Publication date:
July 2022
Author:
Tanner Johnson

Quantifying the Public Vulnerability Market: 2022 Edition

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

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Trend Micro

Contents

Executive summary

Overview

Omdia conducted a comprehensive comparative analysis of the output of 11 organizations that disclose information security vulnerabilities. As part this research, Omdia cross-referenced data from these vendors against information organized and published by various government agencies, including the following:

- The MITRE Corporation
- The National Institute of Standards and Technology (NIST)
- The US Computer Emergency Response Team/Coordination Center (US CERT/CC)
  - While the US CERT/CC is listed alongside other reporting organizations, it is a government agency, not a security vendor.

Research scope

Omdia's analysis applied 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 2021 calendar year.
- All vulnerabilities must have been assigned a common vulnerability and exposure (CVE) number.
- Disclosed vulnerabilities with associated CVEs that were not credited to the organizations within our scope are not included or discussed as part of our overall analysis.
- In instances where two or more vendors claim credit for a vulnerability, Omdia grants credit to each vendor making the claim because there is no way to independently validate credit.
  - As many as 1,527 vulnerabilities were claimed once, and 8 vulnerabilities claimed twice.
  - This results in a total of 1,535 unique verified vulnerabilities.

- Since Omdia attributes credit for each vulnerability to all vendors that claim it, the total verified vulnerabilities claimed by the 10 research organizations for 2021 is 1,543.

Analysis methodology

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

- Primary internal research
- Individual vendor interviews
- Open source publications
- Publicly disclosed reports

Omdia collected all publicly available vulnerability data from 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; this means the organization directly oversaw the release of the vulnerability.

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

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

- To be verified, all vulnerabilities in Omdia's analysis must have an associated CVE number. This is to prevent the introduction of rejected or duplicated entries in the analysis. Vulnerabilities must also have a common vulnerability scoring system (CVSS) value assigned by the NVD.
- Vulnerabilities without a CVE, while still credited to their respective vendors, 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 their disclosed vulnerabilities, and the attack methodology of the vulnerabilities that each vendor was credited with.

Vulnerability market analysis

A vulnerability is a weaknesses, 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 these can be exploited in ways that compromise the systems on which they reside. The longer the duration between the

discovery of a vulnerability, its disclosure, and 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. Such vulnerabilities pose the greatest threat to information security and are viewed as the greatest prize for cybercriminals to attain and share. Since vulnerabilities can only be addressed once they are discovered and shared with 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 vulnerability identification and remediation 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 (with little to no impact) are merely annoying, while others are critical enough to have catastrophic consequences for vulnerable systems and their users.

To conduct a comprehensive analysis on any vulnerability, several characteristics and values must first be identified so they can be cross-referenced across reporting organizations:

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

Results

The CVSS scores attached to each vulnerability by the NVD provides organizations a visible metric by which to gauge a vulnerability's severity and help prioritize threat remediation tactics.

- Critical vulnerabilities are those yielding 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 denial of service (DoS). Threats are often elevated to this level if an attacker can gain access without any special conditions or advanced knowledge. Vulnerabilities with critical CVSS scores accounted for roughly 9% of all disclosed threats.

- High-level vulnerabilities can also substantially damage an organization's information security. However, vulnerabilities with high CVSS scores are traditionally more challenging to exploit because they require certain conditions to be first met. However, any exploitation can still result in privilege escalation and loss of data access. High-scoring vulnerabilities made up the most vulnerabilities disclosed, comprising 67% of such vulnerabilities.

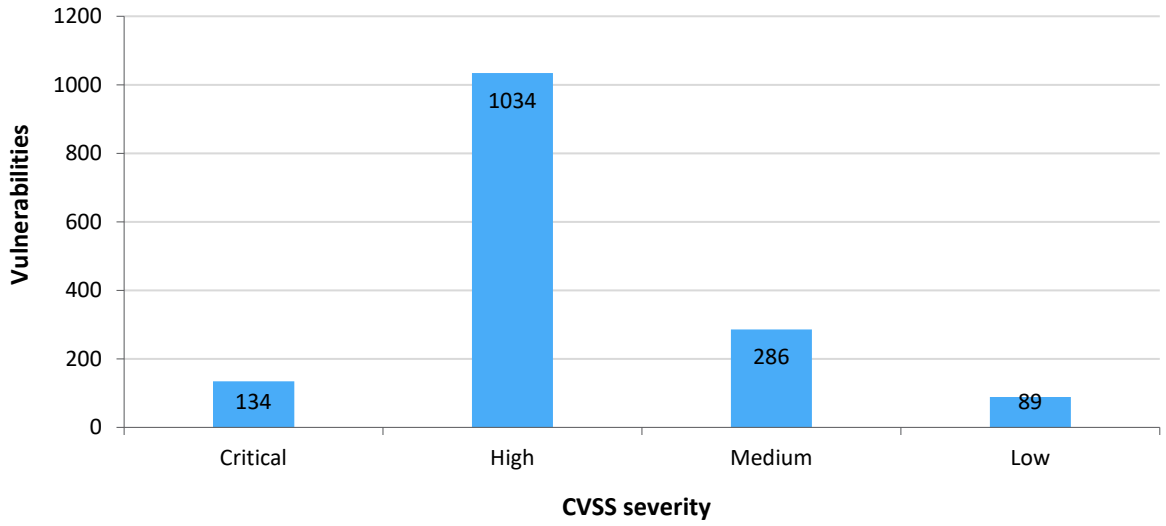
- Medium-level vulnerabilities can affect an organization's data security but are often more challenging to exploit, because specific requirements must be met to effectively exploit the vulnerability. Such vulnerabilities ranked second, comprising 18% of all vulnerabilities.

- Vulnerabilities with low or "N/A" CVSS scores have little to no impact on an organization's data security, appearing more as an annoyance than a legitimate threat. These low-grade threats accounted for less than 6% of all disclosed vulnerabilities.

Conclusion

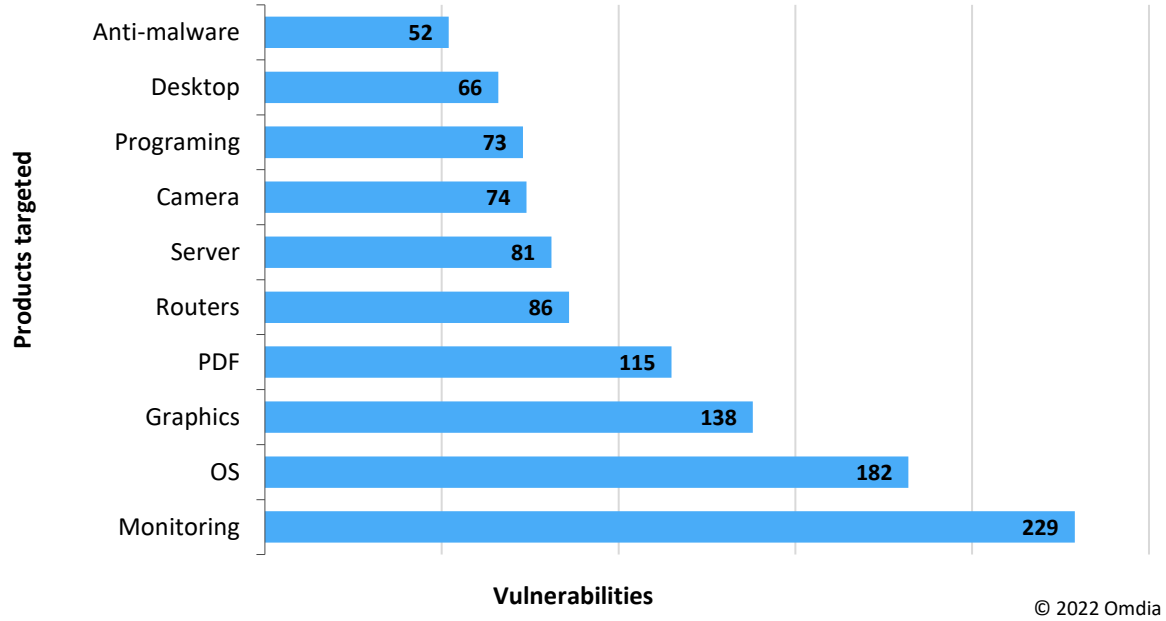
Each of the organizations analyzed as part of this research contributes toward industry-wide efforts to discover and disclose information security vulnerabilities. It is through the diligence of vendors such as these that data security can become more robust, because flaws can only be addressed once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

Figure 1: Number of vulnerabilities by CVSS severity



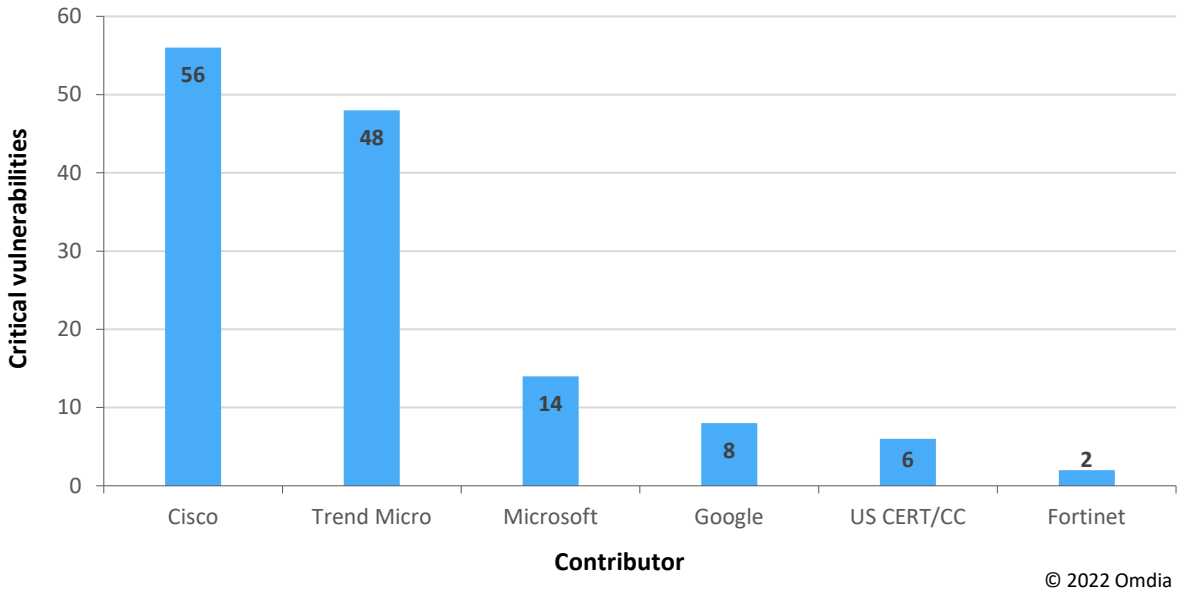
Source: Omdia

Figure 2: Number of vulnerabilities by type of products targeted



Source: Omdia

Figure 3: Number of critical vulnerabilities by contributor



Source: Omdia

Figure 4: Number of high vulnerabilities by contributor

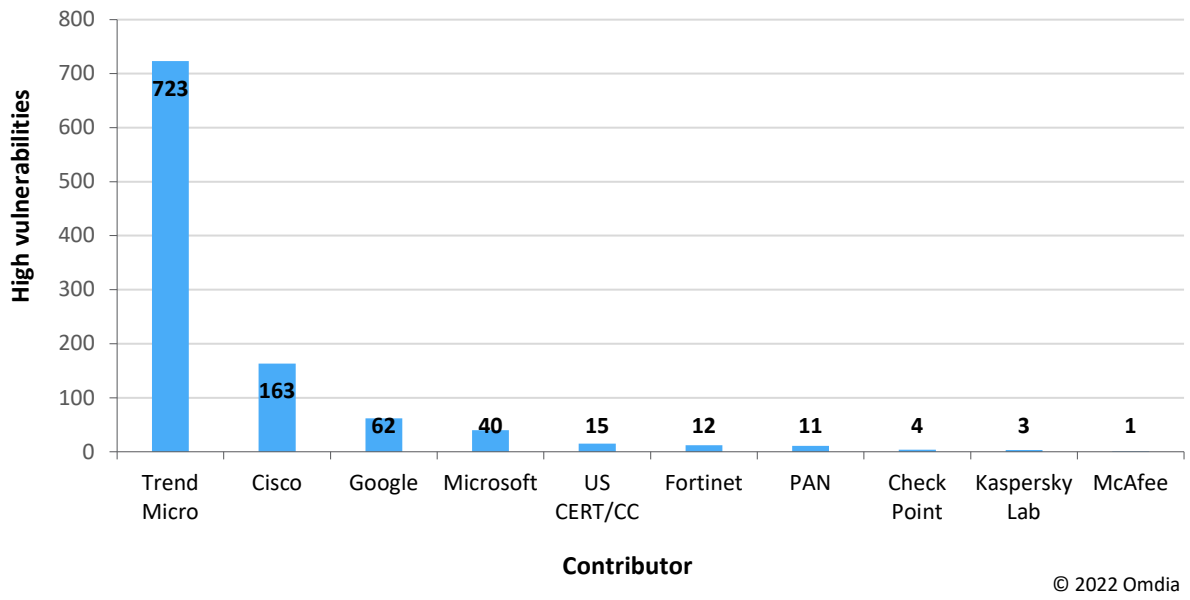
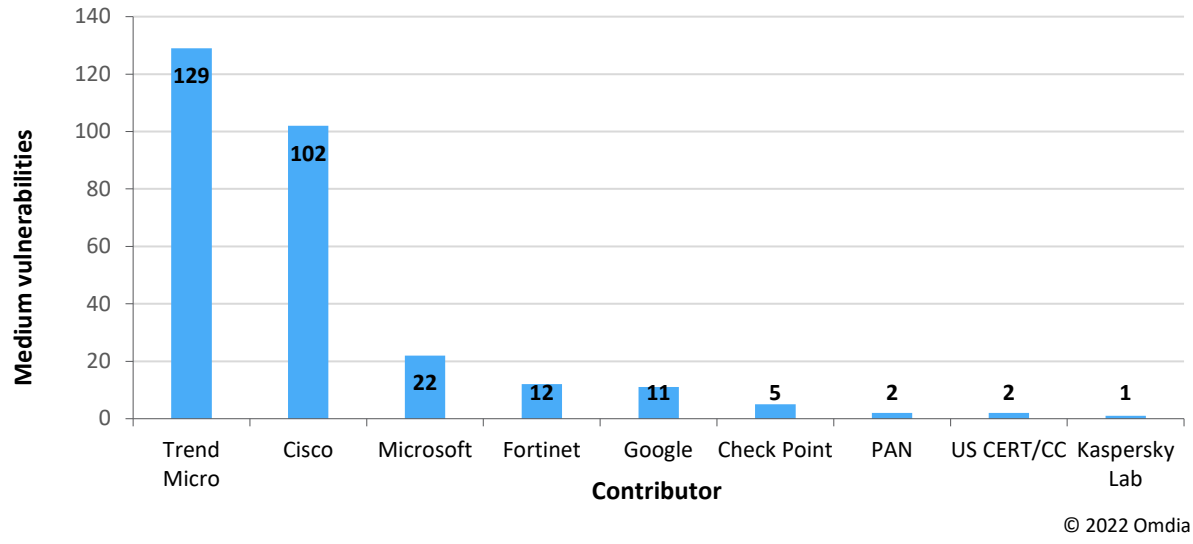


Figure 5: Number of medium vulnerabilities by contributor

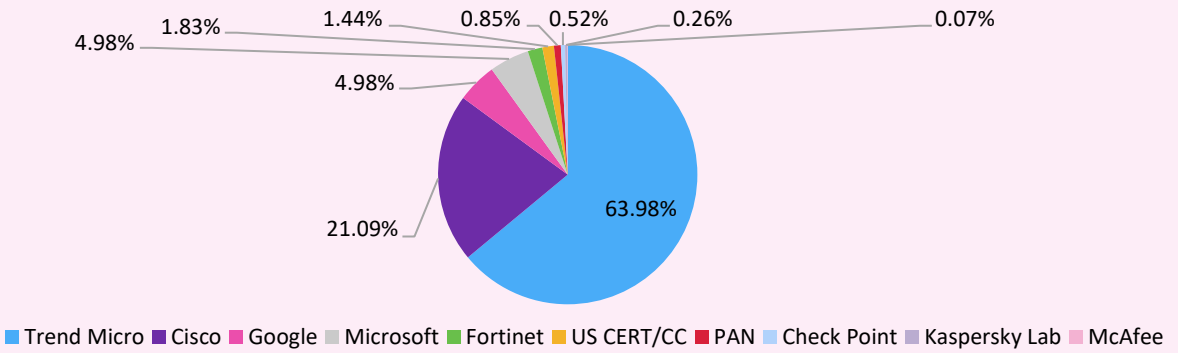


Source: Omdia

Appendix

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

Figure 6: Vulnerability market coverage, 2021



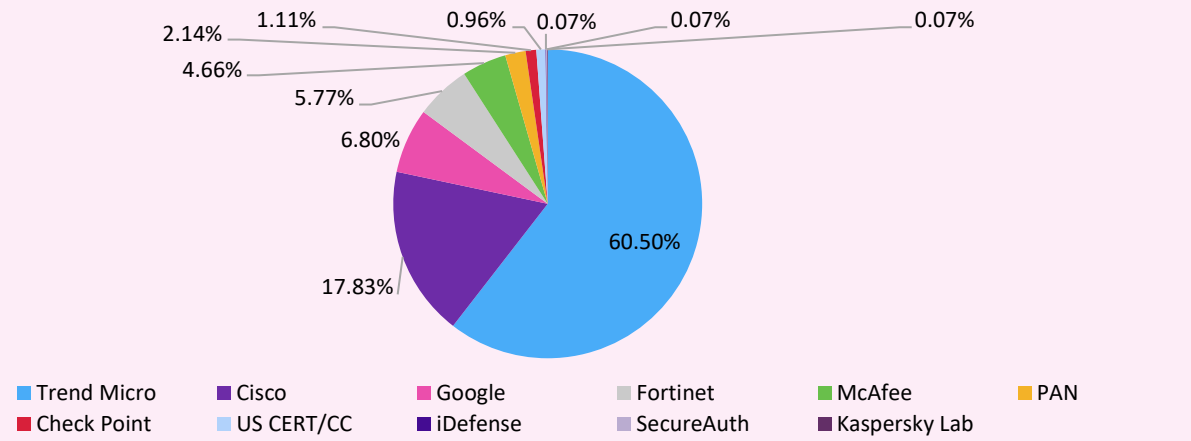
Source: Omdia

Table 1: Omdia's vulnerability market research findings, 2021

Contributor	Vulnerabilities managed	Average base score	Average exploitability score	Average impact score
Trend Micro	984	7.34	2.08	5.15
Cisco	322	7.8	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	8.2	3.02	5.05
PAN	13	7.6	1.95	5.55
Check Point	9	7.01	1.47	5.4
Kaspersky Lab	4	7.23	1.8	5.33
McAfee	1	7.8	1.8	5.9
Grand total	**1,543**	**7.49**	**2.25**	**5.12**

Source: Omdia

Figure 7: Vulnerability market coverage, 2020



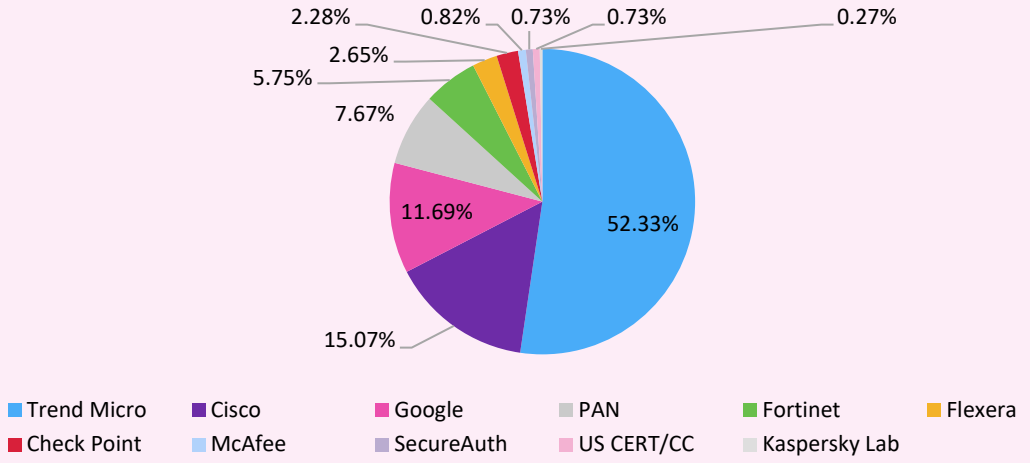
Source: Omdia

Table 2: Omdia's vulnerability market research findings, 2020

Contributor	Vulnerabilities managed	Average base score	Average exploitability score	Average 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	7.8	2.17	5.54
McAfee	63	5.91	1.95	3.83
PAN	33	7.24	1.8	5.34
Check Point	16	8.41	2.74	5.62
US CERT/CC	15	8.11	2.46	5.49
iDefense	3	7.7	1.73	5.9
Kaspersky Lab	1	7.5	1.6	5.9
SecureAuth	1	5.4	2.8	2.5
Grand total	**1,378**	**7.62**	**2.42**	**5.07**

Source: Omdia

Figure 8: Vulnerability market coverage, 2019



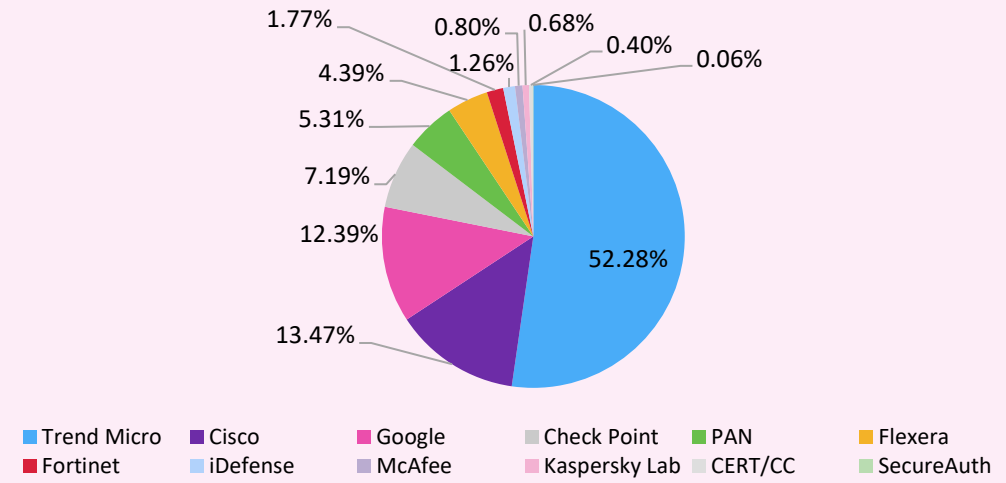
Source: Omdia

Table 3: Omdia's vulnerability market research findings, 2019

Contributor	Vulnerabilities managed	Average base score	Average exploitability score	Average impact score
Trend Micro	573	7.57	2.41	5.04
Cisco	165	7.9	2.91	4.91
Google	128	8.18	2.67	5.39
PAN	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	9	6.09	1.19	4.81
SecureAuth	8	6.85	2.6	4.14
US CERT/CC	8	7.73	2.33	5.33
Kaspersky Lab	3	7.8	1.8	5.9
Grand total	**1,095**	**7.76**	**2.66**	**4.99**

Source: Omdia

Figure 9: Vulnerability market coverage, 2018



Source: Omdia

Table 4: Omdia's vulnerability market research findings, 2018

Contributor	Vulnerabilities managed	Average base score	Average exploitability score	Average impact score
Trend Micro	916	7.64	2.49	5.04
Cisco	236	7.83	2.34	5.33
Google	217	6.31	1.79	4.43
Check Point	126	7.45	2.61	4.79
PAN	93	7.22	2.48	4.66
Flexera	77	7.1	2.7	4.31
Fortinet	31	7.81	2.19	5.5
iDefense	22	7.7	2.61	5.01
McAfee	14	7.49	2.06	5.26
Kaspersky Lab	12	8.04	2.46	5.52
CERT/CC	7	8.53	3.74	4.76
SecureAuth	1	7.8	1.8	5.9
Grand total	**1,752**	**7.45**	**2.4**	**4.95**

Source: Omdia

Author

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

Get in touch

www.omdia.com
askananalyst@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