ScienceLogic: Your Safe Route to Intelligent Automated Ops

Risky IT Transformations Further Derailed by Covid-19, Cyberattacks

2020 was a year of many 'unprecedenteds'. In response to Covid-19, enterprises already trying to stay ahead of their planned digital transformation efforts were scrambling to ensure uninterrupted operations for remote worker and customer engagement needs. While security was already top of mind for most IT leaders (cybercrime increased by 63% since Covid per Security Magazine), the highly sophisticated supply chain compromise of the SolarWinds Orion portfolio escalated secure operations to the top priority.

So what happened? The SolarWinds Orion update servers were compromised, allowing a bad actor to insert a trojan horse-style malware (called SunBurst) into signed Orion updates. Customer downloads of the affected code allowed the third-party to control the updated server, allowing them to access additional information and systems. While this particular attack appears to have been specific to the SolarWinds Orion portfolio, it serves as a critical reminder that we have a sacred duty to our customers and employees – to ensure to the greatest extent possible that our software and systems are hardened against these kinds of attacks and do not serve as a vector to compromise their data, systems, and networks. While ScienceLogic was not directly affected by this event, we are doing everything we can to protect our customers and our business from similar attacks.

Impact on ScienceLogic Customers

The ScienceLogic Security team continually monitors and evaluates security risks reported in the industry and the news. We took immediate action to confirm that the safety of the ScienceLogic systems and code from the SL1 application have not been impacted by the SunBurst malware directly or indirectly or via the SolarWinds breach. We have found no evidence that our internal systems have been affected in any way. We do not use the SolarWinds Orion and FireEye security software (FireEye is an Orion user) in our systems. We are continuously monitoring our environment and have found no signs of SunBurst and other malware. Further, every vendor in the ScienceLogic supply chain has confirmed no impact to their systems and software from this attack. We've also taken the extra precaution of confirming that all possible patches and security protocols are in place to protect against the stolen FireEye hacking tools.

A History of Building Customer Relationships with Trust

ScienceLogic prides itself with building strategic customer partnerships over the last 20 years to deliver highly scalable, reliable, and secure solutions that meet their ongoing customer-centric operational needs. To retain this customer trust, ScienceLogic remains vigilant and committed to updating and validating our security posture and protocols to assist our customers and partners in their response.

Application	• Software development security practices include OWASP Top 10, annual developer training, peer code-reviews, multiple gate-checks for code release • Inclusion of security considerations in product design phase • Major software versions verified for compliance with security posture • Customers regularly engaged to update security certificates (e.g., SSL)
Users	• User logins protected by multi-factor authentication • Configurable password requirements, SSO, and granular role-based access align with corporate policies for each customer
Data	• Data collection and transmission from SL1 Agents, SL1 Collectors, or via platform integrations secured with white-listing, SSH tunnels, PhoneHome methods, and 'Least Privileged' access to each customer environment • Stored data protected with AES encryption • Data Communications protected via Transport Layer Security (TLS)

Architecture/ SaaS	• Hosting environments available via ScienceLogic or partners certified for ISO 27001, PCI/DSS Service Provider Level 1, and strict Federal and Defense requirements (FISMA Moderate level, DIACAP, FedRAMP) • On-going third-party penetration testing
Corporate	• Annual employee security training with quarterly boosters and spot-training as needed • Employee background checks and secure remote access via VPN
Physical	• Security cameras at every entry/exit point and sensitive areas on ScienceLogic premises • Badged employee access, badge must be displayed at all times • Visitors must be escorted by employees at all times
Supply Chain	• Detailed security assessments conducted during purchase • Ongoing annual vendor security reviews
Compliance and Privacy	• First end-to-end IT infrastructure monitoring solution named on the U.S. Dept. of Defense Information Network Approved Products List (DoDIN APL) • Each major software version certified for DoDIN APL, SOC2, and GDPR
Continuous Evaluation	• On-going vulnerability scans (e.g., external penetration testing, employee access, code checks) of our development tools, environments and security protocols

An Increased Commitment to Retain Customer's Trust

While ScienceLogic was not impacted by this attack, events like these behoove us to re-examine our security posture and protocols thoroughly to ensure that we're leaving no stones unturned when it comes to securing our systems and our customer's data. In addition to firing-up an internal tiger team to rapidly harden the *existing multi-pronged and robust security plan*, ScienceLogic maintains security as a top strategic priority through various initiatives:

Secure-By-Default
- Extend DoD practices and secure default configurations to all software versions as applicable

Secure Development Practices
- Add additional developer security training
- Add additional code vulnerability analytics tools and code release gate-checks

Harden Internal Systems
- Enhance surveillance with added security cameras
- Enhance new hire background checks with terror list cross-check

Fortify Supply Chain
- Evaluate vendor's supply chain in annual security reviews

A Pathway to Keep Your IT Transformation on Track

Digital transformations are hard enough. And disruptive Cyberattacks are the new norm. As you address your most critical security issues, you should not have to worry about the security gaps in your supply chain. ScienceLogic helps you lay the foundation for your digital transformations with its secure, scalable, reliable, and future-proof I&O platform. Augment your security efforts by first gaining visibility into your end-to-end service landscape, including critical business services, applications, and infrastructure. Next, free-up critical resources to focus on security and other high-priority efforts by automating mundane incident management tasks. And finally, leverage AI/ML to drive intelligent workflow automations to further reduce human error, or worse, the security risks associated with manual and non-standardized workflows. Let ScienceLogic pave your secure way to AIOps.