients, applying Zero Trust principles at the enterprise level should have alerted to unknown/unauthorized behavior as identified by the FireEye analyst. Leveraging behavioral analysis in the detection process would have identified the unauthorized activity despite the use of valid credentials and protocols.

Key Takeaways

- The SolarWinds attack demonstrates the vulnerability of conventional cybersecurity approaches to compromises based on implicit trust.
- An effective Zero Trust approach could have detected and stopped the SolarWinds attack at multiple points.
- Pursuing a Zero Trust strategy does not mean "rip and replace" existing solutions. The approach is a paradigm, not a product. Its tenets are foundational, integrated into a wide range of consistently-enforced policies, processes and solutions.
- Maximizing granularity minimizes risk. The level of Zero Trust enforcement should be scaled to strategic choices defining acceptable risk.

Vital Questions

Can you prevent a trusted vendor from opening you to compromise?

Will your current security architecture identify and alert on new/unknown users, actions or devices?

Do you have a complete inventory of your environment? Have you implemented policy controls, and ensured that they are followed?

If so, how long would it take for your security team to analyze and determine an effective response?

What is your financial and brand exposure to a breach like SolarWinds?

Are you equipped to mitigate it?

How can a Zero Trust approach improve your security posture?

About StealthPath:

From inception in 2017, StealthPath has been solely focused on developing a purpose-built, holistic Zero Trust strategy and portfolio of products. Foundational to our Zero Trust training, consulting services and products is our proprietary Zero Trust Capability and Maturity Model, developed by a leading global practitioner and former White House Executive Fellow. The model provides a vendor with agnostic guiding strategy for enterprise Zero Trust adoption that extends beyond the network. Our training and consulting services are focused on helping organizations understand and implement a Zero Trust strategy:

- StealthPath's ZAware service provides organizations with full visibility into their operating environment, the foundation of a Zero Trust strategy.
- ZAlert takes it to the next level. With continuous monitoring of network traffic, network classification capabilities, and the introduction of behaviorial analysis for effective monitoring and alerting on anomalies.
- ZProtect (still in delelopment and testing) exends the approach to enforcement through integration with market-leading SIEM and Firewall products.

Our solutions are frictionless with no agent required, allowing for seamless integration with current tools. StealthPath's success is driven by bold leadership, innovation, comprehensive knowledge and commitment to evolving Zero Trust solutions.