UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM SD

SPECIALIZED DISCLOSURE REPORT

FORTINET, INC.
(Exact Name of Registrant as Specified in its Charter)

Delaware	**001-34511**	**77-0560389**
(State or other jurisdiction of incorporation or organization)	**(Commission File Number)**	**(IRS Employer Identification No.)**

909 Kifer Road, Sunnyvale, California	**94086**
(Address of Principal Executive Offices)	**(Zip Code)**

John Whittle
(408) 235-7700
(Name and telephone number, including area code, of the person to contact in connection with this report.)

Not Applicable
(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below to indicate the rule pursuant to which this form is being filed, and provide the period to which the information in this form applies:

☒ Rule 13p-1 under the Securities Exchange Act (17 CFR 240.13p-1) for the reporting period January 1, 2023 to December 31, 2023

Item 1.01. Conflict Minerals Disclosure and Report.

Conflict Minerals Disclosure

A copy of the Conflict Minerals Report of Fortinet, Inc. ("Fortinet") for the reporting period January 1, 2023 to December 31, 2023 is filed as Exhibit 1.01 to this specialized disclosure report on Form SD and is also available at Fortinet's website at https://investor.fortinet.com/sec-filings.

Item 1.02. Exhibit.

Fortinet has filed, as an exhibit to this Form SD, a Conflict Minerals Report as required by Item 1.01 of this Form.

Item 3.01. Exhibits.

Exhibit Number	Description of Document
1.01	Fortinet, Inc. Conflict Minerals Report for the reporting period January 1, 2023 to December 31, 2023

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the duly authorized undersigned.

FORTINET, INC.

Dated: May 20, 2024

By: /s/ John Whittle
Name: John Whittle
Title: Chief Operating Officer

Fortinet, Inc.
Conflict Minerals Report
For the Reporting Period January 1, 2023 to December 31, 2023

This Conflict Minerals Report ("CMR") has been prepared by Fortinet, Inc. (herein referred to, alternatively, as "Fortinet," "we" and "our"). This CMR for the reporting period January 1, 2023 to December 31, 2023 is presented to comply with the final conflict minerals implementing rules ("Final Rules") promulgated by the Securities and Exchange Commission ("SEC"), as modified by SEC guidance issued on April 29, 2014 and the SEC order issued on May 2, 2014. The Final Rules were adopted by the SEC to implement reporting and disclosure requirements related to conflict minerals as directed by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 as codified in Section 13(p) of the Securities Exchange Act of 1934. The Final Rules impose certain reporting obligations on SEC registrants whose manufactured products contain conflict minerals that are necessary to the functionality or production of their products. "Conflict minerals" are currently defined by the SEC as cassiterite, columbite-tantalite (coltan), gold, wolframite, or their derivatives, which the SEC has currently limited to tin, tantalum and tungsten.

To comply with the Final Rules, we conducted due diligence on the origin, source and chain of custody of the conflict minerals that were necessary to the functionality or production of the products that we manufactured or contracted to manufacture to attempt to ascertain whether these conflict minerals originated in the Democratic Republic of the Congo or an adjoining country (collectively, "Covered Countries") and financed or benefited armed groups (as defined in Section 1, Item 1.01(d)(2) of Form SD) in any of these countries.

Pursuant to SEC guidance issued April 29, 2014 and the SEC order issued May 2, 2014, Fortinet is not required to describe any of its products as "DRC conflict free" (as defined in Section 1, Item 1.01(d)(4) of Form SD), "DRC conflict undeterminable" (as defined in Section 1, Item 1.01(d)(5) of Form SD) or "having not been found to be 'DRC conflict free,'" and therefore makes no conclusion in this regard in the report presented herein. Furthermore, given that Fortinet has not voluntarily elected to describe any of its products as "DRC conflict free," an independent private sector audit of the report presented herein has not been conducted.

I. Company Overview

Fortinet is a global leader in cybersecurity solutions provided to a wide variety of organizations, including enterprises, communications and security service providers, government organizations and small businesses. Fortinet's cybersecurity solutions are designed to provide broad visibility and segmentation of the digital attack surface through our integrated Fortinet Security Fabric cybersecurity mesh platform, which features automated protection, detection and response along with consolidated visibility across both Fortinet developed solutions and a broad ecosystem of third-party solutions and technologies.

II. Product Overview

Fortinet's product offerings consist of a core software platform, FortiOS which is delivered through appliances (FortiGate), virtual machines (FortiGate VM) and the cloud. FortiGate uses proprietary ASIC technology to accelerate performance. FortiGuard threat intelligence provides services to the core platform.

The core platform can be extended into a security fabric which includes various additional offerings.

III. Supply Chain Overview

Fortinet outsources the manufacture of its security hardware appliance products to a variety of contract manufacturers and original design manufacturers. Fortinet submits purchase orders to its contract manufacturers that describe the type and quantities of products to be manufactured, the delivery date and other delivery terms. Fortinet's proprietary FortiASICs, which are incorporated in certain of Fortinet's hardware appliance products, are fabricated by contract manufacturers. The components included in Fortinet's products are sourced from various suppliers by Fortinet or more frequently by Fortinet's contract manufacturers. Some of the components important to Fortinet's business, including specific types of central processing units, network chips, and solid-state drives (silicon-based storage devices), are available from a limited or sole source of supply. For purposes of this CMR, references to our "products" refer to our manufactured hardware products, and references to our "suppliers" refer to our product suppliers.

IV. Conflict Minerals Analysis and Reasonable Country of Origin Inquiry

Based upon a review of our products and our reasonable country of origin inquiry ("RCOI"), we have concluded that:

- Our products contain conflict minerals that are necessary to the production or functionality of such products; and
- We are unable to determine whether the conflict minerals present in our products originate in the Covered Countries.

V. Design of Due Diligence Measures

Fortinet designed its due diligence with respect to the source and chain of custody of the conflict minerals contained in its products based on the five-step framework set forth in the Third Edition of the Organisation for Economic Co-operation and Development's Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas and the supplements thereto (the "OECD Guidance").

VI. Due Diligence Measures Performed by Fortinet

Fortinet performed the following due diligence measures in accordance with the OECD Guidance and the Final Rules:

OECD Guidance Step #1: Establish Strong Company Management Systems

- Fortinet maintains a Responsible Minerals Sourcing Policy (the "Responsible Minerals Sourcing Policy") that sets forth its commitments regarding the sourcing of conflict minerals and its expectations of its suppliers regarding the same.
- The implementation of Fortinet's RCOI and the conducting of due diligence on the source and chain of custody of Fortinet's necessary conflict minerals are managed by Fortinet's legal and operations departments.
- The legal and operations staff responsible for conflict minerals compliance (i) have received training regarding conflict minerals compliance and (ii) are required to be familiar with Fortinet's Responsible Minerals Sourcing Policy and with Fortinet's conflict minerals-related processes.
- Material conflict minerals-related records, including completed CMRTs (as defined below), will be maintained by Fortinet for a period of five (5) years from the date of creation.
- Fortinet's Responsible Minerals Sourcing Policy has been made available to existing suppliers, and Fortinet makes the Responsible Minerals Sourcing Policy available to new suppliers during the conflict minerals diligence process. In addition, Fortinet's form manufacturing purchase agreement contains a conflict minerals compliance provision (the "Conflict Minerals Contractual Provision") that incorporates the Responsible Minerals Sourcing Policy as an exhibit thereto. The Conflict Minerals Contractual Provision was incorporated into (i) new manufacturing purchase agreements entered into in the 2023 reporting year and (ii) amendments to existing manufacturing purchase agreements entered into in the 2023 reporting year.
- Interested parties can report improper activities in violation of the Responsible Minerals Sourcing Policy via email at environmental_relations@fortinet.com.

OECD Guidance Step #2: Identify and Assess Risk in the Supply Chain

- Fortinet has requested that its suppliers complete in full the Responsible Minerals Initiative's (the "RMI") Conflict Minerals Reporting Template (the "CMRT"). The CMRT is designed to request from Fortinet's suppliers sufficient information regarding such suppliers' practices with respect to the sourcing of conflict minerals to enable Fortinet to comply with its requirements under the Final Rules.

- Fortinet's legal and operations departments manage and oversee the collection of information reported on the CMRT by Fortinet's suppliers, and Fortinet relies on a third party to analyze certain information as requested by Fortinet.

OECD Guidance Step #3: Design and Implement a Strategy to Respond to Identified Risks

- If, on the basis of areas of concern that are identified as a result of either (i) the supplier data acquisition or engagement processes or (ii) the receipt of information from other sources, Fortinet determines that a supplier is sourcing conflict minerals that are directly or indirectly financing or benefiting armed groups, Fortinet will enforce the Responsible Minerals Sourcing Policy by means of a series of escalations.
- Such escalations may range from prompt engagement with the supplier to resolve the sourcing issue, to requiring such supplier to implement a risk management plan (which plan may involve, as appropriate, remedial action up to and including disengagement from upstream suppliers), to disengagement by Fortinet from the applicable supplier.

OECD Guidance Step #4: Carry Out Independent Third-Party Audit of Supply Chain Due Diligence at Identified Points in the Supply Chain

Given that we do not have a direct relationship with the smelters and refiners that process the conflict minerals that are present in our products, we rely on the RMI to conduct third-party audits of smelters and refiners.

OECD Guidance Step #5: Report on Supply Chain Due Diligence

As required by the Final Rules, we have filed a Form SD and this Conflict Minerals Report as an exhibit thereto for the 2023 reporting year. The Form SD and Conflict Minerals Report are also available on our website at https://investor.fortinet.com/sec-filings.

VII. Smelters and Refiners Identified

As a result of Fortinet's reasonable country of origin inquiry, 41 suppliers, representing approximately 66% of our suppliers, provided completed CMRTs to Fortinet. Fortinet's suppliers identified approximately 348 smelters and refiners from which they source conflict minerals that appear on the RMI's Standard Smelter List, and of those smelters and refiners, approximately 240 smelters and refiners, or approximately 68%, have successfully completed an assessment against the applicable RMI Responsible Minerals Assurance Process ("RMAP") standard. The remainder of the reported smelters and refiners have not, at this time, successfully completed an assessment against the applicable RMAP standard (the "Non-Conformant Smelters and Refiners"). Fortinet was not able to determine the country of origin of the conflict minerals in its products.

The information contained in the preceding paragraph is based on supplier responses received through May 15, 2024. Smelter and refiner status is provided as of May 15, 2024.

VIII. Steps to Mitigate Risk

Fortinet intends to take the following steps to mitigate the risk that conflict minerals benefit armed groups:

- Continue to engage with suppliers to obtain complete CMRTs; and
- Encourage the development of supplier capabilities to perform conflict minerals-related due diligence.

FORWARD-LOOKING STATEMENTS

Statements relating to risk mitigation and other statements herein are forward-looking in nature and are based on Fortinet's management's current expectations or beliefs. These forward-looking statements are not a guarantee of performance and are subject to a number of uncertainties and other factors that may be outside of Fortinet's control and that could cause actual events to differ materially from those expressed or implied by the statements made herein, and Fortinet reserves the right to change its processes and policies related to conflict minerals.

DOCUMENTS INCORPORATED BY REFERENCE

Unless otherwise expressly stated herein, any documents, third-party materials or references to websites (including Fortinet's) are not incorporated by reference in, or considered to be a part of this CMR, unless expressly incorporated by reference herein.