**Arctic Wolf’s Response to the SolarWinds Supply Chain Attack**

Arctic Wolf is aware of the large-scale supply chain attack that has reportedly compromised U.S. government agencies via the SolarWinds Orion Platform.

With over 300,000 organizations in SolarWinds's customer base, there is obvious concern that other government agencies and private sector businesses may also be targeted, so we wanted to share the steps Arctic Wolf has taken in response to this incident.

We can confirm that Arctic Wolf is not a SolarWinds customer, and as such, we have no evidence that Arctic Wolf has been targeted as part of this campaign.

Our Concierge Security® Team has proactively reached out to Arctic Wolf customers that are SolarWinds clients to provide them with guidance on how to remediate and update any impacted systems as outlined in the [emergency directive issued by The Department of Homeland Security](https://cyber.dhs.gov/ed/21-01/).

Arctic Wolf is currently in the process of building and operationalizing several detections for this campaign using network and host-based indicators and will continue to add more detections as new details are made available.

These updated detections come in addition to the steps we take daily to ensure the systems of Arctic Wolf, our partners, and our customers, are never compromised, which include:

* Continuous 24x7 monitoring of Arctic Wolf's entire infrastructure, including partner and customer data, by the full suite of Arctic Wolf security operations solutions and the Arctic Wolf Concierge Security Team
* The implementation of strict data access policies and multi-factor authentication tools for all Arctic Wolf systems
* Regular external audits and risk assessments conducted by both third parties and the Arctic Wolf Concierge Security Team

Want to know more? The [Arctic Wolf Information Security Policy](https://arcticwolf.com/informationsecurity/) on our website provides additional detail on the steps we take to ensure the integrity of our systems.