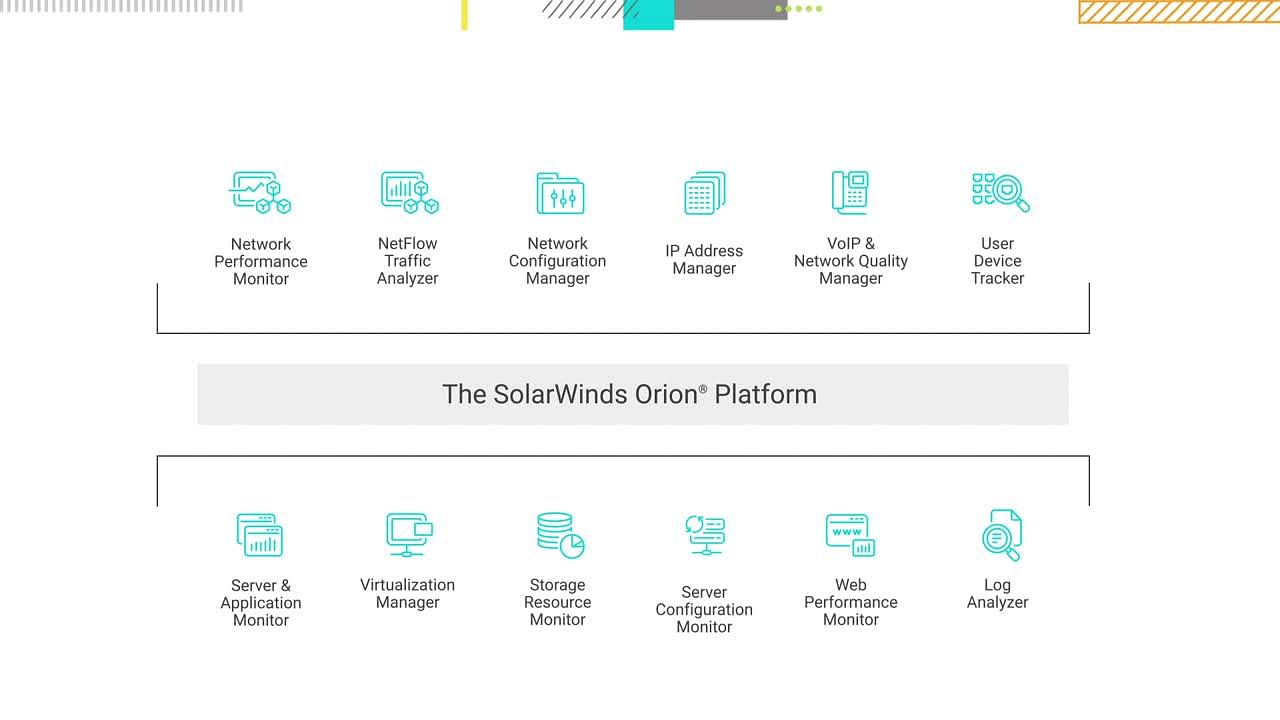
**Solar Winds - Supply Chain Attack**

**What Is SolarWinds?**

SolarWinds is a company based out of Tulsa, Oklahoma, providing [SaaS](https://www.simplilearn.com/saas-paas-iaas-quick-comparison-article) solutions for IT infrastructure, supply management, network administration, and other benefits. As a company that deals with IT infrastructure management, they have complete access to customer data, logs, and workflow details.

**How Did the SolarWinds Attack Happen?**

SolarWinds offers an IT performance management and monitoring system called Orion. The Orion platform was used by customers worldwide. To enhance its effectiveness, Orion has access to customer system performance logs and data, making it a lucrative target for hackers. This platform was a victim of a supply chain attack that affected thousands of systems and customers on a global scale.



Some features of the SolarWinds Orion Platform (Source: [Solarwinds](http://solarwinds.com/" \o "Solarwinds" \t "_blank))

The hackers used a supply chain attack to insert malicious pieces of code into the Orion framework. In a supply chain attack, malicious actors target third-party resources necessary for an organization’s workflow, preferably without the company’s direct jurisdiction.

In the Orion hack, a backdoor was created which could be accessed by the hackers to impersonate accounts and users of victim organizations. This backdoor allowed the hackers to access system files and hide their tracks by blending into the Orion activity, masking the malicious code from antivirus packages.

SolarWinds was a promising target for this kind of supply chain attack. Because many multinational companies and government agencies use their Orion software, all the hackers needed was to install the trojan onto a new batch of updates to be distributed by SolarWinds.

Considering the widespread acceptance and usage of the Orion platform, SolarWinds was a potentially promising target. The software had found use in many multinational corporations and government agencies, allowing the hackers uninterrupted access to confidential information after the SolarWinds update server distributed the malicious code.

By late 2019, the SolarWinds network had already been breached by malicious actors. The update containing the backdoor was a remote access trojan (RAT). This particular malicious update was named the Sunburst update. Come Spring 2020, and this harmful update was already being pushed out to users. Customers had no reason to doubt the update considering it came directly from the SolarWinds servers.

Now that you have learned how the SolarWinds hack expanded, you can learn more about its detection and eventual fixes.

**How Was the Hack Detected and Remedied?**

FireEye, a cybersecurity company, detected the malware spreading to their customers and was able to identify the Sunburst update package responsible for the breach. Once detected, several customers could detect similar behavior in their systems and their customers, indicating a rapid spread of the malware package. First detected in late 2020, the Sunburst update had infected thousands of systems worldwide by then.

The SolarWinds development released quick hotfixes to eliminate the backdoor trojan and was eventually followed by a queue of organizations. Global IT giant Microsoft was also said to find traces of said malware in its customer systems, causing a global release of security patches.

Let us take a look at the primary victims of the SolarWinds Attack of 2020.

**Who Was Affected by the Hack?**

More than 18,000 customers of SolarWinds had applied the Sunburst update, which then allowed the remote access trojan to infect all their customer systems and networks. Among notable victims, the US departments of health, treasury, and state were affected by this attack.

Reports also indicated that private companies like FireEye, Intel, Cisco, and Microsoft are affected by this malware. As detected by Microsoft, the ability of this update to replicate into innumerable customer devices made it a challenge to estimate the headcount of affected organizations and networks.

As of now, there is no clear indication as to who was behind the entire attack. A few fingers have been raised over state-sanctioned hackers in Russia and China, but the lack of concrete proof has left the door open for further investigations as well.

**State of the SolarWinds Hack in 2021**

The repercussions of the SolarWinds attack are still prevalent today. As recently as July of 2021, several Microsoft 365 accounts belonging to state attorneys were breached. Considering the SolarWinds attack saw a dip in the stock value of the parent company, a federal lawsuit was filed against the organization, alleging that they misled shareholders prior to the Orion breach regarding their security measures.

Every few weeks, a new problem arises due to the original hack. Be it confiscated email accounts or customers discovering new backdoors, the unauthorized access of systems opened up many issues that may take years to resolve.