

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

_____ )	
SECURITIES AND EXCHANGE COMMISSION, )	
)	
Plaintiff, )	Judge Paul A. Engelmayer
)	
v. )	Civil Action No. 23-cv-9518-PAE
)	
SOLARWINDS CORP. and TIMOTHY G. )	
BROWN, )	
)	
Defendants. )	
_____ )	

**PLAINTIFF SECURITIES AND EXCHANGE COMMISSION’S MEMORANDUM IN  
SUPPORT OF MOTION FOR ISSUANCE OF LETTER OF REQUEST FOR  
INTERNATIONAL JUDICIAL ASSISTANCE**

Plaintiff Securities and Exchange Commission (the “Commission”) respectfully submits this Memorandum in support of its Motion for Issuance of a Letter of Request pursuant to the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (“Hague Evidence Convention”).

As the Court is aware, this is a securities fraud action in which the SEC alleges that from at least October 2018 through at least December 2020 (the “Relevant Period”), SolarWinds and its then-Vice President of Security and Architecture, Tim Brown (collectively “Defendants”), claimed in its Security Statement, which was publicly posted on SolarWinds’ website, that SolarWinds employed specific cybersecurity practices such as granting access to computer systems on a “least privilege necessary basis.” Amended Complaint at ¶ 181. But internally Defendants recognized and documented the Company’s long-standing, pervasive, and material cybersecurity deficiencies, including that the Company failed to follow the “least privilege

necessary” practice because it had widespread access control problems (including granting elevated permissions to “non-privileged users”) and had determined that, “[a]ccess and privilege to critical systems/data is inappropriate.” *See* Amended Complaint at ¶¶ 182, 192. Through these statements, and an overall scheme to portray SolarWinds as having a stronger cybersecurity posture than it did, SolarWinds and Brown misled the investing public.

The Commission now seeks testimony pursuant to Chapter I of the Hague Evidence Convention from a foreign witness located in the Czech Republic, Robert Krajčír.

During the Relevant Period, Mr. Krajčír was an engineer at SolarWinds with responsibility for managing the company’s corporate network infrastructure. He is referred to in the Amended Complaint as Network Engineer D. Mr. Krajčír, who the Commission interviewed during the investigation from which this litigation arose, is likely to have knowledge of the state of cybersecurity at the company, including in particular concerns he raised regarding a certain network vulnerability involving the ability of unmanaged devices to access to the company’s virtual private network (“VPN”). Mr. Krajčír referred to this vulnerability as a “security gap,” which remained unaddressed by the company over an extended period of time despite repeated attempts by Mr. Krajčír to escalate the gap internally.

While Mr. Krajčír is a former SolarWinds employee, he is represented by counsel for SolarWinds in this litigation. The Commission has offered to organize alternative locations for the proposed depositions of Mr. Krajčír that would not require the issuance of a letter of request, however the witness, through counsel, has expressed an unwillingness to travel outside of the Czech Republic (either to the United States or to another country such as Germany or the United Kingdom) for this purpose, or to voluntarily appear for a deposition at the U.S. Embassy in the Czech Republic for a deposition. Relevant Czech law prohibits the SEC from taking depositions

in Czechia unless it is at the U.S. Embassy or pursuant to an officially approved request (such as the one sought by this motion.).

## ARGUMENT

### **I. This Court Has the Authority to Issue the Letter of Request.**

Congress authorized this Court to issue Letters of Request for testimony from non-parties located in foreign countries for use in an action brought in the United States. *See* 28 U.S.C. § 1781(b)(2) (permitting “the transmittal of a letter rogatory or request directly from a tribunal in the United States to the foreign or international tribunal, officer, or agency to whom it is addressed and its return in the same manner”).

The Czech Republic and the United States are signatories to the Hague Evidence Convention. *See Status Table, Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, Hague Conference on Private Int’l Law, <https://www.hcch.net/en/instruments/conventions/status-table/?cid=82>; *Hague Evidence Convention Acceptances of Accessions*, Hague Conference on Private Int’l Law, <https://assets.hcch.net/docs/f094fd72-6213-4950-96ea-955f41a311eb.pdf> (last updated September 9, 2024). Pursuant to the Hague Evidence Convention, “[i]n civil or commercial matters a judicial authority of a Contracting State may, in accordance with the provision of the law of that State, request the competent authority of another Contracting State, by means of a Letter of Request, to obtain evidence, or to perform some other judicial act.” Hague Evidence Convention, Art. 1, Mar. 18, 1970, 23 U.S.T. 2555. The U.S. Supreme Court recognized that the Hague Evidence Convention is “intended to establish optional procedures that would facilitate the taking of evidence abroad.” *See Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522, 538 (1987).

## II. The Request is Relevant and Likely to Lead to Material Evidence.

“The decision of whether to issue letters rogatory is within the discretion of the court.” *SEC v. Rayat*, No. 21-CV-4777, 2023 WL 1861498, at \*3 (S.D.N.Y. Feb. 9, 2023) (quoting *Pearlstein v. BlackBerry Ltd.*, 332 F.R.D. 117, 120 (S.D.N.Y. 2019)). In deciding whether to issue Letters of Request, “courts apply the principles of Federal Rule of Civil Procedure 26.” *Lovati v. Petroleos De Venezuela, S.A.*, No. 19-CV-4799, 2022 WL 1416646, at \*1 (S.D.N.Y. May 5, 2022) (quoting *Nespresso USA, Inc. v. Williams-Sonoma, Inc.*, No. 19-CV-4223, 2021 WL 942736, at \*2 (S.D.N.Y. Mar. 12, 2021)); *see also Villella v. Chem. & Mining Co. of Chile Inc.*, No. 15-CV-2106, 2018 WL 2958361, at \*3 (S.D.N.Y. June 13, 2018). Federal Rule of Civil Procedure 26(b)(1) permits parties to “obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case,” and such material need not be admissible. Fed. R. Civ. P. 26(b)(1). “Courts routinely issue such letters where the movant makes a reasonable showing that the evidence sought may be material or may lead to the discovery of material evidence.” *Netherby Ltd. v. Jones Apparel Grp., Inc.*, No. 04-CV-7028, 2005 WL 1214345, at \*1 (S.D.N.Y. May 18, 2005).

The Rule 26 relevance and proportionality standard is easily met here. As summarized above, the witness in the Czech Republic could provide testimony regarding the key factual dispute remaining in this litigation, which is the actual state of SolarWinds’ cybersecurity during the Relevant Period. This includes Mr. Krajčír’s expected testimony regarding his efforts to analyze and document cybersecurity vulnerabilities including a known “security gap” involving the company’s VPN and concerns raised by Mr. Krajčír regarding the “basically unlimited” extent of “user admin rights” for employees at SolarWinds.

### III. Comity Considerations Favor Issuing the Letter of Request.

When considering whether to authorize international discovery through the Hague Evidence Convention, courts in this District consider international comity concerns. *See Lantheus Med. Imaging, Inc.*, 841 F. Supp. 2d 769, at 791-92 (S.D.N.Y. 2012) (considering comity issues raised by motion for issuance of letters rogatory). Courts generally apply the following comity factors detailed by the U.S. Supreme Court to determine whether to grant a request for issuance of a Letter of Request:

(1) the importance to the litigation of the documents requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

*Société Nationale Industrielle Aérospatiale*, 482 U.S. at 544 n.28. However, “some of the international comity concerns noted by the Court [in *Aérospatiale*] are lessened when only use of the Hague Convention is at issue because all the relevant nations have consented to the treaty process.” *Jaguar Land Rover Ltd. v. DR. Ing. H.C.F. Porsche AG*, No. 21-mc-62, 2021 WL 3075698, \*2 (D.D.C. June 22, 2021) (quoting *Arcelik A.S. v. E.I. DuPont de Nemours and Co.*, 856 Fed.Appx. 392, 399 (3d Cir. 2021)). “Courts should accordingly focus primarily on the first three comity factors.” *Id.* (citing the Restatement (Third) of Foreign Relations Law § 473 reps. n. 5).

Here, these factors support issuing the Letter of Request for the testimony of Mr. Krajčír. *First*, the Commission is seeking the testimony of a key engineer with direct knowledge of matters that are highly important to the Commission’s claims in this litigation. *Second*, as set forth in the attached Letter of Request and its attachments, the testimonial request is narrow,

specific, and targeted to the key remaining areas of factual dispute in this case. *Third*, the witness is located outside of the United States and the unique testimony he may provide and information he possesses “originates” outside the United States and cannot be found in this country. Despite efforts by counsel for the Commission to pursue more efficient means of obtaining the requested testimony, the witness through counsel has refused to travel outside of the Czech Republic, even though he is represented by the same counsel as the Defendants, thus necessitating this motion.

Accordingly, comity considerations favor issuing the Letter of Request to obtain limited testimony from the identified witness.

\* \* \*

For the foregoing reasons, the Commission respectfully requests that the Court grant this motion and execute the attached Letter of Request.

Dated: November 1, 2024

Respectfully submitted,

/s/ Christopher J. Carney

Christopher J. Carney

Christopher M. Bruckmann

(SDNY Bar No. CB-7317)

Kristen M. Warden

(admitted *pro hac vice*)

John J. Todor

(admitted *pro hac vice*)

William B. Ney

(admitted *pro hac vice*)

Benjamin Brutlag

(SDNY Bar No. BB-1196)

Lory Stone

(admitted *pro hac vice*)

Securities and Exchange Commission

100 F Street, NE

Washington, D.C. 20549

202-551-2379 (Carney)

202-551-5986 (Bruckmann)

202-551-4661 (Warden)

202-551-5381 (Todor)

202-551-5317 (Ney)

202-551-2421 (Brutlag)

202-551-4931 (Stone)

CarneyC@sec.gov

BruckmannC@sec.gov

WardenK@sec.gov

TodorJ@sec.gov

NeyW@sec.gov

BrutlagB@sec.gov

StoneL@sec.gov

*Attorneys for Plaintiff*

*Securities and Exchange Commission*

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

_____ )	
SECURITIES AND EXCHANGE COMMISSION, )	
)	
Plaintiff, )	Judge Paul A. Engelmayer
)	
v. )	Civil Action No. 23-cv-9518
)	
SOLARWINDS CORP. and TIMOTHY G. )	
BROWN, )	
)	
Defendants. )	
_____ )	

**LETTER OF REQUEST FOR INTERNATIONAL JUDICIAL ASSISTANCE  
PURSUANT TO THE HAGUE CONVENTION OF 18 MARCH 1970 ON THE TAKING  
OF EVIDENCE ABROAD IN CIVIL OR COMMERCIAL MATTERS**

The United States District Court for the Southern District of New York (“District Court”) presents its salutations to the Ministry of Justice of the Czech Republic, and requests assistance in obtaining testimony in conformity with Chapter I of the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (“Hague Evidence Convention”), to which both the United States and the Czech Republic are Contracting Parties. See Hague Conference on Private International Law, *Status Table for the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, available at <https://www.hcch.net/en/instruments/conventions/status-table/?cid=82> (last visited Aug. 16, 2024).

Specifically, the District Court requests assistance in obtaining oral testimony from Robert Krajčír, a citizen of the Slovak Republic residing in the Czech Republic, for use at trial. Mr. Krajčír is represented by counsel for defendant SolarWinds Corporation, where Mr. Krajčír is a former employee.



**SECTION I**

**1. SENDER:**

The Honorable Paul A. Engelmayer  
Judge for the United States District Court for the Southern District of New York  
Thurgood Marshall  
United States Courthouse  
40 Foley Square  
New York, NY 10007  
Tel: (212) 805-0268  
Email: engelmayernysdchambers@nysd.uscourts.gov

**2. CENTRAL AUTHORITY OF REQUESTED STATE:**

Ministry of Justice of the Czech Republic  
Vyšehradská 16  
128 10 Praha 2  
Czech Republic  
Tel: +420 221 997 925  
Fax: +420 224 919 919  
Email: [moc@msp.justice.cz](mailto:moc@msp.justice.cz)

**3. PERSON TO WHOM THE EXECUTED REQUEST IS TO BE RETURNED:**

The Honorable Paul A. Engelmayer  
Judge for the United States District Court for the Southern District of New York  
Thurgood Marshall  
United States Courthouse  
40 Foley Square  
New York, NY 10007  
Tel: (212) 805-0268  
Email: engelmayernysdchambers@nysd.uscourts.gov

*With a Copy to the Parties' Legal Representatives:*

**a. Plaintiff:**

United States Securities and Exchange Commission  
c/o Christopher Bruckmann, Esq.  
100 F Street NE  
Washington, D.C. 20549  
Tel: +1 202 551 5986  
Email: [bruckmannc@sec.gov](mailto:bruckmannc@sec.gov)

**b. Defendants:**

SolarWinds Corporation  
c/o Serrin Turner, Esq.  
Latham & Watkins LLP  
1271 Avenue of the Americas  
New York, NY 10020  
Tel: +1 212 906 1330  
Email: [serrin.turner@lw.com](mailto:serrin.turner@lw.com)

Timothy G. Brown  
c/o Alec Koch, Esq.  
King & Spalding LLP  
1700 Pennsylvania Avenue, NW  
Suite 900  
Washington, D.C. 20006  
Tel: +1 202 626 8982  
Email: [akoch@kslaw.com](mailto:akoch@kslaw.com)

**4. SPECIFICATION OF THE DATE BY WHICH THE REQUESTING AUTHORITY REQUIRES RECEIPT OF THE RESPONSE TO THE LETTER OF REQUEST.**

The Requesting Judicial Authority would greatly appreciate a response to the Request for International Judicial Assistance within 60 days or as soon as is practicable. This is to ensure that the requested testimony is received in a timely manner for use at trial in the civil proceedings described below and that trial counsel has sufficient time to utilize information obtained in preparation of their respective cases. Although the trial date is not currently scheduled, it is expected to take place in 2025 and the Parties will be able to take overseas depositions up until fourteen days before trial begins.

**SECTION II**

In conformity with Article 3 of the Hague Evidence Convention, the undersigned applicant has the honor to submit the following judicial information regarding the instant request:

**5. a. REQUESTING JUDICIAL AUTHORITY (Article 3(a))**

The Honorable Paul A. Engelmayer  
Judge for the United States District Court for the Southern District of New York  
Thurgood Marshall  
United States Courthouse  
40 Foley Square  
New York, NY 10007  
Tel: (212) 805-0268  
Email: engelmayer@nysd.uscourts.gov

**b. TO THE COMPETENT AUTHORITY OF THE CZECH REPUBLIC  
(Article 3(a)):**

Ministry of Justice of the Czech Republic  
Vyšehradská 16  
128 10 Praha 2  
Czech Republic  
Tel: +420 221 997 925  
Fax: +420 224 919 919  
Email: [moc@msp.justice.cz](mailto:moc@msp.justice.cz)

**c. NAME OF THE CASE AND ANY IDENTIFYING NUMBER**

*Securities and Exchange Commission v. SolarWinds Corporation and Timothy G. Brown*,  
No. 1:23-cv-9518 (PAE), United States District Court for the Southern District of New York,  
USA

**6. NAMES AND ADDRESSES OF THE PARTIES AND THEIR  
REPRESENTATIVES (Article 3(b)):**

**a. Plaintiff:**

United States Securities and Exchange Commission  
c/o Christopher Bruckmann, Esq.  
100 F Street NE  
Washington, D.C. 20549  
Tel: +1 202 551 5986  
Email: [bruckmann@sec.gov](mailto:bruckmann@sec.gov)

**b. Defendants:**

SolarWinds Corporation  
c/o Serrin Turner, Esq.  
Latham & Watkins LLP  
1271 Avenue of the Americas

New York, NY 10020  
Tel: +1 212 906 1330  
Email: [serrin.turner@lw.com](mailto:serrin.turner@lw.com)

Timothy G. Brown  
c/o Alec Koch, Esq.  
King & Spalding LLP  
1700 Pennsylvania Avenue, NW  
Suite 900  
Washington, D.C. 20006  
Tel: +1 202 626 8982  
Email: [akoch@kslaw.com](mailto:akoch@kslaw.com)

**7. NATURE AND PURPOSE OF THE PROCEEDINGS AND SUMMARY OF THE FACTS (Article 3(c)):**

**a. Nature of the proceedings**

The above-captioned proceeding is a **civil** case brought by the United States Securities and Exchange Commission (“SEC”)—an independent agency of the United States government responsible for enforcing U.S. federal securities laws—against SolarWinds Corporation (“SolarWinds” or the “company”) and Timothy G. Brown (“Brown”) in a Complaint filed on October 30, 2023, which was amended on February 16, 2024 (the “Amended Complaint”).

The SEC’s Amended Complaint alleges that from at least October 2018 through at least December 2020, SolarWinds and its then-Vice President of Security and Architecture, Brown, claimed in its Security Statement, which was publicly posted on SolarWinds’ website, that SolarWinds employed specific cybersecurity practices such as granting access to computer systems on a “least privilege necessary basis.” Amended Complaint at ¶ 181. But internally they recognized and documented the Company’s long-standing, pervasive, and material cybersecurity deficiencies, including that the Company failed to follow the “least privilege necessary” practice because it had widespread access control problems (including granting elevated permissions to “non-privileged users”) and had determined that, “[a]ccess and privilege

to critical systems/data is inappropriate.” *See* Amended Complaint at ¶¶ 182, 192. Through these statements, and an overall scheme to portray SolarWinds as having a stronger cybersecurity posture than it did, SolarWinds and Brown misled the investing public.

Based on these actions, and as relevant here, the SEC alleges in its Amended Complaint that the Defendants violated the **civil** antifraud provisions of multiple U.S. federal laws, including 15 U.S.C. §§ 77q(a), 78j(b) and 17 C.F.R. § 240.10b-5.<sup>1</sup> As remedies, the SEC seeks: (1) a permanent injunction prohibiting Defendants from violating these laws and prohibiting Brown from acting as an officer or director of any public company; (2) an order requiring Defendants to disgorge their ill-gotten gains, plus prejudgment interest; and (3) an order requiring Defendants to pay **civil** money penalties.

Under United States law, the **SEC** has the authority to act as a **civil plaintiff** to bring lawsuits in civil courts. *See* 15 U.S.C. §§ 77t(b), 78u(d)(1). The SEC brought the above-captioned proceeding under this authority and **the proceeding is** designated as a **civil case** by the United States District Court in which it was filed. This matter is **not an administrative proceeding**. The SEC is authorized to file a **civil** law action against a corporation or its officers (such as the defendants) in breach of federal laws requiring them to disgorge their ill-gotten gains, plus prejudgment interest and pay **civil** money penalties. This follows from 15 U.S.C. §§ 77t(b), 78u(d)(1).

Within the scope of this legislation and these remedies, the SEC brought the above captioned **civil** proceeding against the defendants in which the testimony of Mr. Krajčír is sought by this Letter of Request. The SEC may then petition the presiding court to distribute any funds

---

<sup>1</sup> These provisions are distinct from charges under the criminal securities fraud statute, 18 U.S.C. § 1348, which the SEC, as a **civil** law enforcement agency, cannot bring.

so retrieved among the aggrieved parties pursuant to the issuance of a final judgment. The final judgment may be issued after this proceeding is resolved either on the merits or pursuant to a negotiated settlement between the parties.

This is a **civil** matter pursuant to U.S. law and carries no potential for criminal liability for SolarWinds or Mr. Brown. As to how “civil or commercial” is to be defined within the context of the Hague Evidence Convention, the Practical Handbook on the Operation of the Evidence Convention clearly states that the term civil or commercial should be “interpreted in an autonomous manner,” without just referring to the law of the Requesting State or Requested State. Hague Conference on Private Int’l Law, *Practical Handbook on the Operation of the Evidence Convention* ¶ 50, at 21 (3d ed. 2016) (“Handbook”).<sup>2</sup> In addition, during the most recent Special Commission meeting convened in July 2024 by the Hague Conference on Private International Law for Contracting Parties to the Hague Evidence Convention, the Special Commission adopted Conclusions and Recommendations which specifically emphasized that the term “civil or commercial” is to be “interpreted in a broad, liberal and autonomous manner” and the focus should be on the “nature of the cause of action.”<sup>3</sup>

**8. DOCUMENTS TO BE OBTAINED OR OTHER JUDICIAL ACT TO BE PERFORMED (Article 3(d)):**

**a. Evidence to be obtained:**

The assistance requested of the Czech Republic consists of obtaining **oral testimony** from **a former SolarWinds network engineer, Robert Krajčír**, who resides and works in the

---

<sup>2</sup> The Handbook is a reliable source for interpretation and implementation questions related to the Hague Evidence Convention. It was drafted by the Permanent Bureau of the Hague Conference on Private International Law, reviewed by a Special Commission convened to review the practical operation of the Convention, and approved by the Council on General Affairs and Policy of the Hague Conference.

<sup>3</sup> Conclusions and Recommendations at p. 13, ¶¶ 122-23, SC 1965 Service & 1970 Evidence & 1980 Access to Justice, July 2024: <https://assets.hcch.net/docs/6aef5b3a-a02c-408f-8277-8c995d56f255.pdf>

**Czech Republic.** The Parties intend to elicit testimony from Mr. Krajčír on the questions contained in Attachment A and related questions. In addition, assistance is requested in the form of having Mr. Krajčír review and authenticate documents which are to be presented to him, attached to this Request as Attachment B.

Mr. Krajčír was an engineer at SolarWinds with responsibility for managing the company's corporate network infrastructure and is likely to have knowledge of the state of cybersecurity at the company, including concerns he raised regarding a certain network vulnerability involving the ability of unmanaged devices to access to the company's virtual private network ("VPN").

**b. Purpose of the testimony sought:**

The testimony sought in this Letter of Request pertains to the allegations described above and are to be used only in legal proceedings in the matter described. The information sought in this Request is relevant to the SEC's allegations as set forth above and in the Amended Complaint. The information sought in this Request is relevant to the SEC's allegations that Defendants misleadingly touted SolarWinds' cybersecurity practices and products, while at the same time understating the company's cybersecurity risks. As a network engineer at SolarWinds during the period relevant to the remaining claims at issue in the Amended Complaint, between 2018-2020, Mr. Krajčír has information relevant to the SEC's allegations as they relate to SolarWinds' corporate network infrastructure, known network vulnerabilities, and policies and practices that were inconsistent with SolarWinds' public statements regarding its cybersecurity practices.

**SECTION III**

**9. IDENTITY AND ADDRESS OF ANY PERSON TO BE EXAMINED (Article 3(e)):**

Mr. Robert Krajčír (former network engineer at SolarWinds):  
Rolnická 660/5, 625 00 Brno, Czech Republic  
Email: [krajcir.robo@gmail.com](mailto:krajcir.robo@gmail.com)

Mr. Krajčír is represented by counsel for SolarWinds:  
Serrin Turner, Esq.  
Latham & Watkins LLP  
1271 Avenue of the Americas  
New York, NY 10020  
Tel: +1 212 906 1330  
Email: [serrin.turner@lw.com](mailto:serrin.turner@lw.com)

**10. QUESTIONS TO BE PUT TO PERSONS TO BE EXAMINED OR STATEMENT OF THE SUBJECT MATTER ABOUT WHICH THEY ARE TO BE EXAMINED (Article 3(f)):**

The questions to be put to Mr. Krajčír relate to the subject matter described in Paragraph 8(b) above and the allegations in the Amended Complaint, in addition to questions relating to preliminary matters of witness knowledge and competence. The specific questions that the Parties seek to put to Mr. Krajčír are attached to this Request in Attachment A. We also request that Mr. Krajčír authenticate certain documents which are to be presented to him, attached to this Request as Attachment B. The Parties also request the ability to ask clarifying and follow-up questions of Mr. Krajčír as appropriate.

**11. DOCUMENTS OR OTHER PROPERTY TO BE INSPECTED**

None.

**12. ANY REQUIREMENT THAT THE EVIDENCE BE GIVEN ON OATH OR AFFIRMATION AND ANY SPECIFIC FORM TO BE USED (Article 3(h)):**

If agreeable to the Ministry of Justice of the Czech Republic, it is hereby requested as follows:



a. It is requested that the oral testimony of Mr. Krajčír be taken under oath or affirmation in accordance with the laws of the Czech Republic before an appropriate judicial official of the Czech Republic.

b. The SEC has authorized Lucie Oršulová (“Ms. Oršulová”), Partner at Bányaiová Vožehová, s.r.o., to represent its interests and serve as its counsel in the execution of this Request in the Czech Republic. Please contact Ms. Oršulová for any questions and notices regarding this Letter of Request. Please notify the Court that shall be designated to execute this Letter of Request that Ms. Oršulová shall represent the SEC in connection with any procedures, hearings, and motions that shall be taken and heard in connection with the examination of the witnesses. Ms. Oršulová’s contact information is:

Lucie Oršulová, Partner  
Bányaiová Vožehová, s.r.o.  
Lazarská 13/8 building B, 4th floor  
Prague 2 120 00, Czech Republic  
Tel: +420 602 655 590  
FAX: +420 222 517 088  
Email: [lucie.orsulova@bvlaw.cz](mailto:lucie.orsulova@bvlaw.cz)

c. It is requested that the oral testimony requested by the SEC be taken through questioning by counsel for the SEC in the Czech Republic, law offices of Bányaiová Vožehová, s.r.o. by partner Lucie Oršulová or her designee, with an opportunity afforded to counsel for Defendants to ask questions of Mr. Krajčír on the topics raised by the SEC’s questions.

d. It is requested that counsel for the SEC and counsel for Defendants be notified in advance of the time and place of the proceedings and that counsel be permitted to attend in person, or by video or audio teleconference for those not able to attend in person. Ms. Oršulová shall inform counsel for Defendants by email of the procedures to be followed in the proceeding,

including such arrangements as are necessary to attend in person or by video or audio teleconference.

e. It is further requested that the affirmation and oral examination be transcribed verbatim by a qualified stenographer and that the written transcript be provided to:

The Honorable Paul A. Engelmayer  
Judge for the United States District Court for the Southern District of New York  
Thurgood Marshall  
United States Courthouse  
40 Foley Square  
New York, NY 10007  
Email: [engelmayernysdchambers@nysd.uscourts.gov](mailto:engelmayernysdchambers@nysd.uscourts.gov)

*With a Copy to the Parties' Legal Representatives:*

United States Securities and Exchange Commission  
c/o Christopher Bruckmann, Esq.  
100 F Street NE  
Washington, D.C. 20549  
Tel: +1 202 551 5986  
Email: [bruckmann@sec.gov](mailto:bruckmann@sec.gov)

SolarWinds Corporation  
c/o Serrin Turner, Esq.  
Latham & Watkins LLP  
1271 Avenue of the Americas  
New York, NY 10020  
Tel: +1 212 906 1330  
Email: [serrin.turner@lw.com](mailto:serrin.turner@lw.com)

Timothy G. Brown  
c/o Alec Koch, Esq.  
King & Spalding LLP  
1700 Pennsylvania Avenue, NW  
Suite 900  
Washington, D.C. 20006  
Tel: +1 202 626 8982  
Email: [akoch@kslaw.com](mailto:akoch@kslaw.com)

f. It is further requested that, if any portion of this Request is deemed to be unacceptable under the laws of the Czech Republic, that counsel for the SEC, Mr. Bruckmann

and local counsel Ms. Oršulová, and counsel for Defendants, Mr. Turner and Mr. Koch, please be informed of that fact and be allowed to respond substantively prior to the decision and that the Ministry of Justice of the Czech Republic please comply with as much of the Request as possible.

**13. SPECIAL MEHODS OR PROCEDURES TO BE FOLLOWED (Article 3(i) & 9):**

Please see Paragraph 12, above.

**14. REQUEST FOR NOTIFICATION OF THE TIME AND PLACE FOR THE EXECUTION OF THE REQUEST AND IDENTITY AND ADDRESS OF ANY PERSON TO BE NOTIFIED (Article 7):**

It is requested that the execution of the Request be provided to the Parties' representatives identified in Paragraphs 6 and 12, above.

**15. REQUEST FOR ATTENDANCE OR PARTICIPATION OF JUDICIAL PERSONNEL OF THE REQUESTING AUTHORITY AT THE EXECUTION OF THE LETTER OF REQUEST (Article 8):**

None.

**16. SPECIFICATION OF PRIVILEGE OR DUTY TO REFUSE TO GIVE EVIDENCE UNDER THE LAW OF THE REQUESTING STATE (Article 11(b)):**

The Parties will not seek to elicit testimony from Mr. Krajčír that would disclose information protected by the attorney-client privilege or privileges applicable under the laws of the Czech Republic.

**17. THE FEES AND COSTS INCURRED WHICH ARE REIMBURSABLE UNDER THE SECOND PARAGRAPH OF ARTICLE 14 OR UNDER ARTICLE 26 OF THE CONVENTION WITH BE BORNE BY:**

This Court understands that certain fees and costs incurred in the execution of this Request may be reimbursable under the second paragraph of Article 14 or Article 26 of the Hague Evidence Convention. The fees and costs of this Hauge Evidence Convention process

will be borne by the SEC. Each of the SEC and Defendants will be responsible for the fees and expenses, if any, of its own attorneys relating to any proceedings arising from the Hague Evidence Convention process. The U.S. Government's local counsel, Ms. Oršulová, should be informed before any costs are incurred under Article 14 and 26 of the Hague Evidence Convention.

**SECTION IV**

This Court expresses its gratitude to the authorities of the Czech Republic for their assistance and courtesy under the terms of the Hague Evidence Convention.

Signature and Seal of the Requesting Judicial Authority:

Dated:

\_\_\_\_\_  
PAUL E. ENGELMAYER  
UNITED STATES DISTRICT JUDGE

**ATTACHMENT A**

**QUESTIONS TO BE PRESENTED TO ROBERT KRAJCIR**

**General Background Questions**

1. Please state and spell your full legal name for the record.
2. How old are you?
3. Where are you from?
4. Are you a citizen of Slovakia?
  - a. Are you a citizen of any other country?
5. Where do you currently reside?
6. What is your highest level of education?
7. Where did you attend university?
8. What did you study?
9. What was your first job after graduation?
  - a. What was your role?
  - b. How long did you work there?
10. Where were you next employed?
  - a. What was your role?
  - b. How long did you work there?
11. Did you at some point begin to work for SolarWinds Corporation? We will hereafter refer to SolarWinds Corporation as SolarWinds.
12. What were your dates of employment at SolarWinds?
  - a. What was your title?
  - b. Did your title change?

Attachment A – Questions to be Presented to Robert Krajcir

- c. Did you stay in the same role throughout your time at SolarWinds?
13. Who was your direct manager while you were at SolarWinds?
14. Did you manage any other employees while you were at SolarWinds?
- a. If so, who did you manage while you were at SolarWinds?
15. I refer you to the document marked as **Exhibit 1**.
- a. Do you recognize this exhibit?
  - b. Is it a copy of your LinkedIn profile?
  - c. Did you author this exhibit?
  - d. Is this exhibit accurate?
  - e. Under both “Network Engineer, Intermediate” and “Senior Network Engineer” at SolarWinds the document states that you “manag[ed] entire corporate network infrastructure (routers, switches, firewalls, wireless and more)”.
    - i. Describe each of the following terms and how they relate to SolarWinds’ corporate network infrastructure: (i) routers, (ii) switches, (iii) firewalls, and (iv) wireless.
    - ii. Describe your role in managing each of these elements of SolarWinds’ network infrastructure.
  - f. Under both “Network Engineer, Intermediate” and “Senior Network Engineer” at SolarWinds the document states that you “provid[ed] all tiers of support from monitoring (alert setup and tuning), through support (troubleshooting incidents, implementing changes), to complex design (new sites, acquisitions, office moves, feature requests and upgrades to existing environment)”.
    - i. Describe your role in providing each of these tiers of support.

Attachment A – Questions to be Presented to Robert Krajcir

- g. Under “Senior Network Engineer” at SolarWinds, the document states that you “provid[ed] reports to management.”
  - i. What areas did these reports relate to?
  - ii. Who did you provide these reports to?

**Questions Concerning the VPN Vulnerability**

- 16. Are you familiar with the term “unmanaged device”?
  - a. What does the term “unmanaged device” refer to?
- 17. Are you familiar with the term “VPN”?
  - a. What does the term “VPN” refer to?
- 18. Did you raise concerns about the security of VPN access at SolarWinds in 2018?
  - a. What was the concern?
  - b. Did that concern relate to the use of unmanaged devices at SolarWinds?
  - c. Was it a concern about the use of VPN generally, or about VPN access as it applied to SolarWinds, specifically?
- 19. I refer you to the document marked as **Exhibit 2**.
  - a. Do you recognize this document?
  - b. Did you send the e-mail on June 4, 2018?
  - c. Did you send the e-mail on June 5, 2018?
  - d. Did you send the e-mail on June 7, 2018?
  - e. Did you send the e-mail on August 24, 2018?
  - f. Did you send the e-mail on August 30, 2018?

Attachment A – Questions to be Presented to Robert Krajcir

- g. Did you author the PowerPoint attachment to this exhibit titled “BYOD solution, Machine certificate authentication?” I will refer to the PowerPoint as the “BYOD PowerPoint.”
- h. Did you attach the BYOD PowerPoint to the August 30, 2018 e-mail?
  - i. Were the concerns raised in the BYOD PowerPoint actual concerns that you had at the time you sent the presentation?
  - ii. Did anyone ever tell you that those were not valid concerns? Who? When?
- i. With respect to the June 4, 2018 e-mail:
  - i. Why did you send this e-mail?
  - ii. With respect to the following statements in the June 4, 2018, email:
    - 1. a “firewall cleanup and optimization.”
      - a. Describe what you meant by this.
    - 2. a “security gap we are facing”.
      - a. Describe what you meant by “security gap.”
      - b. When did you first notice the “security gap”?
    - 3. “It is not very secure for resources currently accessible via VPN and data stored there.”
      - a. What was “not very secure”?
      - b. What about it was not secure?
    - 4. “it is no problem for almost any user to download it” to any device, “without Netskope, proper Antivirus, security patches or updates, etc.”



Attachment A – Questions to be Presented to Robert Krajcir

- a. Was that true with VPN generally or was it specific to the VPN that SolarWinds used?
- iii. Did you propose a solution to the concern that you raised?
  1. What was the solution?
  2. You refer to “certificates for machine authentication.”
    - a. What does that mean?
    - b. How would “us[ing] certificates for machine authentication” resolve the security gap you identified?
- iv. What was needed to implement the solution you proposed?
  1. Would you describe this as an easy fix?
  2. You state that “there are no additional costs associated with implementing certificates.”
    - a. Was this accurate?
- v. At the end of your e-mail, you said that you reached out to the e-mail recipients because you wanted their “thoughts on the solution itself.”
  1. How did you select the recipients for this e-mail?
  2. Why did you want their thoughts in particular?
  3. What steps did you expect to be taken by SolarWinds?
- j. With respect to the June 5, 2018, e-mail:
  - i. Who is Joe Murray?
    1. What was his role at SolarWinds?
  - ii. Who is Eric Quitugua?
    1. What is his role at SolarWinds?

Attachment A – Questions to be Presented to Robert Krajcir

2. Why did you include him on these emails?
- iii. You state that “vendors, or non-domain computers in general should not have unrestricted access to our network”
  1. What is a “non-domain computer?”
  2. Is a “non-domain computer” an unmanaged device?
  3. Did “vendor, or non-domain computers” have unrestricted access to SolarWinds’ network?
- iv. You state that certain users without a “company-owned device.... Should have stricter policy and tier access should be limited.”
  1. What did you mean by this?
  2. Why was is important to impose a “stricter policy and tier access” for these users?
- v. You state that “there could be also separate groups for vendors, contractors, etc., depending on how many levels of restriction will be required.”
  1. Why was it important to create these separate groups?
- vi. Did you receive any other response to your June 4, 2018 proposal?
- vii. Did you meet any other resistance to your proposal?
- viii. Why do you think your proposal met with resistance?
- k. With respect to the August 24, 2018, e-mail:
  - i. You state “I’d like to drag your attention back to this topic.”
    1. How did SolarWinds respond to the potential VPN vulnerability you identified in June 2018?

Attachment A – Questions to be Presented to Robert Krajcir

2. Were any steps taken to remedy the VPN vulnerability between June and August 2018? If so, what were they?
- ii. You state that “implementing certificates is essential to enforce proper security policies.”
  1. Why did you say that?
  2. Would you describe the implementation of machine certificates to be an industry best practice? If so, why?
- iii. You state “We see every day, that people are accessing our corporate wifi with their smartphones or other devices that are not joined in the domain - this seems to be common practice!!!”
  1. How did you determine how individuals were accessing SolarWinds’ corporate Wi-Fi?
  2. What were the risks to SolarWinds associated with this practice?
- iv. You state that “I don’t want to look like panicking.”
  1. How serious to SolarWinds’ cybersecurity was the practice you described here?
  2. How urgent was it for SolarWinds to remedy the vulnerability that you identified in this e-mail?
- v. You state: “I’d like to schedule a call about this.”
  1. Was a call scheduled to discuss the vulnerability you identified in this e-mail?
  2. If yes, when did this call happen? How long did it last? Who attended the call?

Attachment A – Questions to be Presented to Robert Krajcir

1. With respect to the August 30, 2018, e-mail:
  - i. You state “thank you for coming and sharing your ideas on this topic. Please find attached the presentation I used today, so you can show it to anyone you deem appropriate.”
    1. Is this a reference to the call you proposed scheduling in your e-mail from August 24, 2018?
    2. If yes, when did this call happen? How long did it last? Who attended the call?
    3. What do you recall about that meeting?
    4. What issues were discussed during that meeting?
    5. Did you show the call attendees the BYOD PowerPoint?
  - ii. On Slides 3-4 of the BYOD PowerPoint, titled “Risks for the Company,” please detail each of the stated risks and their potential impacts on SolarWinds.
  - iii. On Slide 6 of the BYOD PowerPoint, there is a bullet point that says, “Manage user admin rights” and below it says, “At this time basically unlimited.”
    1. Did you have a concern about the extent of admin rights available to SolarWinds’ employees?
    2. Were user admin rights basically unlimited at that time?
    3. What did you mean by that?
    4. Did employees have admin rights who did not need them for their jobs?

Attachment A – Questions to be Presented to Robert Krajcir

5. How would you describe the extent of user access rights throughout SolarWinds’ at the time you gave this presentation?
6. Was that the case throughout your time at SolarWinds?
  - iv. Were there any subsequent calls or meetings to address the risks detailed in the BYOD PowerPoint?
20. Was there any follow-up discussion after August 2018 of the risks identified in the BYOD PowerPoint?
21. What steps did SolarWinds take to remedy the VPN vulnerability you identified in Exhibit 2?
22. Do you feel that SolarWinds properly addressed the concern you raised?
  - a. Why do you say that?
23. Did SolarWinds at any point restrict unmanaged devices from accessing the company’s VPN network?
  - a. If so, approximately when was that?
24. Were any individuals at SolarWinds beyond those to whom you sent the e-mails included in Exhibit 2 made aware of the VPN vulnerability discussed therein?
  - a. If so, who?
  - b. How do you know?
25. Did SolarWinds require Multi-Factor Authentication or “MFA” for access to its VPN network during your time at SolarWinds?

**General Questions Concerning the SolarWinds Security Statement**

26. Are you aware that SolarWinds published a Security Statement on its public website?
  - a. What is your understanding as to the purpose of the Security Statement?

Attachment A – Questions to be Presented to Robert Krajcir

- b. Was it used to describe SolarWinds’ cybersecurity practices?
27. I refer you to the document marked as **Exhibit 3**.
- a. Do you recognize the document, which is titled “SolarWinds Security Statement”?
  - b. Did you have any role in preparing this Security Statement?
    - i. If yes, describe your role and those of others who you may have worked with to prepare the Security Statement.
    - ii. If no, who prepared the Security Statement?
  - c. Did you have any role in disseminating the Security Statement?
    - i. If yes, describe your role and those of others who you may have worked with to disseminate the Security Statement.
    - ii. If no, who disseminated the Security Statement?
28. I refer you to the page marked Page 10 of Exhibit 3 and the heading titled “Operational Security.”
- a. Are you familiar with the concept of Change Management?
    - i. What is the Change Management?
  - b. Are you familiar with the concept of “Auditing and Logging”?
    - i. What is Auditing and Logging?
  - c. Are you familiar with the concept of Vulnerability Management?
    - i. What is Vulnerability Management?
  - d. Please review the language in Exhibit 3 under the heading titled “Operational Security.” This includes among others, the subheadings (i) “Change

Attachment A – Questions to be Presented to Robert Krajcir

Management,” (ii) “Auditing and Logging,” and (iii) “Vulnerability Management.”

- i. Based on your knowledge and experience working at SolarWinds, are the statements in Exhibit 3 under the heading titled “Operational Security” accurate?
- ii. If not, please explain in detail which of these statements are not accurate and why they are not accurate.

29. I refer you to the page marked Page 11 of Exhibit 3 and the heading titled “Access Controls.”

- a. Are you familiar with the concept of access controls?
- b. What are access controls?
- c. Would the concerns you expressed in Exhibit 2 fall under your understanding, generally, of access controls?
- d. Please review the language in Exhibit 3 under the heading titled “Access Controls.” This includes the subheadings (i) “Role Based Access” (which refers to access controls “set on a need-to-know / least privilege necessary basis”) and (ii) “Authentication and Authorization” (which addresses SolarWinds’ password policy).
  - i. Based on your knowledge and experience working at SolarWinds, are the statements in Exhibit 3 under the heading titled “Access Controls” accurate?
  - ii. If not, please explain in detail which of these statements are not accurate and why they are not accurate.

Attachment A – Questions to be Presented to Robert Krajcir

- iii. Would unlimited user admin rights throughout SolarWinds be inconsistent with the concept of granting access on a least-privilege basis?

30. Were you familiar with SolarWinds' password policy at the time that you worked at SolarWinds?

- a. I refer you to the page marked Page 11 of Exhibit 3 and the heading titled "Authentication and Authorization." It states: "Our password policy covers all applicable information systems, applications, and databases."
  - i. Were you aware of information systems, applications, or databases that were not compatible with SolarWinds' password policy during your time at SolarWinds?
    - 1. If yes, which systems?
  - ii. Were you aware of information systems, applications, or databases to which SolarWinds' password policy was not applied during your time at SolarWinds?
    - 1. If yes, which systems?
- b. That section goes on to state: "Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use passwords."
  - i. Were you aware of information systems that did not enforce SolarWinds' password requirements during your time at SolarWinds?
    - 1. If yes, which systems?
  - ii. Were you aware of information systems at SolarWinds that permitted the use of non-complex passwords during your time there?



Attachment A – Questions to be Presented to Robert Krajcir

1. If yes, which systems?
- iii. Were you aware of information systems that used the password “solarwinds123” during your time at SolarWinds?
  1. If yes, which systems?
- iv. Would you agree that “solarwinds123” was not a complex password?
- v. Were you aware of other non-complex passwords that were in use for any SolarWinds’ information systems, applications or databases?
  1. If yes, for which systems?
  2. What were the passwords?
- c. The statement goes on to say: “Passwords are individually salted and hashed.”

What does that mean?

- i. Were you aware of any information systems, applications, or databases at SolarWinds where individual passwords were not individually salted or hashed?
- ii. If yes, which systems?
- iii. Were you aware of instances at SolarWinds where database passwords were not encrypted within the configuration files?
  1. If yes, describe the instances.
  2. Would you agree that that is inconsistent with passwords being individually salted and hashed?
- iv. Were you aware of instances at SolarWinds where login credentials were stored in plain text in configuration files?
  1. If yes, describe the instances.

Attachment A – Questions to be Presented to Robert Krajcir

2. Would you agree that that is inconsistent with passwords being individually salted and hashed?
  - v. Were you aware of instances at SolarWinds where passwords were stored in plain text on the public web server in the web configuration file and in the system registry of the machine.
    1. If yes, describe the instances?
    2. Would you agree that that is inconsistent with passwords being individually salted and hashed?
31. I refer you to the page marked Page 11 of Exhibit 3 and the heading titled “Software Development Lifecycle.”
- a. Are you familiar with the concept of Software Development Lifecycle?
  - b. What is the Software Development Lifecycle?
  - c. Please review the language in Exhibit 3 under the heading titled “Software Development Lifecycle.”
    - i. Based on your knowledge and experience working at SolarWinds, are the statements in Exhibit 3 under the heading titled “Software Development Lifecycle” accurate?
    - ii. If not, please explain in detail which of these statements are not accurate and why they are not accurate.

**General Questions Concerning Cybersecurity**

32. Did you have any concerns about SolarWinds access controls other than those previously discussed today?
- a. If so, what were they?

Attachment A – Questions to be Presented to Robert Krajcir

33. Did you have any other concerns regarding cybersecurity at SolarWinds other than those previously discussed today?

a. If so, what were they?

34. During your time at SolarWinds, did the company dedicate sufficient resources to cybersecurity?

a. Why do you say that?

**ATTACHMENT B**

**DOCUMENTS TO BE PRESENTED TO ROBERT KRAJCIR**

**Exhibit 1**



**Róbert Krajčír**  
Network & Security Architect



Codasip



Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií

Brno, South Moravia, Czechia · [Contact info](#)

305 connections

[Connect](#) [Message](#) [More](#)

### About

Network architect and technician with hands-on experience with Cisco, Checkpoint, Palo Alto, VMware and F5 products since 2013, familiar with management of complex networks with various L2/L3 protocols (STP, OSPF, BGP) and services (VPN, wireless), focused on security, with project management (IPMA certified) skills. I love challenging work, learning new things and problem solving, as well as managing bigger projects that need involvement of more people, even other teams. I also have passion for automation (Python, PowerShell), programming (C, Java) and electronics. Even though I mostly thrive in designing new solutions and perfecting existing ones, no matter how complex, I also do a lot of things around budgeting and long term planning. People consider me a good team player, optimistic and playful person with good ideas, but also assertive, independent and decisive when needed. I have good presentation skills and I am able to interpret my ideas even to management which is not technical at all. What I can't stand however is an over-processed company where implementing any idea means bureaucracy that takes weeks or even months.

### Activity

312 followers

[Posts](#) [Comments](#) [Images](#)

Róbert Krajčír posted this • 5mo



After having opportunity to attend Cisco Live last year, I am lucky enough to visit yet another event organised by major player in my area of expertise. Looking forward to learn and g...

19

[Show all posts →](#)

## Experience



### Infrastructure Engineer

Codasip · Full-time  
Aug 2023 - Present · 1 yr 1 mo  
Brno, South Moravia, Czechia · On-site



### Network & Security Architect / Lead

RWS Group · Full-time  
Nov 2020 - Jul 2023 · 2 yrs 9 mos  
Brno, South Moravia, Czechia

Creating, maintaining and improving network architecture and security in all company locations to support company business strategy, responsible for network operations and further development/investments. Taking care of internal and external infrastructure, public and private clouds. Leading team of 6 engineers responsible for network and security infrastructure and related projects. Working here involves design, deployment and operations of advanced technologies following the latest trends in industry, such as:

- VMware NSX-T
- VMware NSX Advanced Load Balancer (formerly AVI)
- Infoblox DDI
- Cisco routing, switching, wireless (Catalyst, Nexus)
- Cisco ISE
- Cisco SDWAN (formerly Viptela)
- Check Point NGFW

Team I am leading is also involved with technologies such as PKS, Terraform, vCloud, Cisco email security, Trend Micro Apex One and many more.

My daily duties also involve coordination and evaluation of my team members, hiring process, budgeting/procurement, communicating with business and participating on major business-critical projects such as:

- migration to new O365 tenant
- large scale mergers/acquisitions and related WAN/security designs
- ITSM / CMDB implementation
- IP readdressing of entire sites
- office moves/closures

📄 Documentation, Architecture and +9 skills



### SolarWinds

Full-time · 3 yrs

#### • Senior Network Engineer

Aug 2020 - Oct 2020 · 3 mos  
Brno, South Moravia, Czech Republic

Managing entire corporate network infrastructure (routers, switches, firewalls, loadbalancers, wireless and more). Providing all tiers of support from monitoring (alert setup and tuning), through support (troubleshooting incidents, implementing changes) to complex design (new sites, acquisitions, office moves, feature requests and upgrades to existing environment) - includes travel several times a year as well. Responsible for budget planning and spending (i.e. site equipment refresh, implementing new technologies), including quotes for new devices and services. Providing reports to management, moderating team meetings and keeping overview of team goals and current project status.

📄 Documentation, Architecture and +1 skill

#### • Network Engineer, Intermediate

Nov 2017 - Jul 2020 · 2 yrs 9 mos  
District Brno-City, Czech Republic

Managing entire corporate network infrastructure (routers, switches, firewalls, loadbalancers, wireless and more). Providing all tiers of support from monitoring (alert setup and tuning), through support (troubleshooting incidents, implementing changes) to

complex design (new sites, acquisitions, office moves, feature requests and upgrades to existing environment) - includes travel several times a year as well. Responsible for budget planning and spending (i.e. site equipment refresh, implementing new technologies), including routes for new devices and services.

📌 Documentation and Packet Switching



**Tier 2 Network Specialist**

AT&T · Full-time  
May 2013 - Oct 2017 · 4 yrs 6 mos  
Okres Brno-město, Česká republika

Managing corporate networks of our customers, troubleshooting incidents. Cooperating with other teams within AT&T a ...see more

📌 Packet Switching



**Referee**

Západoslovenský futbalový zväz  
Jun 2011 - Jun 2014 · 3 yrs 1 mo

Show all 8 experiences →

**Education**



**Brno University of Technology**

Master's degree, Computer Systems Networking and Telecommunications  
2012 - 2014

Activities and societies: Studenti pro studenty, o.s., Cisco Networking Academy, e-fekt magazine

Master's thesis: Computer analysis of medical image data

📌 Packet Switching



**Brno University of Technology**

Bachelor's degree, Computer Systems Networking and Telecommunications  
2009 - 2012

Activities and societies: Studenti pro studenty, Hudba z FEKTu, Florbal VUT vs. MU, e-fekt magazine, Institute of Experimental...

Bachelor's thesis: Design of measurement net

📌 Packet Switching

**Licenses & certifications**



**ÖSD - Österreichisches Sprachdiplom Deutsch - B1**

Österreich Institut Brno  
Issued Feb 2020



**CCNA Security**

Cisco  
Issued Dec 2018 · Expired Dec 2021

Show all 7 licenses & certifications →

**Volunteering**



**Event creator**

Studenti pro Studenty  
Sep 2010 - Present · 14 yrs  
Social Services



Creating, organizing and co-organizing variety of cultural, sport, education and leisure activities for students. Example: Hudba z...

### Skills

#### Packet Switching

4 experiences across RWS Group and 2 other companies

2 educational experiences at Brno University of Technology

#### Technical Architecture

Network & Security Architect / Lead at RWS Group

Show all 33 skills →

### Recommendations

Received Given

#### Nothing to see for now

Recommendations that Róbert receives will appear here.

### Courses

#### Cisco Advanced Switching

#### Cisco Networking Academy

Associated with Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií

Show all 3 courses →

### Languages

#### Czech

Native or bilingual proficiency

#### English

Full professional proficiency

Show all 5 languages →

### Interests

Companies Schools



Cisco 6,511,065 followers

+ Follow



Nokia for service providers 444,336 followers

+ Follow

Show all companies →

### Causes

Economic Empowerment • Education • Environment • Health • Science and Technology

More profiles to browse



**Stanislav Hubáček** · 3rd+

Infrastructure engineer ve společnosti Home Credit International

Message



**Martin Kiska** · 3rd+

Senior Network Engineer at Avast

Message



**Vladislav W.** · 3rd+

Principal Software Maintenance Engineer at Red Hat

Message



**Jakub Srp** · 3rd+

Network Security Engineer ve společnosti Anect

Message



**Josef Hošek** · 3rd+

Technical Team Lead @ RWS Group

Message

Show all

Grow your network

Premium peer suggestions



**Jeanie Armstrong** · 3rd+

Senior Principal Fraud Consultant

Message



**Allie Forbes** · 3rd+

Senior Research Associate | Experimental Design, Data Analysis, Molecular Biology

Message

People you may know



**Meghan Leibold**

Enforcement Attorney, Securities and Exchange Commission

Connect



**Stephen Konya**

Director of Workforce Planning at US Securities and Exchange Commission

Connect



**Elliot Weingarten**

Attorney, Division of Enforcement at U.S. Securities and Exchange Commission  
[Connect](#)



**Michael Jaeger**

Attorney at the U.S. Securities and Exchange Commission

[Connect](#)



**Howard Kaplan**

Data Analyst at US Securities and Exchange Commission

[Connect](#)

[Show all](#)

**You might like**

Pages for you



**ImmunityBio, Inc.**

Biotechnology Research

18,596 followers

[+ Follow](#)



**Azira**

Technology, Information and Media

25,036 followers

[+ Follow](#)

[Show all](#)

- About
- Professional Community Policies
- Privacy & Terms
- Sales Solutions
- Safety Center

- Accessibility
- Careers
- Ad Choices
- Mobile

- Talent Solutions
- Marketing Solutions
- Advertising
- Small Business

- Questions?**  
Visit our Help Center.
- Manage your account and privacy**  
Go to your Settings.
- Recommendation transparency**  
Learn more about Recommended Content.

Select Language

English (English)

**Exhibit 2**

**From:** Krajcir, Robert [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=26414B37173741E09B795763D9ADA51D-KRAJCIR, RO]  
**Sent:** 8/30/2018 3:14:57 PM  
**To:** Taylor, Brody [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=71bea8d4ba2b4cf987d83d5ca8710846-Taylor, Bro]; Cline, Brad [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c1da7afa0bce413f9c32ce66040660f3-Cline, Brad]  
**CC:** Quitugua, Eric [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=227693e84bc0400b84364660f692bc85-Quitugua, E]; Trebacz, Marek [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=40b8e8d595274bc88506232551df513a-Trebacz, Ma]; Kenneally, Jonathan [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d039a086eac64dec81834f18ca486dad-Kenneally,]; Straub, Carol [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=18af4e35519d4f259ed12f407ada725f-Straub, Car]; Pierce, Charles [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8821c5f3c8734a3fbd33de946353d52b-Pierce, Cha]; Sejna, Tomas [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0f1c6bd3d32f4ca0966247ae2386cc56-Sejna, Toma]; Murray, Joe [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=13b5b9a696a44963a928819f1732caf6-Murray, Joe]; Henry, Jonathan [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=6edbe5d0a713413d9e003350861120bc-Henry, Jona]  
**Subject:** RE: Machine certificate authentication - BYOD solution  
**Attachments:** BYOD.pptx

Hello all,

First of all, big thank you for coming and sharing your ideas on this topic. Please find attached the presentation I used today, so you can show it to anyone you deem appropriate.

I also summarized some ideas that I have heard today, so it will be easier for you to recall what we discussed:

*Certificates issued via GPO/SCCM, there already are some, but Marek can deploy even more if needed*

*from security perspective we also need a proper written policy first to support us*

*will HD have capacity to support all users once they won't have admin rights? Marek presented idea that user can be redirected to portal every time, even when downloading unlicensed/unsupported software*

*bring this to attention of senior management, start from higher level – Brody, Brad*

*multiple IT teams involved - do the thing as a project, show the presentation to CIO (Rany)*

*consider to start implementing/deploying new systems without full admin rights, and do the rest during refreshes, or in waves*

*attendees – Robert Krajcir (Network), Charles Pierce (Network), Joe Murray (Systems), Tomas Sejna (InfoSec), Eric Quitugua (InfoSec), Marek Trebacz (SCCM guru :), Jonathan Kenneally (HD/SDM), Carol Straub (HD/compliance)*

Best regards,

Robert



**Róbert Krajčír | Network Engineer**

Office: +420 511 12 6277 | Cell: +420 775 395 043

---

**From:** Krajcir, Robert

**Sent:** Friday, August 24, 2018 11:13

**To:** Taylor, Brody <brody.taylor@solarwinds.com>; Murray, Joe <Joe.Murray@solarwinds.com>; Henry, Jonathan <jonathan.henry@solarwinds.com>

**Cc:** Quitugua, Eric <eric.quitugua@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; Kenneally, Jonathan <Jonathan.Kenneally@solarwinds.com>; Straub, Carol <carol.straub@solarwinds.com>; Cline, Brad <brad.cline@solarwinds.com>; Pierce, Charles <charles.pierce@solarwinds.com>; Masar, Marek <Marek.Masar@solarwinds.com>

**Subject:** RE: Machine certificate authentication

Hello all,

I would like to drag your attention back to this topic.

Implementing certificates is essential to enforce proper security policies not only on VPN, but also on corporate wireless, to properly address BYOD problem. We see every day, that people are accessing our corporate wifi with their smartphones or other devices that are not joined in the domain – **this seems to be common practice !!!** While we do not have any control over such device (proper antivirus, NetScope, OS updates etc.), it can easily reach any resource on any port on our corporate or swdev network.

To summarize the **risk we are facing**:

- Anyone with AD credentials can access our corporate wifi or corporate VPN from ANY device, no matter if company owned or not
- While on corporate wifi, or VPN, such device can basically do whatever without us detecting it until it's too late:
  - o It can easily download any content without being detected by NetScope, which is normally installed on all domain PCs
  - o it can compromise entire network by spreading malware (spyware, viruses, trojans, ransomware), because we cannot ensure that such device will be fully compliant in terms of OS updates, antivirus, software installed etc.

I do not want to look like panicking, but I hope I do not have to explain what would be the impact on this company, if someone connects non-domain PC or phone with ransomware like WannaCry into our network. Even though we will be able to see who's AD credentials were used to access the network, it will be to very little use once we will have to deal with stolen or encrypted data or malware epidemic, especially when we know that sometimes people are leaving the company, but their AD creds remain active for few more days.

I would like to emphasize, that we need to get some solution together as soon as possible. For the one I proposed, we would need to:

- trim down user admin rights, so that they won't be able to export certificates on their PC
- enroll certificates
- set VPN and wireless policies to accept only devices with valid certificate, and with valid AD credentials

I would like to schedule a call about this with all interested parties to agree on some action plan, so that we can get things moving. Let me know if you have any questions or concerns.

Best regards,

Robert



**Róbert Krajčír | Network Engineer**

Office: +420 511 12 6277 | Cell: +420 775 395 043

---

**From:** Krajcir, Robert

**Sent:** Thursday, June 7, 2018 18:37

**To:** Taylor, Brody <[brody.taylor@solarwinds.com](mailto:brody.taylor@solarwinds.com)>; Murray, Joe <[Joe.Murray@solarwinds.com](mailto:Joe.Murray@solarwinds.com)>; Cline, Brad <[brad.cline@solarwinds.com](mailto:brad.cline@solarwinds.com)>

**Cc:** Quitugua, Eric <[eric.quitugua@solarwinds.com](mailto:eric.quitugua@solarwinds.com)>; OConnell, Tara <[Tara.OConnell@solarwinds.com](mailto:Tara.OConnell@solarwinds.com)>; Trebacz, Marek <[Marek.Trebacz@solarwinds.com](mailto:Marek.Trebacz@solarwinds.com)>; Kenneally, Jonathan <[Jonathan.Kenneally@solarwinds.com](mailto:Jonathan.Kenneally@solarwinds.com)>; Straub, Carol <[carol.straub@solarwinds.com](mailto:carol.straub@solarwinds.com)>

**Subject:** RE: Machine certificate authentication on GlobalProtect VPN

Hi Brody,

That is a good question. At this moment, it seems it is everyone. Looking at the membership in AD groups, most of SWI employees can use the VPN. Yes, I believe there are groups of users who do not need access to on-premise resources at all, but I do not know how to determine which groups.

Best regards,

Robert



**Róbert Krajčír | Network Engineer**

Office: +420 511 12 6277 | Cell: +420 775 395 043

---

**From:** Taylor, Brody

**Sent:** Wednesday, June 6, 2018 22:55

**To:** Krajcir, Robert <[robert.krajcir@solarwinds.com](mailto:robert.krajcir@solarwinds.com)>; Murray, Joe <[Joe.Murray@solarwinds.com](mailto:Joe.Murray@solarwinds.com)>; Cline, Brad <[brad.cline@solarwinds.com](mailto:brad.cline@solarwinds.com)>

**Cc:** Quitugua, Eric <[eric.quitugua@solarwinds.com](mailto:eric.quitugua@solarwinds.com)>; OConnell, Tara <[Tara.OConnell@solarwinds.com](mailto:Tara.OConnell@solarwinds.com)>; Trebacz, Marek <[Marek.Trebacz@solarwinds.com](mailto:Marek.Trebacz@solarwinds.com)>; Kenneally, Jonathan <[Jonathan.Kenneally@solarwinds.com](mailto:Jonathan.Kenneally@solarwinds.com)>; Straub, Carol <[carol.straub@solarwinds.com](mailto:carol.straub@solarwinds.com)>

**Subject:** RE: Machine certificate authentication on GlobalProtect VPN

Dumb question, who are the user segments needing to access our domain assets post O365 / SharePoint?



**Brody Taylor | Director ITSM & EUS | SolarWinds**

Office: 512.682.9320 | Mobile: 512.652.8345

---

**From:** Krajcir, Robert

**Sent:** Tuesday, June 5, 2018 8:23 AM

**To:** Murray, Joe <[Joe.Murray@solarwinds.com](mailto:Joe.Murray@solarwinds.com)>; Cline, Brad <[brad.cline@solarwinds.com](mailto:brad.cline@solarwinds.com)>; IT HD Leads <[ithelpdeskleads@solarwinds.com](mailto:ithelpdeskleads@solarwinds.com)>; Trebacz, Marek <[Marek.Trebacz@solarwinds.com](mailto:Marek.Trebacz@solarwinds.com)>; OConnell, Tara

<[Tara.OConnell@solarwinds.com](mailto:Tara.OConnell@solarwinds.com)>; Quitugua, Eric <[eric.quitugua@solarwinds.com](mailto:eric.quitugua@solarwinds.com)>

Cc: Network Team <[NetworkTeam@solarwinds.com](mailto:NetworkTeam@solarwinds.com)>

Subject: RE: Machine certificate authentication on GlobalProtect VPN

Hey Joe,

Thanks for your email.

Yes, I agree that we have a lot to consider, that is why I have started this discussion at the first place. However, I would like to move our environment a bit further, as the only other option is to do nothing.

Regarding your concern – let me explain my vision a bit further. There should be two groups (or eventually more) of users:

Users accessing our VPN from company-owned device – should use machine certificate to authenticate their PC, should possess unlimited access (as if they were in the office)

Other users – should still have an option to connect to VPN, but their profile should have stricter policy and tier access should be limited. Also the number of gateways can be lower, i.e. just a few per region – Austin, Lehi/Denver, Ottawa, Cork, Brno, Manila, Singapore...

There could be also separate groups for vendors, contractors etc., depending on how many levels of restriction will be required.

So in my point of view, vendors, or non-domain computers in general should not have unrestricted access to our network, and thus should fall under one of the restricted categories that does not need any certificates. As for acquisitions – this initiative should motivate them to join tier PC to domain, especially laptops. Workstations that are always in the office do not matter, as there they are protected by our firewalls all the time. However, laptops, that can be carried away are what matters – if they are not in the domain, we cannot control their security outside of our network.

One other challenge is to issue a certificate to each machine in the domain, so it will not be exportable (user will not be able to read the private key), otherwise it would be easy to copy the certificate from one machine to other and bypass the entire idea. Question also is whether to create unique certs for each machine (i.e. bound to hostname, preferred method), or use one universal (wildcard one) and distribute everywhere.

@Tara, Marek – are we able to push certificates to machines so that users won't be able to export them / read private key? Will we need to trim user rights to achieve this?

Best regards,

Robert

 solarwinds

**Róbert Krajčír | Network Engineer**

Office: +420 511 12 6277 | Cell: +420 775 395 043

---

**From:** Murray, Joe

**Sent:** Tuesday, June 5, 2018 9:28

**To:** Krajcir, Robert <[robert.krajcir@solarwinds.com](mailto:robert.krajcir@solarwinds.com)>; Cline, Brad <[brad.cline@solarwinds.com](mailto:brad.cline@solarwinds.com)>; IT HD Leads <[ithelpdeskleads@solarwinds.com](mailto:ithelpdeskleads@solarwinds.com)>; Trebacz, Marek <[Marek.Trebacz@solarwinds.com](mailto:Marek.Trebacz@solarwinds.com)>; OConnell, Tara <[Tara.OConnell@solarwinds.com](mailto:Tara.OConnell@solarwinds.com)>; Quitugua, Eric <[eric.quitugua@solarwinds.com](mailto:eric.quitugua@solarwinds.com)>

**Cc:** Network Team <[NetworkTeam@solarwinds.com](mailto:NetworkTeam@solarwinds.com)>

**Subject:** RE: Machine certificate authentication on GlobalProtect VPN



Hi Robert,

I agree with the reasoning, however, I think it is needed as is for now.

Between vendors and all the acquisitions, we utilize VPN a lot for off domain computers (in fact they can be very reliant on it).

If Infosec would really like this looked at further, we could discuss possible ways to implement, but I think we have a lot to consider.

**Note:** if we did proceed, the root cert is already on all domain joined computers. It would just mean issuing a cert from our internal CA which would only take 2 minutes.

Thanks,

Joe

---

**From:** Krajcir, Robert

**Sent:** Monday 4 June 2018 15:49

**To:** Cline, Brad <[brad.cline@solarwinds.com](mailto:brad.cline@solarwinds.com)>; IT HD Leads <[ithelpdeskleads@solarwinds.com](mailto:ithelpdeskleads@solarwinds.com)>; Trebacz, Marek <[Marek.Trebacz@solarwinds.com](mailto:Marek.Trebacz@solarwinds.com)>; OConnell, Tara <[Tara.OConnell@solarwinds.com](mailto:Tara.OConnell@solarwinds.com)>; Quitugua, Eric <[eric.quitugua@solarwinds.com](mailto:eric.quitugua@solarwinds.com)>

**Cc:** Network Team <[NetworkTeam@solarwinds.com](mailto:NetworkTeam@solarwinds.com)>; Murray, Joe <[Joe.Murray@solarwinds.com](mailto:Joe.Murray@solarwinds.com)>

**Subject:** Machine certificate authentication on GlobalProtect VPN

Hello all,

By this initiative, I would like to address following problem:

These days, we are in process of firewall cleanup and optimization, which showed us a security gap we are facing with our VPN service. As GlobalProtect VPN client is publicly available for download, it is no problem for almost any user to download it to any PC they like, and log in to our VPN from 3<sup>rd</sup> party device – without Netskope, proper Antivirus, security patches or updates etc. This is not only a major drawback from opening access to our network via VPN completely (as we intend to in the future, as it will be required by teleworkers, on business trips etc.), but I guess we all will also agree, that it is not very secure for resources currently accessible via VPN and data stored there, especially considering stricter legislation such as GDPR.

What I propose:

Use certificates for machine authentication. Basically it would mean, that users will only be able to connect to our VPN from verified/trusted devices, that are under IT control, joined the domain, are properly updated and have the required software properly installed and in use. For everyone else, there could be one or two separate VPN gateways per region with stricter policy (access to less resources).

What do we need:

As far as I have researched, there are no additional costs associated with implementing certificates. We do not need additional licenses or hardware. Joe also informed me, that we already have our internal CA server that can be used for this purpose. So what we need to do is basically this:

- configure new connection profiles on our firewalls,
- import root certificate on the firewall
- Issue, push and install certificates to client machines – i.e. in waves via SCCM, or let users download manually from a server accessible only from office... subject to further discussion

- Implement a pilot (i.e. all IT people as testers)
- Roll out to all users
- Create/modify the policies for access from corporate devices and from 3<sup>rd</sup> party devices

The reason why I am writing this email:

I would like to get inputs from you folks, especially your thoughts on the solution itself, on how exactly to push the certificates to user machines, how the support should look like, testing period etc. Feel free to comment or forward to anyone who may be interested but I accidentally omitted him/her from the recipient list.

Thank you!

Best regards,

Robert

**solarwinds** 

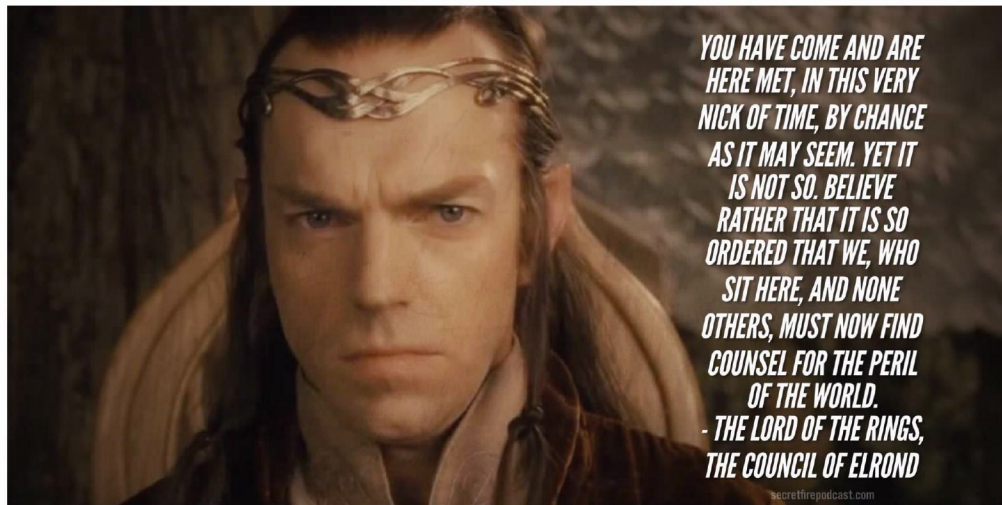
**Róbert Krajčír | Network Engineer**

Office: +420 511 12 6277 | Cell: +420 775 395 043



7/30/2021

0



CONFIDENTIAL INTERNAL USE ONLY -- NOT FOR DISTRIBUTION © 2018 SolarWinds Worldwide, LLC. All rights reserved.

1

7/30/2021

1

## CURRENT STATUS

No BYOD restrictions applied

- No means to enforce or monitor what devices connect to our network
- No options how to guarantee user identity
  - certificates are easily exportable
- Employees do not respect security guidelines
  - Installing 3<sup>rd</sup> party software, even games
  - Using torrents
  - Connect own devices or phones to Solarwinds SSID instead of guest
- Aerohive deployment
  - Better policy enforcement based on OS, still gap with Windows
- Out of 365 users on Solarwinds SSID (EMEA morning):
  - About ½ are Microsoft clients
    - Most probably all are regular clients, no guarantee
  - 24 clients are MAC-OS
    - Not in domain, centralized management still possible via Apple tools
  - 75 clients are Android, iPhone, Linux, Linksys, or Unknown
    - Cannot be reached or monitored by our tools

Solarwinds SSID usage (non-Win machines)

Device Type	Count
Apple	44
Linux-Workstation	22
Unknown	22
Android	5
OS_X-Workstation	5
Linksys-Device	3

CONFIDENTIAL INTERNAL USE ONLY -- NOT FOR DISTRIBUTION © 2019 SolarWinds Worldwide, LLC. All rights reserved.

2

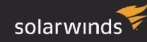
Mention situation I witnessed in AMS and BUC  
 We cannot track windows devices  
 Torrenting software has been found on several laptops by HD recently  
 Many PCs not in the domain

7/30/2021

2

**RISKS FOR COMPANY**

Summary and evaluation



- Unmanaged (non-domain) machines summary:
  - We have no control over critical device features:
    - Antivirus
    - OS updates
    - NetScope
    - Installed software
    - Applications running
  - Possess the same level of access as all other devices in CORP zone
    - Can reach any resource on any port (exc. DMZ, HIGHSECURITY zones etc.)
    - Access from CORP VPN is a bit restricted
  - Capable of doing anything to our core systems
    - Can be weak spot in our network (old OS, or obsolete updates)
    - May serve as unintentional back door access to our core systems if infected
    - Spread malware
    - Access resources (code, databases...)
    - Can upload code or GDPR sensitive data outside (no NetScope)
- Worst-case scenarios for the company:
  - Data theft
    - GDPR – sensitive data (employees, customers...)
    - Code or other intellectual property
    - Strategical documents (future acquisitions, stock market documents etc.)
  - Malware infection
    - Ransomware (Wannacry)
    - Viruses, Trojans, backdoor access
  - In all cases there will be major reputation and financial loss to the company

CONFIDENTIAL INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2018 SolarWinds Worldwide, LLC. All rights reserved.


3

7/30/2021

3

## RISKS FOR COMPANY

Possible scenarios




**Outside attack**

1. Phishing attack
  - Attacker gets AD credentials
2. Connection to corporate wireless or corporate VPN
3. Access to resources
  - Depends on account group membership
  - Fileshares
  - Bitbucket/Artifactory
  - Sharepoint
  - SolarHR
4. Consequences
  - Data theft
  - Disclosure
  - Corruption
  - Installs backdoor
  - Intentional malware release
  - Get info for future attacks
  - ...
  - Nobody notices

**Infected device**

1. Device is infected outside of SWI network
  - Personal use
  - OS not patched properly
  - Antivirus missing or obsolete
2. Device connects to SWI network via wireless or VPN
3. Malware spreads automatically
  - Email
  - Teams
  - Local network
  - ...
4. Consequences
  - Encrypted files
  - Attacks from our IP addresses outside
  - Data theft
  - Backdoor
  - ...




CONFIDENTIAL INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2019 SolarWinds Worldwide, LLC. All rights reserved.
4

It is only matter of time until someone finds out, some may even know. Hackers can be very creative  
 Scenario 1 – all devices vulnerable, targets on user weakness, then avoids our security mechanisms like NetScope  
 Phishing attack on One-Note like Tim Brown specified on all-hands. Risk is even bigger if done by someone who knows the environment – former employee who was fired, someone who overheard a conversation, friend of an employee etc.  
 Attacker does not have to be in the office, just somewhere nearby  
 Take into consideration what could have been done just using the vulnerability in dnsstuff

Scenario 2 – devices that are not in the domain are vulnerable to threats even if user has good intentions  
 Firewall antivirus or threat prevention mechanisms apply only when the malware / suspicious traffic is crossing firewall – in AUS, BRN, KRA offices multiple networks can be compromised without any filtering

7/30/2021

4

**PLAN FUTURE STEPS** solarwinds 

- What to do with the risk described?
  - Accept
  - Suppress to acceptable level
  - Mitigate completely
  
- Aerohive WAP deployment
  - In progress
  - Affects only corporate wireless, not VPN
  - Does not cover Windows devices
  - It will take a lot of time and resources to deploy everywhere
  
- Implement proper security policies
  - Firewall cleanup is in finish line
  - Decide how to treat offices like London or Japan
  
- Implement BYOD policy and enforce it
  - 2F authentication
  - Device certificates
  - Tools like ISE, ACS, NAC...
  - ...
  - Any ideas?

CONFIDENTIAL INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2019 SolarWinds Worldwide, LLC. All rights reserved.

5

This is what we need to discuss after what was presented in slides before  
We already know that we cannot rely on some handbooks or guidelines – BYOD policies have to be enforced  
Need to prevent non-company devices to easily access our network – how to achieve this?  
London/Japan – firewalls which allow access to SWI network, but we have no visibility of what connects behind

7/30/2021

5



**IMPLEMENTING CERTIFICATES**

Example of possible approach



- Manage user admin rights
  - At this time basically unlimited
  - Needed, so that users will not be able to export certificates
  - TBD by helpdesk
- Enroll certificates
  - Build CA authority or use existing one
  - Issue server and client certificates
    - Bound to machine?
    - Universal one?
  - PC would have to connect to the wired network in the office first (so it will download required certificates and config)
  - TBD by Helpesk and Systems teams
- Implement certificate authentication
  - Machine only authentication
    - Machine is in the domain, so it can download certificate
    - If in domain, it has proper OS patches and antivirus
    - It can connect to our resources without user credentials
  - Machine certificate + user credential authentication
    - More complicated to implement, but safer
  - Non-domain machines (no cert.) – can be allowed to our network, but with limited access
  - Start with some group of test users as a pilot
  - Create new SSID and VPN profile for testing
  - TBD by Network team

CONFIDENTIAL INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2019 SolarWinds Worldwide, LLC. All rights reserved.

6

Importing/exporting certificates is quite easy – everyone can use the google, and there is a Windows wizard to help, so even cleaning lady could be capable of that  
 Machine certificate – using PEAP or EAP-TLS  
 User auth after machine auth – web portal

7/30/2021

6



...Or it's just a beginning of our journey?



7/30/2021

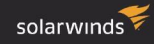
7

Let's go through the presentation again and discuss the points you are interested in :)

# Q&A

7/30/2021

8



The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

CONFIDENTIAL INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2018 SolarWinds Worldwide, LLC. All rights reserved.

9

7/30/2021

9

**Exhibit 3**

- [EMEA: +353 21 5002900](#)
  - [APAC: +61 2 8412 4900](#)
  - [Submit a Ticket](#)
- [Training & Certification](#)
  - [SolarWinds Academy](#)
  - [SolarWinds Certified Professional](#)
- [Customer Portal](#)
  - [Access the Customer Portal](#)
- [Community](#)
  - [THWACK](#)
    - [View THWACK](#)
  - [Orange Matter](#)
    - [View Orange Matter](#)
  - [LogicalRead Blog](#)
    - [View LogicalRead Blog](#)
  - [COVID-19 Resource Center](#)
    - [View Covid-19 Resources](#)
    - [View Security Resources in our Trust Center](#)
- [FREE TRIALS](#)
- [Contact Sales](#)
- [Online Quote](#)
- [View All Products](#) [View Free Tools](#)

SolarWinds asks all customers to upgrade immediately to Orion Platform version 2020.2.1 HF 1 to address a security vulnerability. More information is available [here](#).

✘

## SolarWinds Security Statement

This Security Statement is aimed at providing you with more information about our security infrastructure and practices. Our privacy policy contains more information on how we handle data that we collect.

### Information Security Policy

SolarWinds maintains a written Information Security policy that defines employee's responsibilities and acceptable use of information system resources. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before providing authorized access to SolarWinds information systems. This policy is periodically reviewed and updated as necessary.

Our security policies cover a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering internal applications and information systems.

### Organizational Security

Information security roles and responsibilities are defined within the organization. The security team focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of SolarWinds' hardware infrastructure.

The security team receives information system security notifications on a regular basis and distributes security alert and advisory information to the organization on a routine basis after assessing the risk and impact as appropriate.

SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents. The information security manager is also responsible for tracking incidents, vulnerability assessments, threat mitigation, and risk management.

### Asset Management

SolarWinds' data and information system assets are comprised of customer and end-user assets as well as corporate assets. These asset types are managed under our security policies and procedures. SolarWinds authorized personnel who handle these assets are required to comply with the procedures and guidelines defined by SolarWinds security policies.

### Personnel Security

SolarWinds employees are required to conduct themselves in a manner consistent with the company's guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees are required to sign confidentiality agreements and to acknowledge the SolarWinds code of conduct policy. The code outlines the company's expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors. Processes and procedures are in place to address employees who are on-boarded and off-boarded from the company.

Employees are provided with security training as part of new hire orientation. In addition, each SolarWinds employee is required to read, understand, and take a training course on the company's code of conduct.

## Physical and Environmental Security

SolarWinds has policies, procedures, and infrastructure to handle both physical security of its data centers as well as the environment from which the data centers operate.

Our information systems and infrastructure are hosted in world-class data centers that are geographically dispersed to provide high availability and redundancy to SolarWinds and its customers. The standard physical security controls implemented at each data center include electronic card access control systems, fire alarm and suppression systems, interior and exterior cameras, and security guards. Physical access is centrally managed and strictly controlled by data center personnel. All visitors and contractors are required to present identification, are required to log in, and be escorted by authorized staff through the data center.

Access to areas where systems, or system components, are installed or stored are segregated from general office and public areas. The cameras and alarms for each of these areas are centrally monitored 24x7 for suspicious activity, and the facilities are routinely patrolled by security guards. Servers have redundant internal and external power supplies. Data centers have backup power supplies, and can draw power from diesel generators and backup batteries. These data centers have completed a Service Organization Controls (SOC) 2 Type II audit and are SSAE16 accredited.

## Operational Security

### Change Management

SolarWinds maintains a change management process to ensure that all changes made to the production environment are applied in a deliberate manner. Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.

### Supplier and Vendor Relationships

SolarWinds likes to partner with suppliers and vendors that operate with the same or similar values around lawfulness, ethics, and integrity that SolarWinds does. As part of its review process, we screen our suppliers and vendors and bind them to appropriate confidentiality and security obligations, especially if they manage customer data.

SolarWinds does not give our suppliers or vendors direct access to network/equipment management responsibility. Our procurement department may perform audits from time to time on SolarWinds suppliers and vendors in an effort to ensure the confidentiality, integrity, and availability of data that our third party suppliers or vendors may handle.

### Auditing and Logging

We maintain audit logs on systems. These logs provide an account of which personnel have accessed which systems. Access to our auditing and logging tool is controlled by limiting access to authorized individuals. Security events are logged, monitored, and addressed by trained security team members. Network components, workstations, applications and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to events are defined. Security events that record critical system configuration changes and administrators are alerted at the time of change. Retention schedules for the various logs are defined in our security control guidelines.

### Antivirus and Malware Protection

Antivirus and malicious code protection is centrally managed and configured to retrieve the updated signatures and definitions available. Malicious code protection policies automatically apply updates to these protection mechanisms. Anti-virus tools are configured to run scans, virus detection, real-time file write activity and signature file updates. Laptop and remote users are covered under virus protection. Procedures to detect and remove unauthorized or unsupported (e.g. freeware) applications are documented.

### System Backups

SolarWinds has backup standards and guidelines and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data (onsite and off-site). We also work to ensure that customer data is securely transferred or transported to and from backup locations. Periodic tests are conducted to test whether data can be safely recovered from backup devices.

### Network Security

Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats. Firewalls are utilized to help restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need.

SolarWinds maintains separate development and production environments. Our next generation firewalls (NGFWs) provide adequate network segmentation through the establishment of security zones that control the flow of network traffic. These traffic flows are defined by strict firewall security policies.

Automated tools are deployed within the network to support near-real-time analysis of events to support of detection of system-level attacks. Next generation firewalls deployed within the data center as well as remote office sites monitor outbound communications for unusual or unauthorized activities, which may be an indicator of the presence of malware (e.g., malicious code, spyware, adware).

#### **Data Protection**

SolarWinds continually works to develop products that support the latest recommended secure cipher suites and protocols to encrypt traffic while in transit. We monitor the changing cryptographic landscape closely and work to upgrade our products to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility for older clients.

#### **Vulnerability Management**

Security assessments are done to identify vulnerabilities and to determine the effectiveness of the patch management program. Each vulnerability is reviewed to determine if it is applicable, ranked based on risk, and assigned to the appropriate team for remediation.

#### **Patch Management**

SolarWinds strives to apply the latest security patches and updates to operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Patch management processes are in place to implement security patch updates as they are released by vendors. Patches are tested prior to being deployed into production.

#### **Secure Network Connections**

HTTPS encryption is configured for customer web application access. This helps to ensure that user data in transit is safe, secure, and available only to intended recipients. The level of encryption is negotiated to either SSL or TLS encryption and is dependent on what the web browser can support.

### **Access Controls**

#### **Role Based Access**

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

#### **Authentication and Authorization**

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords. Passwords are individually salted and hashed.

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

### **Software Development Lifecycle**

We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.

Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

### **Incident Management**

SolarWinds has a formalized incident response plan (Incident Response Plan) and associated procedures in case of an information security incident. The Incident Response Plan defines the responsibilities of key personnel and identifies processes and procedures for notification. Incident response personnel are trained, and execution of the incident response plan is tested periodically.

An incident response team is responsible for providing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.



### Business Continuity and Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, we implement a disaster recovery program at all our data center locations. This program includes multiple components to minimize the risk of any single point of failure. Application data is replicated to multiple systems within the data center and, in some cases, replicated to secondary or backup data centers that are geographically dispersed to provide adequate redundancy and high availability. High-speed connections between our data centers help to support swift failover.

### Data Protection

We apply a common set of personal data management principles to customer data that we may process, handle, and store. We protect personal data using appropriate physical, technical, and organizational security measures.

We give additional attention and care to sensitive personal data and respect local laws and customs, where applicable.

SolarWinds only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorized in accordance with our privacy policy. We take all reasonable steps to protect information we receive from our users from loss, misuse or unauthorized access, disclosure, alteration and/or destruction.

We're Geekbuilt.®

Developed by network and systems engineers who know what it takes to manage today's dynamic IT environments, SolarWinds has a deep connection to the IT community.

The result? IT management products that are effective, accessible, and easy to use.

- 
- 
- 
- 

[Company](#) [Investors](#) [EVENTS](#) [Career Center](#) [Resource Center](#)  
[Email Preference Center](#) [For Customers](#) [For Government](#) [GDPR Resource Center](#) [SOLARWINDS TRUST CENTER](#)  
[Legal Documents](#) [Privacy](#) [California Privacy Rights](#) [Security Information](#) [Documentation & Uninstall Information](#) [Sitemap](#)

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

[Close](#) 

{{STATIC\_CONTENT}}



{{CAPTION\_TITLE}}

{{CAPTION\_CONTENT}}

{{TITLE}}

