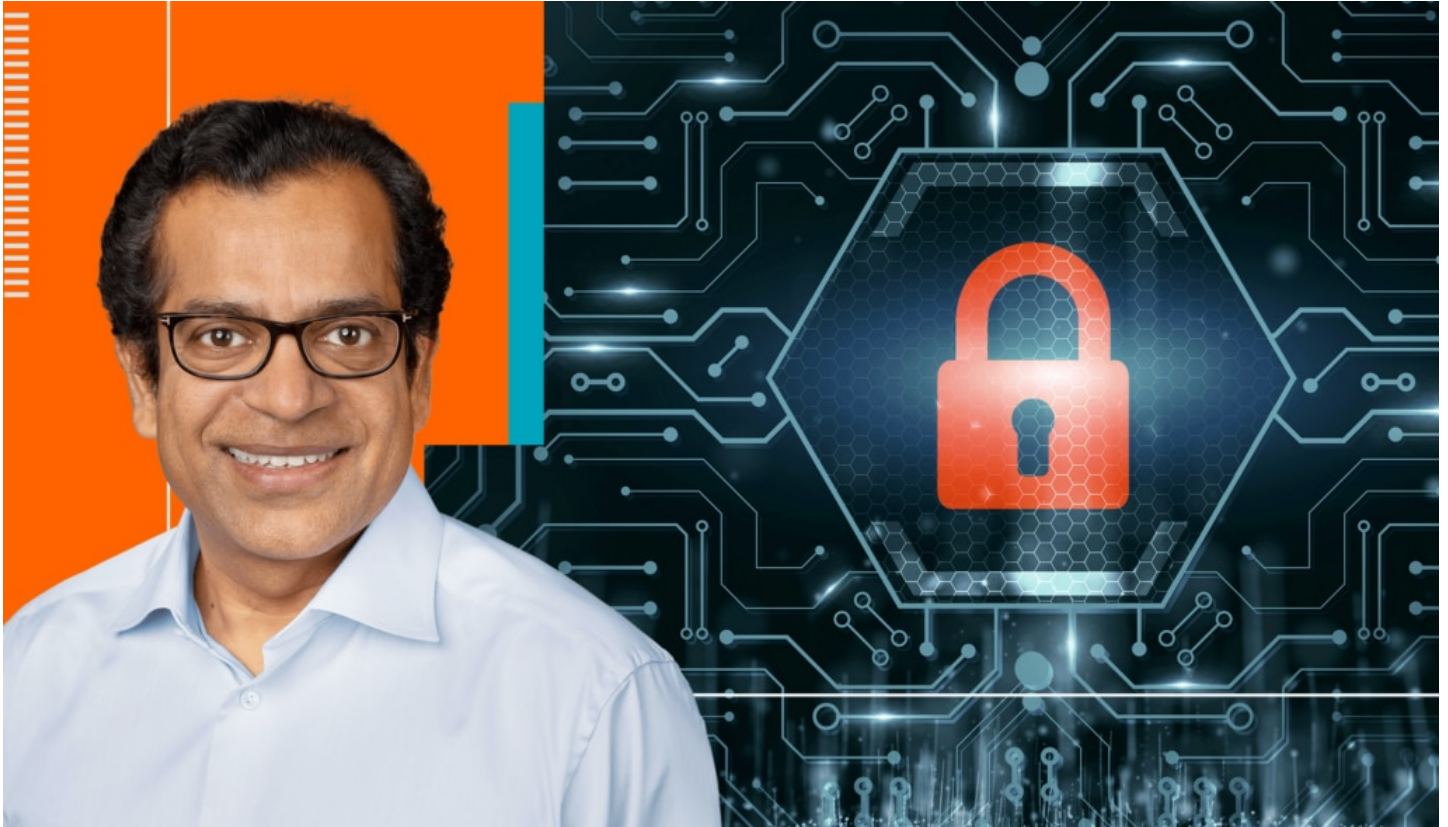


# Transparency, Information-Sharing, and Collaboration Make the Software Industry More Secure. We Must Not Risk Our Progress.


By Sudhakar Ramakrishna (<https://orangematter.solarwinds.com/author/sudhakar-ramakrishna/>)

October 30, 2023 | SolarWinds News (<https://orangematter.solarwinds.com/category/solarwinds-news/>)



Soon after the highly sophisticated Russian cyberattack on SolarWinds and other technology companies was discovered in December 2020, the U.S. government and the security community determined it was carried out by persistent Russian threat actors. SUNBURST used novel techniques the world's best cybersecurity experts had never seen before.

Since SUNBURST, there have been several reports of successful, highly resourceful, and capable technology companies—and even federal agencies—falling victim to nation-state cyberattacks, further illustrating that no one is immune to the new, advanced threats that have unfortunately become commonplace. As we practice and advocate, a community vigil is the only way to improve our collective security. It is imperative for victims of cyberattacks to come forward and share their experiences for the benefit of the broader community—and it is imperative these victims not be further victimized.

When I joined SolarWinds just days after the company learned of SUNBURST, my immediate focus was supporting our customers as we quickly contained, remediated, and eradicated the issue—while helping our customers ensure their environments were secure. We shared information about the  incident as it was confirmed. The transparency of our response and our ongoing commitment to

public-private partnerships has been widely praised in the global IT and security communities. We defined and implemented our Secure by Design (<https://orangematter.solarwinds.com/2021/02/03/continuing-our-journey-to-becoming-secure-by-design/>) initiative and have been commended broadly for advancing cybersecurity.

How we responded to SUNBURST is exactly what the U.S. government seeks to encourage. So, it is alarming that the Securities and Exchange Commission (SEC) has now filed what we believe is a misguided and improper enforcement action against us, representing a regressive set of views and actions inconsistent with the progress the industry needs to make and the government encourages.

The truth of the matter is that SolarWinds maintained appropriate cybersecurity controls prior to SUNBURST and has led the way ever since in continuously improving enterprise software security based on evolving industry standards and increasingly advanced cybersecurity threats. For these reasons, we will vigorously oppose this action by the SEC.

Our commitment to transparent communication has extended beyond customers to the entire industry and our government partners. We made a deliberate choice to speak—candidly and frequently—with the goal of sharing what we learned to help others become more secure. We partnered closely with the government and encouraged other companies to be more open about security by sharing information and best practices. We have advocated strongly for robust public-private partnerships to prevent future nation-state attacks. As a result of our efforts, the industry has made considerable progress in this regard since SUNBURST. Fierce business competitors now understand the need to be cooperative partners focused on defending our nation's cyberinfrastructure against new and constantly changing attacks.


The SEC's charges now risk the open information-sharing across the industry that cybersecurity experts agree is needed for our collective security. They also risk disenfranchising earnest cybersecurity professionals across the country, taking these cyber warriors off the front lines. I worry these actions will stunt the growth of public-private partnerships and broader information-sharing, making us all even more vulnerable to security attacks.

The actions we have taken over the last two and half years motivate us to stay the course and to push back against any efforts that will make our customers and our industry less secure. We will continue to move forward guided by our fundamental principles of transparency, urgency, collaboration, communication, and humility.

---

## ADDITIONAL RESOURCES

### ***SUNBURST investigation updates:***

- Orange Matter Blog (December 17, 2020): <https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-security-vulnerability/> (<https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-security-vulnerability/>)
- Orange Matter Blog (January 11, 2021): <https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/> 

(<https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/>)

- Orange Matter Blog (May 7, 2021): <https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/>

### **Secure by Design resources:**

- SolarWinds Secure by Design resource center: <https://www.solarwinds.com/secure-by-design-resources> (<https://www.solarwinds.com/secure-by-design-resources>)
- SolarWinds Day virtual event with CISA and Congressional Representatives (June 28, 2023): [https://www.youtube.com/watch?reload=9&v=Ak6RX\\_cX4Qo](https://www.youtube.com/watch?reload=9&v=Ak6RX_cX4Qo) ([https://www.youtube.com/watch?reload=9&v=Ak6RX\\_cX4Qo](https://www.youtube.com/watch?reload=9&v=Ak6RX_cX4Qo))
- SolarWinds Aims to Set New Standard in Software Development With Next-Generation Build System: <https://orangematter.solarwinds.com/2022/03/10/setting-the-new-standard-in-secure-software-development/> (<https://orangematter.solarwinds.com/2022/03/10/setting-the-new-standard-in-secure-software-development/>)

*This Blog Post contains "forward-looking" statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, including statements regarding the recent enforcement action filed by the Securities and Exchange Commission against SolarWinds relating to the 2020 cyberattack (the "Cyber Incident"). The information in this Blog Post is based on management's beliefs and assumptions and on information currently available to management. Forward-looking statements include all statements that are not historical facts and may be identified by terms such as "aim," "anticipate," "believe," "can," "could," "seek," "should," "feel," "expect," "will," "would," "plan," "intend," "estimate," "continue," "may," or similar expressions and the negatives of those terms. Forward-looking statements involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to be materially different from any future results, performance, or achievements expressed or implied by the forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to risks related to the Cyber Incident, including with respect to (a) numerous financial, legal, reputational and other risks to us related to the Cyber Incident, including risks that the incident, SolarWinds' response thereto or litigation and investigations related to the Cyber Incident may result in the loss of business as a result of termination or non-renewal of agreements or reduced purchases or upgrades of our products, reputational damage adversely affecting customer, partner and vendor relationships and investor confidence, increased attrition of personnel and distraction of key and other personnel, indemnity obligations, damages for contractual breach, penalties for violation of applicable laws or regulations, significant costs for remediation and the incurrence of other liabilities, and risks related to the impact of any such costs and liabilities resulting from the exhaustion of our insurance coverage related to the Cyber Incident, (b) litigation and investigation risks related to the Cyber Incident, including as a result of the civil complaint recently filed by the Securities and Exchange Commission against us and our current Chief Information Security Officer relating to the previously disclosed Wells Notices, including that we may incur significant costs in defending ourselves and may be unsuccessful in doing so, resulting in exposure to potential penalties, judgements, fines, settlement-related costs and penalties and other costs and liabilities related thereto, and (c) the possibility that our steps to secure our internal environment, improve our product development environment and ensure the security and integrity of the software that we deliver to our customers may not be successful or sufficient to protect against future threat actors or attacks or be perceived by existing and prospective customers as sufficient to address the harm caused by the Cyber Incident, and (d) such other risks and uncertainties described more fully in documents filed with or furnished to the U.S. Securities and Exchange Commission by SolarWinds, including the risk factors discussed in SolarWinds' Annual Report on Form 10-K for the year ended December 31, 2022 filed on February 22, 2023, SolarWinds' Quarterly Report on Form 10-Q for the quarter ended March 31, 2023 filed on May 4, 2023, SolarWinds' Quarterly Report on Form 10-Q for the quarter ended June 30, 2023 filed on August 9, 2023 and SolarWinds' Quarterly Report on Form 10-Q for the quarter ended September 30, 2023 that SolarWinds anticipates filing on or before November 9, 2023. All information provided in this Blog Post is as of the date hereof, and SolarWinds undertakes no duty to update this information except as required by law.*



(<http://www.facebook.com/share.php?u=https://orangematter.solarwinds.com/2023/10/30/transparency-information-sharing-and-collaboration/&title=Transparency,Information-Sharing, and Collaboration Make the Software Industry More Secure. We Must Not Risk Our Progress.>)

### **Share:**

information-sharing-and-collaboration/&title=Transparency, Information-Sharing, and Collaboration Make the Software Industry More Secure. We Must Not Risk Our Progress.)



(<http://twitter.com/home?status=Transparency,Information-Sharing, and Collaboration Make the Software Industry More Secure. We Must Not Risk Our Progress.>)

<https://orangematter.solarwinds.com/2023/10/30/transparency-information-sharing-and-collaboration/>)

### **Tags**



### **Sudhakar Ramakrishna**

(<https://orangematter.solarwinds.com/author/sudhakar-ramakrishna/>)

Sudhakar Ramakrishna joined SolarWinds as President and Chief Executive Officer in January 2021. He is a global technology leader with nearly 25 years of experience...

**Read more** (<https://orangematter.solarwinds.com/author/sudhakar-ramakrishna/>)

