Publication date:
June 2024

Authors:
Tanner Johnson
Adam Strange
Elvia Finalle

Quantifying the Public Vulnerability Market: 2023 Edition

An analysis of vulnerability disclosures, impact severity, and product analysis

OMDIA

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Trend Micro

Contents

Omdia’s overall research methodology

Overview

Omdia conducted comprehensive comparative research and analysis, examining the output of 9 organizations that disclose information security vulnerabilities. As a component of this research, Omdia cross-referenced the data from these vendors against the information organized and published by various government agencies, including

- The MITRE Corporation
- The National Institute of Standards and Technology (NIST)
- The United States Computer Emergency Response Team Coordination Center (US CERT/CC)
  - Though listed with other reporting organizations, the US CERT/CC is a US government agency and not a security vendor of any kind

Research scope

The scope of Omdia’s analysis used the following constraints:

- Vulnerabilities are only credited to a vendor if it is ultimately responsible for *managing the disclosure* of the vulnerability.

- All vulnerabilities must have been disclosed within the calendar year 2023.

- All vulnerabilities must have been assigned a Common Vulnerabilities and Exposures (CVE) number.

- Disclosed vulnerabilities with associated CVEs that were not credited to the organizations within our scope are not incorporated or discussed as part of our overall analysis.

- In the instances where credit for a vulnerability was claimed by two or more vendors, Omdia grants credit to each vendor making the claim, because there is no way to independently validate credit:

  - In 2023, 1,201 vulnerabilities were claimed once, and 10 vulnerabilities were claimed twice.
  - This results in 1,211 unique and verified vulnerabilities.
- Omdia attributes credit for each vulnerability to all vendors that claimed it, so the total number of all verified vulnerabilities claimed by the nine research organizations for 2023 is *1,211*.

Analysis methodology

The data collected for this report stems from multiple sources, including

- Primary internal research
- Individual vendor interviews
- Open source publication

Omdia collected all publicly available vulnerability data from each of the organizations listed in the executive summary and assigned credit for each vulnerability. However, to be attributed credit for a listed vulnerability, an organization had to be responsible for effectively managing its disclosure, meaning that the organization directly oversaw the release of the vulnerability:

- Credit for *managing* a vulnerability was not assigned to a vendor simply because it was listed on the vendor's public-facing advisory website.

Omdia then collected data on all verified vulnerabilities during 2021 using the NIST National Vulnerability Database (NVD) data feeds and used this data as the baseline for vendor comparison:

- To be considered verified, all vulnerabilities in Omdia's analysis must have an associated CVE number (in order to prevent rejected or duplicated entries from being introduced into the analysis) and to have a Common Vulnerability Scoring System (CVSS) value assigned by the NVD.
- Vulnerabilities without a CVE, though still credited to the respective vendor, are not included in Omdia's analysis.

The CVSS and Common Weakness Enumeration (CWE) metrics assigned by the NVD allowed Omdia to conduct a comparative analysis of the performance of all vendors, the severity of the vulnerabilities they disclosed, and the attack methodology of the vulnerabilities each vendor was credited with.

Vulnerability market analysis

A vulnerability is a weakness, error, defect, flaw, or bug that poses a threat to the confidentiality, integrity, and availability of data within an information system. Adversaries seek to take advantage of vulnerabilities present in hardware, software, and firmware, because they can be exploited in ways that compromise the systems on which they reside. The longer the time between the discovery of a vulnerability, its disclosure, and its ultimate remediation, the more time a potential hacker has to exploit the vulnerability.

Vulnerabilities that exist but are unknown to the affected vendor are commonly referred to as zero-day vulnerabilities. Zero-day vulnerabilities pose the greatest threat to information security and are viewed as the greatest prize for cybercriminals to attain and share. Because vulnerabilities can only be addressed once they are discovered and shared within the affected vendor, there is an incentive among researchers and others with a vested interest in cybersecurity to report a vulnerability as quickly as possible. Even if a vulnerability is mitigated through a security patch, the threat remains for every system that has not been updated.

As more product vendors, security organizations, and individual researchers contribute to the process, the associated threats introduced by vulnerabilities can be mitigated with greater efficacy. The potential impact of these vulnerabilities can vary greatly: some security flaws may merely be annoying; others are critical enough to have potentially catastrophic consequences for the vulnerable system, its users, and the organizations concerned.

To conduct a comprehensive analysis of any vulnerability, there are several characteristics and values that need to be identified first in order to cross-reference them across reporting organizations:

- CVE value
  - Unique identifier given to each vulnerability by a CVE Numbering Authority (CNA)
- CWE value
  - Preliminary identifier used to categorize and define common software weaknesses
- CVSS value
  - Numerical score reflecting the severity of the vulnerability

Results

The associated CVSS score attached to each vulnerability by the NVD provides organizations with a visible metric by which to gauge any vulnerability’s severity and help prioritize any threat remediation tactics:

- Critical vulnerabilities are those that can have potentially catastrophic effects on an organization's information security. These threats typically surround unauthorized root-level access and can result in the unauthorized modification or disclosure of data or a denial of service (DoS). Threats are often elevated to this level if an attacker can gain access without any special conditions or advanced knowledge. Critical-scoring vulnerabilities accounted for roughly 10% of all disclosed threats.

- High-level vulnerabilities can also have damaging effects on an organization's information security. However, vulnerabilities scored as high are traditionally more challenging to exploit because they require certain conditions be met first, though any exploitation can still result in privilege escalation or loss of access to data. High-scoring vulnerabilities accounted for the majority of those disclosed, comprising 69% of all vulnerabilities.

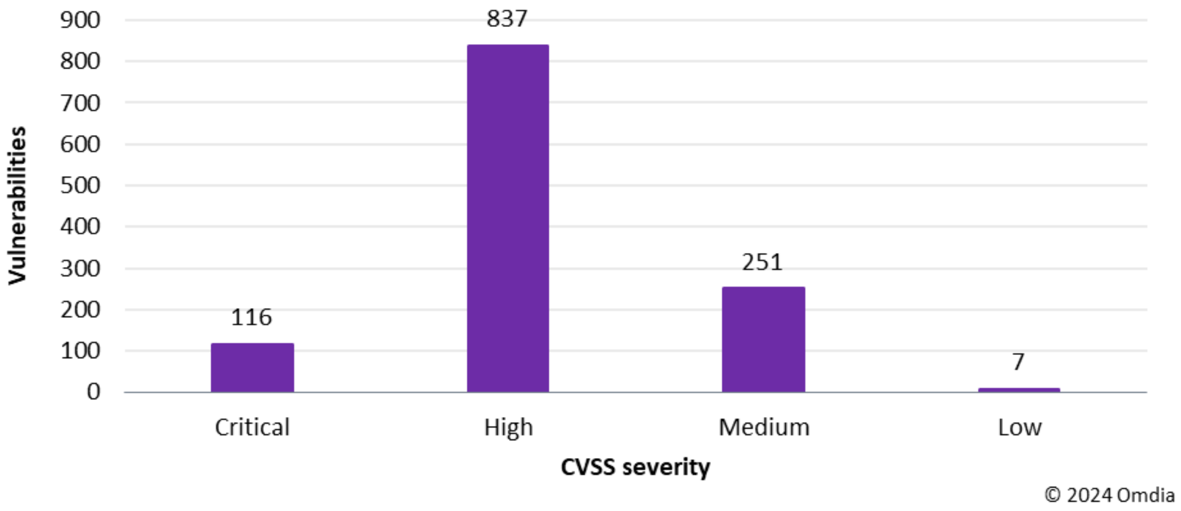
- Medium-level vulnerabilities can have a damaging impact an organization's data security, but they are often more challenging to exploit because specific requirements must be met in order to effectively exploit the vulnerability. Medium-scoring vulnerabilities were the second most common type, comprising 21% of all vulnerabilities.

- Low- or N/A-scored vulnerabilities have little to no impact on the data security of an organization and pose more of an annoyance than a legitimate threat. These low-grade threats accounted for *fewer than 1%* of all disclosed vulnerabilities.

Conclusion

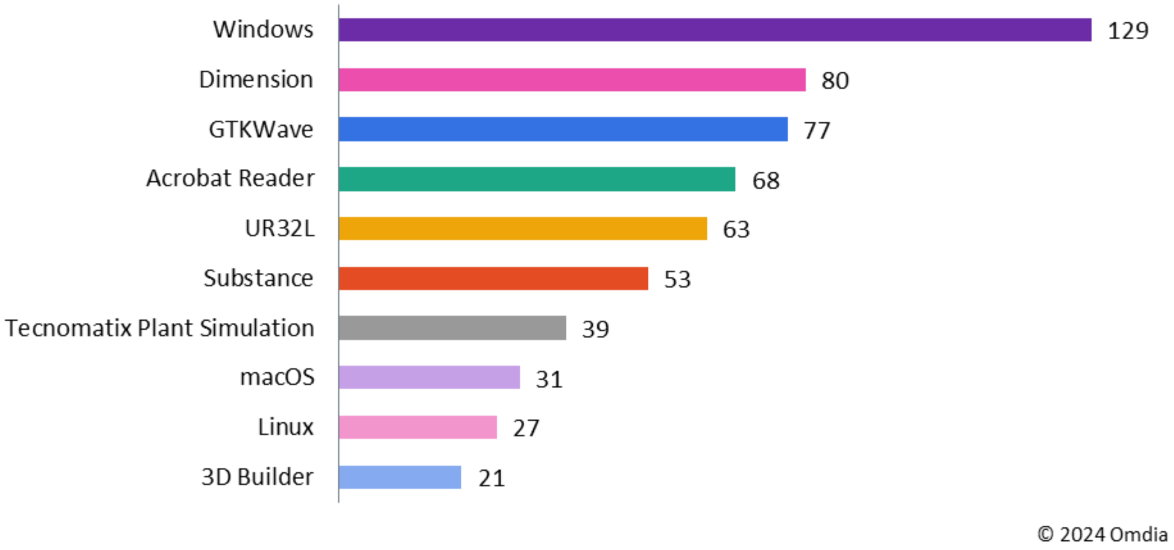
Each of the organizations analyzed as part of this research contributes to the industrywide effort to discover and disclose information security vulnerabilities. It is through the diligence of these vendors that the security of data can become more robust, because flaws can only be addressed once they are acknowledged. It is imperative that this work continue and, specifically, that discovery and reporting programs are continuously refined and improved if comprehensive security is to be achieved through the responsible management of vulnerabilities.

Figure 1: Vulnerabilities by CVSS score



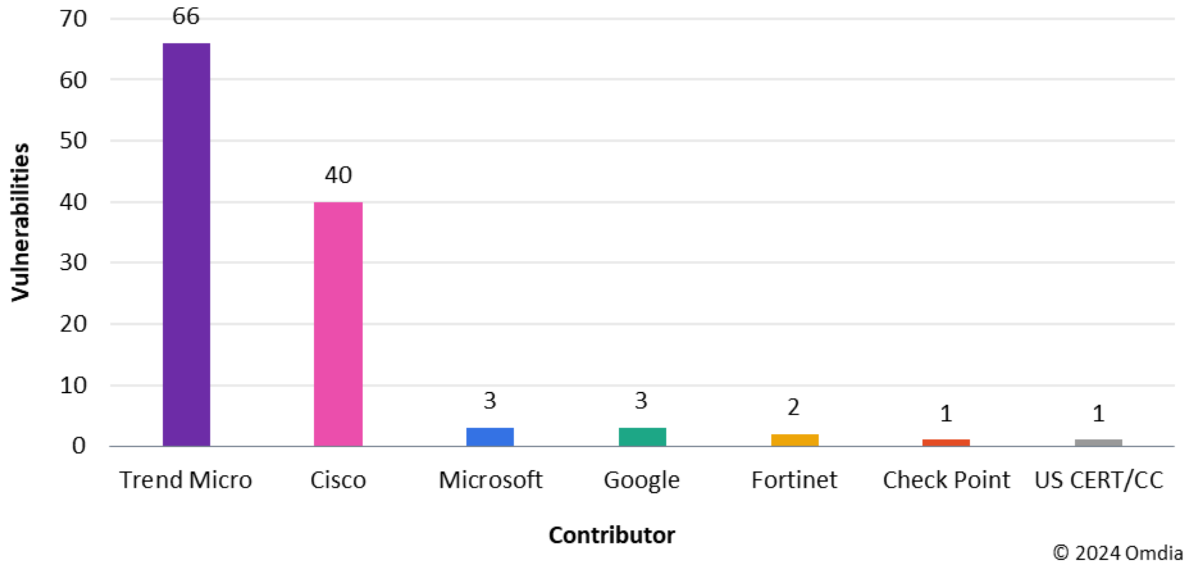
Source: Omdia

Figure 2: Vulnerabilities by product targeted



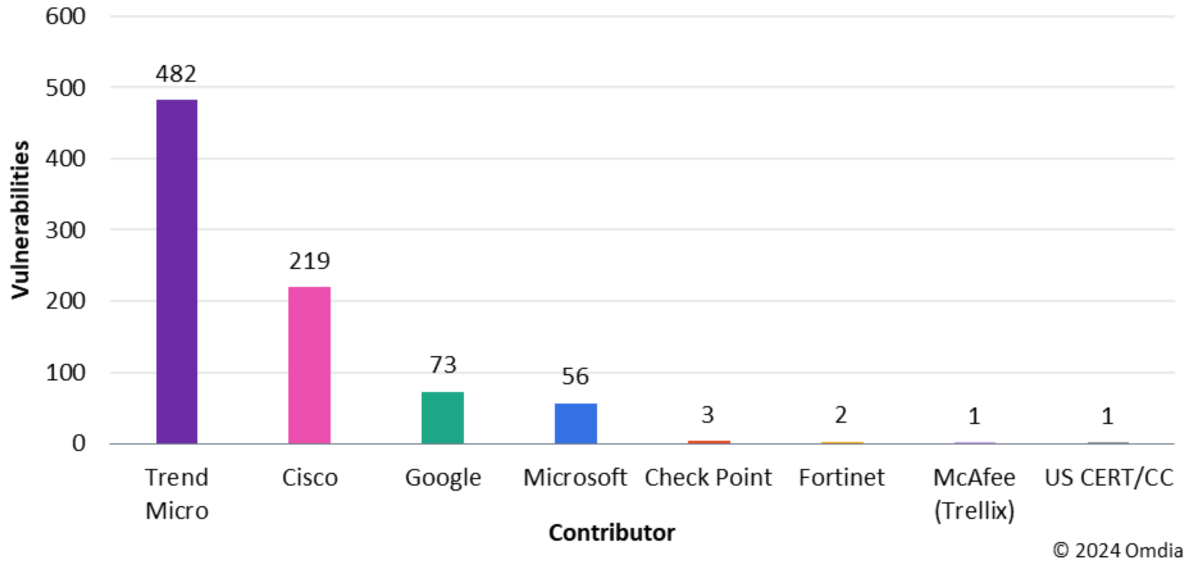
Source: Omdia

Figure 3: Critical vulnerabilities by contributor



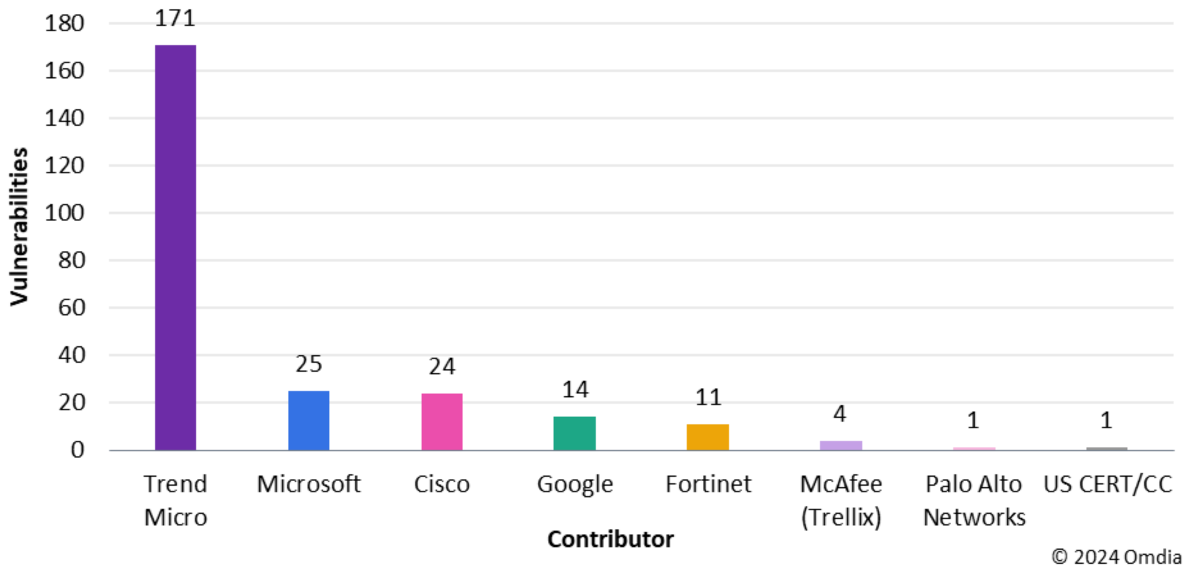
Source: Omdia

Figure 4: High-level vulnerabilities by contributor



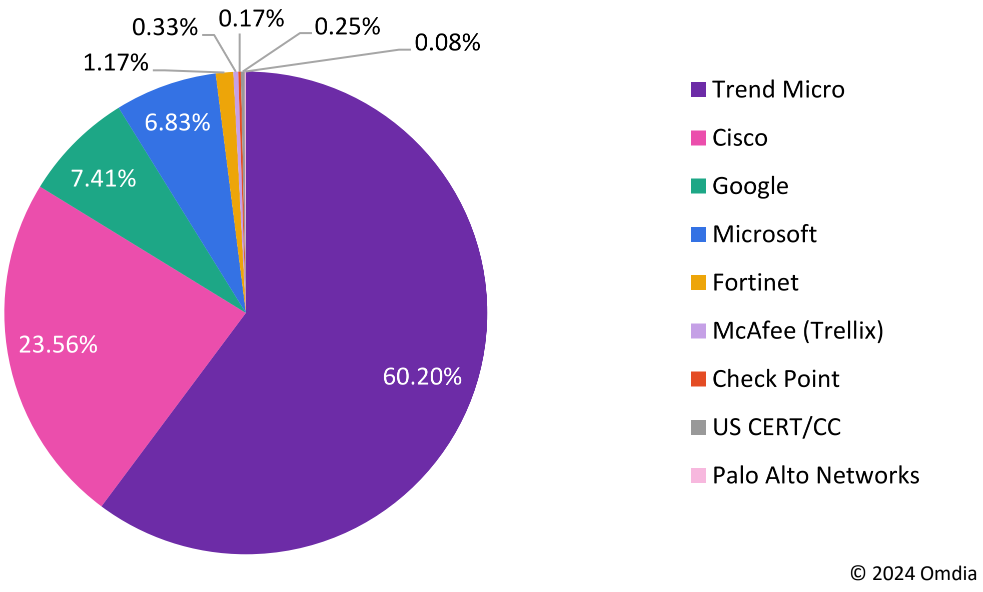
Source: Omdia

Figure 5: Medium-level vulnerabilities by contributor



Source: Omdia

Figure 6: Vulnerability market coverage, 2023



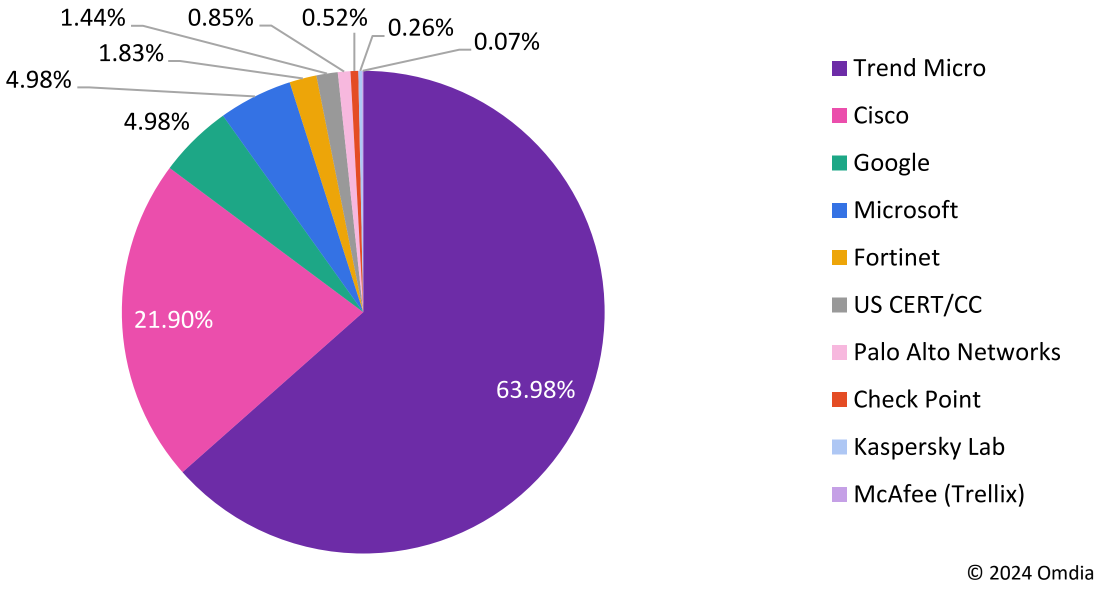
Source: Omdia

Table 1: Vulnerability market coverage, 2023

	Vulnerabilities managed	Average of base score	Average of exploitability score	Average of impact score
Trend Micro	725	7.46	2.15	5.22
Cisco	283	7.90	2.27	5.55
Google	91	7.59	2.18	5.32
Microsoft	84	7.34	2.54	4.74
Fortinet	15	6.63	2.22	4.06
McAfee (Trellix)	5	6.08	1.48	4.52
Check Point	4	8.08	3.90	4.18
US CERT/CC	3	7.70	2.50	5.13
Palo Alto Networks	1	5.40	2.80	2.50
Grand total	**1,211**	**7.55**	**2.21**	**5.25**

Source: Omdia

Figure 7: Vulnerability market coverage, 2021



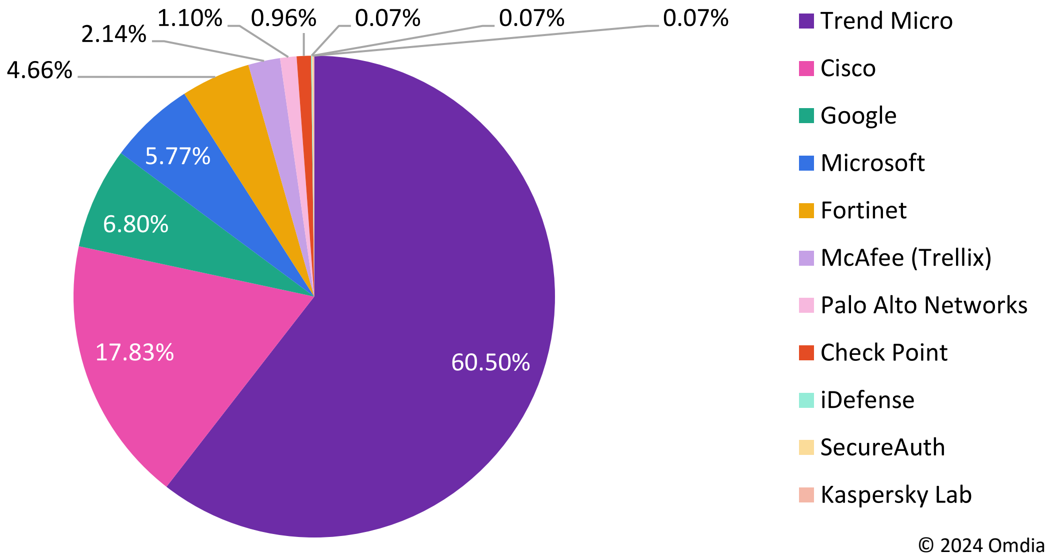
Source: Omdia

Table 2: Vulnerability market coverage, 2021

	Vulnerabilities managed	Average of base score	Average of exploitability score	Average of impact score
Trend Micro	984	7.34	2.08	5.15
Cisco	322	7.80	2.62	5.04
Google	81	7.93	2.35	5.46
Microsoft	76	7.77	2.57	5.05
Fortinet	30	6.57	2.29	4.09
US CERT/CC	23	8.20	3.02	5.05
Palo Alto Networks	13	7.60	1.95	5.55
Check Point	9	7.01	1.47	5.40
Kaspersky Lab	4	7.23	1.80	5.33
McAfee (Trellix)	1	7.80	1.80	5.90
Grand total	**1,543**	**7.49**	**2.25**	**5.12**

Source: Omdia

Figure 8: Vulnerability market coverage, 2020



© 2024 Omdia

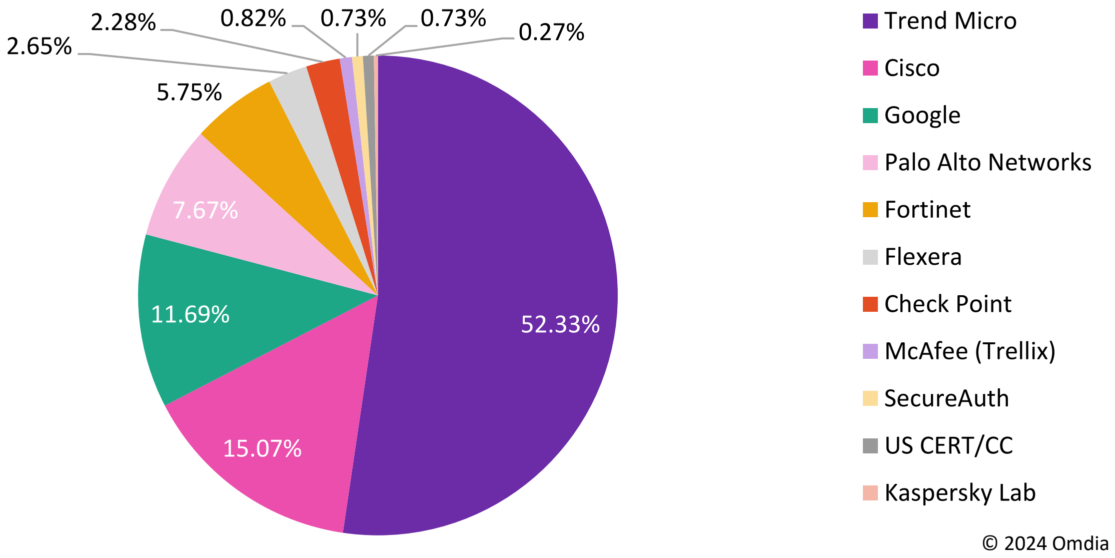
Source: Omdia

Table 3: Vulnerability market coverage, 2020

	Vulnerabilities managed	Average of base score	Average of exploitability score	Average of impact score
Trend Micro	825	7.64	2.47	5.05
Cisco	242	7.96	2.62	5.18
Google	100	7.53	2.25	5.15
Fortinet	79	7.80	2.17	5.54
McAfee (Trellix)	63	5.91	1.95	3.83
Palo Alto Networks	33	7.24	1.80	5.34
Check Point	16	8.41	2.74	5.62
US CERT/CC	15	8.11	2.46	5.49
iDefense	3	7.70	1.73	5.90
Kaspersky Lab	1	7.50	1.60	5.90
SecureAuth	1	5.40	2.80	2.50
Grand total	**1,378**	**7.62**	**2.42**	**5.07**

Source: Omdia

Figure 9: Vulnerability market coverage, 2019



Source: Omdia

Table 3: Vulnerability market coverage, 2019

	Vulnerabilities managed	Average of base score	Average of exploitability score	Average of impact score
Trend Micro	573	7.57	2.41	5.04
Cisco	165	7.90	2.91	4.91
Google	128	8.18	2.67	5.39
Palo Alto Networks	84	8.58	3.69	4.86
Fortinet	63	8.24	2.82	5.33
Flexera	29	6.51	3.54	2.92
Check Point	25	7.58	2.82	4.68
McAfee (Trellix)	9	6.09	1.19	4.81
SecureAuth	8	6.85	2.60	4.14
US CERT/CC	8	7.73	2.33	5.33
Kaspersky Lab	3	7.80	1.80	5.90
Grand total	**1,095**	**7.76**	**2.66**	**4.99**

Source: Omdia

Omdia has provided access to previous studies in order to facilitate a comparative annual analysis.

Historical data for CVEs include information from 2018 through 2021. Research was not conducted during 2022, and data for that year was excluded.

Appendix

Authors

Tanner Johnson
Principal Analyst, Data Security
customersuccess@omdia.com

Adam Strange
Principal Analyst, Data Security
customersuccess@omdia.com

Elvia Finalle
Analyst, Cybersecurity
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.