Zscaler SolarWinds Response and Recovery

Request a complimentary security assessment and hands-on best practices guidance to safeguard your enterprise from SolarWinds and future supply chain attacks.

1. Get deep insight into the SolarWinds attacks, known as SUNBURST, from Zscaler's ThreatLabZ team.
2. Mitigate the impact of a potential breach with a hands-on security assessment and best practices guidance.
3. Understand how you can eliminate your Internet-facing attack surface, stop potential lateral movement and block command-and-control activity with a Zero Trust architecture.

What is the SolarWinds cyberattack?

A highly sophisticated adversary group compromised SolarWinds to distribute an infected version of the company's Orion software to more than 18,000 SolarWinds customers, including many large enterprises and government agencies. Attacks are able to exploit vulnerable versions of Orion to establish an initial foothold in impacted organizations to carry out future attacks, including data theft or business disruption. To help organizations safely navigate questions related to SolarWinds and other emerging threats, we are making Zscaler's expertise and resources available to those in need.

SolarWinds response and recovery

Zscaler is committed to being your cloud security partner of choice. With more than 150B daily Internet requests going through our inline cloud security platform, we are in a unique position to see, identify, and stop threats related to the SolarWinds SUNBURST campaign, as well as improve your security posture for future software supply chain attacks.

To help enterprises limit the impact of these critical attacks, Zscaler is offering a complimentary security assessment and hands-on best practices guidance to immediately improve your security posture. Our security experts will:

- **Ensure** you are inspecting your entire enterprise for SUNBURST and related threats, including all SSL and server traffic.
- **Examine** your logs to determine if you have any command-and-control traffic that is linked to this attack.
- **Offer** guidance on reducing your attack surface and limiting the impact of lateral movement with a Zero Trust architecture.
- **Provide** hands-on technical support to implement recommended best practices.

Granular ThreatLabZ analysis

We will engage Zscaler's ThreatLabZ team to assess whether you have vulnerable SolarWinds servers, provide relevant indicators of compromise (IoCs), and conduct a deeper analysis of potentially malicious payloads and logs.

Request your complimentary SolarWinds assessment

We've got your back. Engage with our security experts to gain insight into the SolarWinds attacks and get hands-on best practices guidance to better protect your users, applications, and systems:

zscaler.com/solarwinds-cyberattack

120 Holger Way
San Jose, CA 95134
+1 408.533.0288 | **www.zscaler.com**