



# Quantifying the Public Vulnerability Market: 2021 Edition

An Analysis of Vulnerability Disclosures, Impact Severity, and Product Analysis

# Omdia's Overall Research Methodology

## Overview

Omdia conducted comprehensive comparative research and analysis examining the output of 11 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)
  - While listed with other reporting organizations, the US CERT/CC is a U.S. government agency, 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 they are ultimately responsible for managing the disclosure of the vulnerability.
- All vulnerabilities must have been disclosed within the 2020 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 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, as there is no way to independently validate credit.
  - **1,352** vulnerabilities were claimed once, and **13** vulnerabilities claimed twice.
  - This results in a total of **1,365** unique and verified vulnerabilities.
- As Omdia attributes credit for each vulnerability to all vendors who claimed it, the resulting total number of all verified vulnerabilities claimed by the 11 research organizations for 2020 is **1,378**.

## Analysis Methodology

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

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

Omdia collected all publicly available vulnerability data from each of the organizations listed in the executive summary and assigned credit for each vulnerability. However, in order 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 their publicly facing advisory website.

Omdia then collected data on all verified vulnerabilities during 2020 using the NIST 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, as well as have a CVSS value assigned by the NVD.
- Vulnerabilities without a CVE, while still credited to the respective vendor, are not include in Omdia's analysis.

The CVSS and 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 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, as they can be exploited in ways that compromise the systems on which they reside. The greater the window of time 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. Simultaneously, zero-day vulnerabilities pose the greatest threat to information security, and are viewed as the greatest prize for cybercriminals to attain and share. As 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 hasn't 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, as some security flaws may merely be annoying, others are critical enough to have potentially catastrophic consequences for the vulnerable systems and its users.

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

- Common Vulnerability and Exposure (CVE) values
  - Unique identifier given to each vulnerability by a CVE Numbering Authority (CNA)
- Common Weakness Enumeration (CWE) values
  - Preliminary identifier used to categorize and define common software weaknesses
- Common Vulnerability Scoring System (CVSS) values
  - 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 gage 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/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. Critical scoring vulnerabilities accounted for roughly **15%** of all disclosed threats.

**High-level vulnerabilities** can also have substantially damaging effects to the information security of an organization. However, vulnerabilities scored as high are traditionally more challenging to exploit, as they require certain conditions be met first. Although, 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 **62%** of all vulnerabilities.

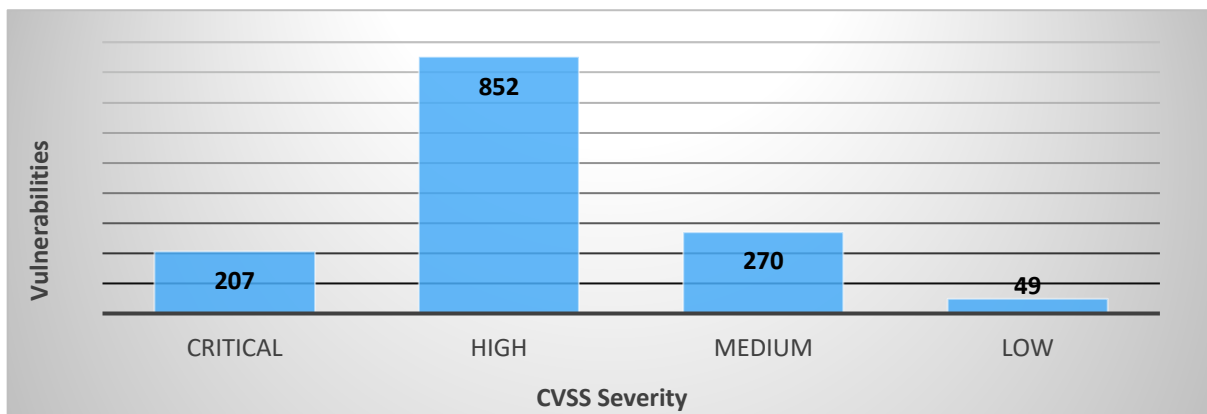
**Medium-level vulnerabilities** can have negative impacts on an organization's data security, but often more challenging to exploit, as specific requirements must be met in order to effectively exploit the vulnerability. Medium scoring vulnerabilities were ranked second, comprising **20%** of all vulnerabilities.

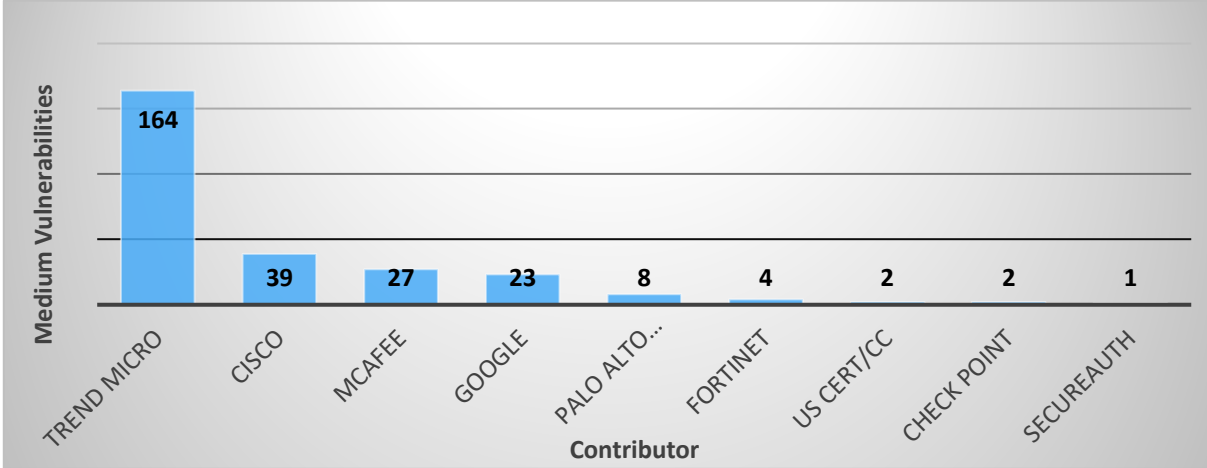
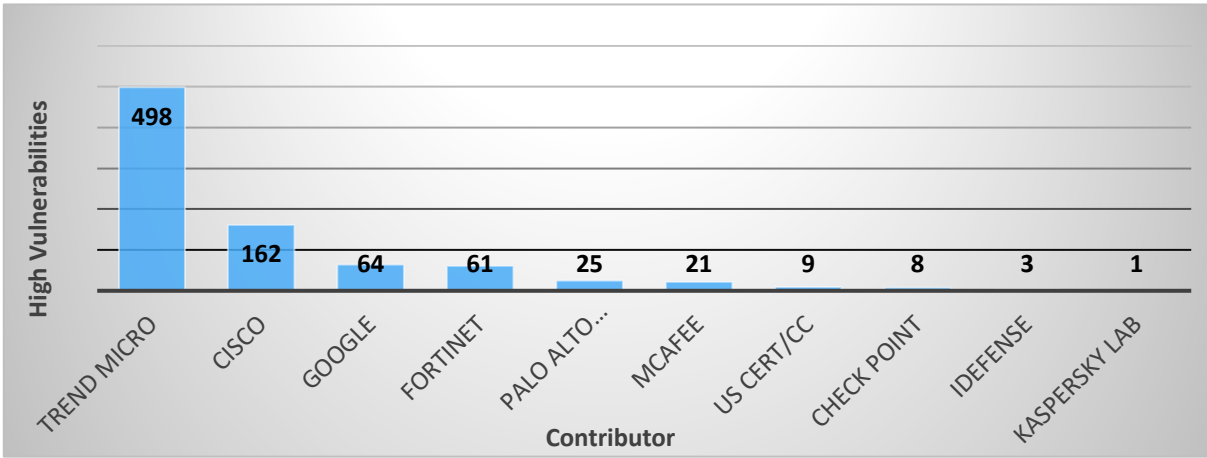
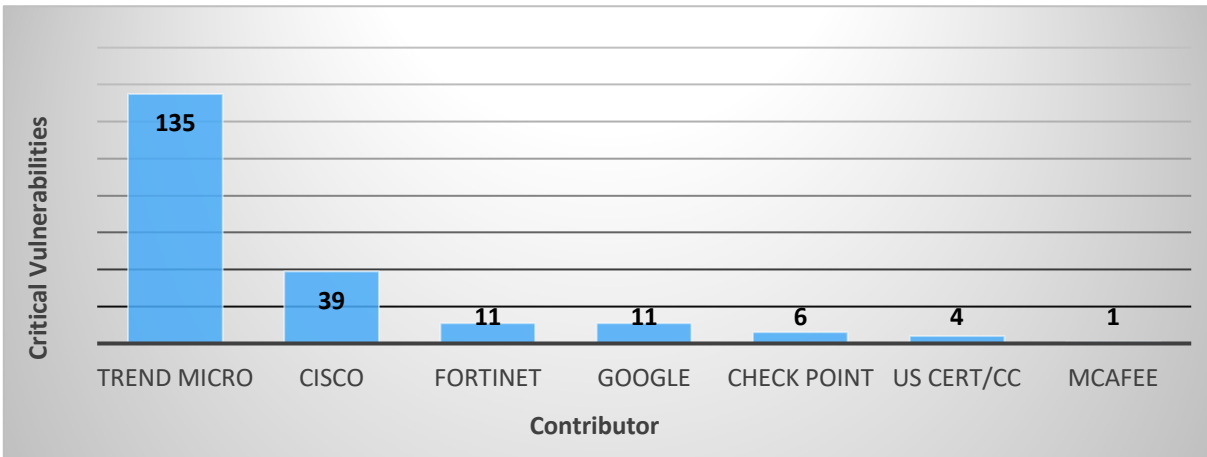
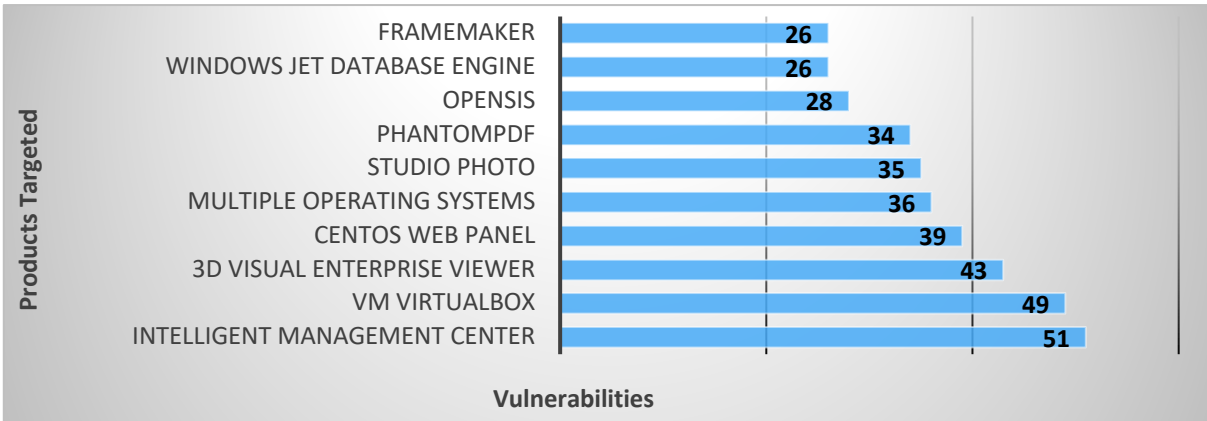
- **Low- or N/A-scored vulnerabilities** have little to no impact on the data security for an organization, and pose more of an annoyance than a legitimate threat.

These low-grade threats accounted for **less than 3%** of all disclosed vulnerabilities.

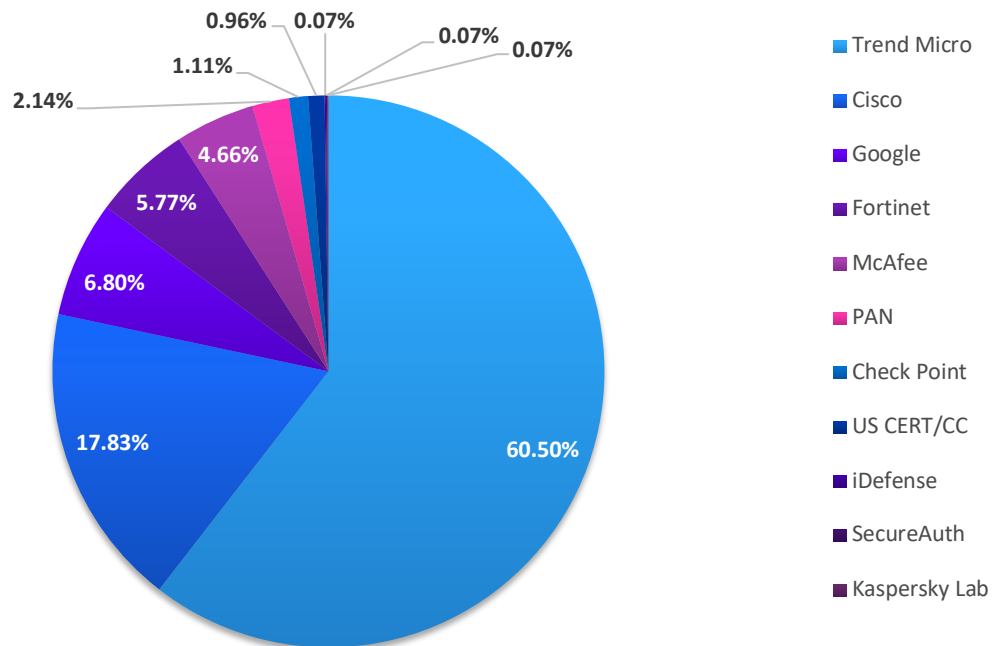
## Conclusion

Each of the organizations analyzed as part of this research contributes toward the industry-wide effort to discover and disclose information security vulnerabilities. It is through the diligence of vendors such as these that the security of data can become more robust, as 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.



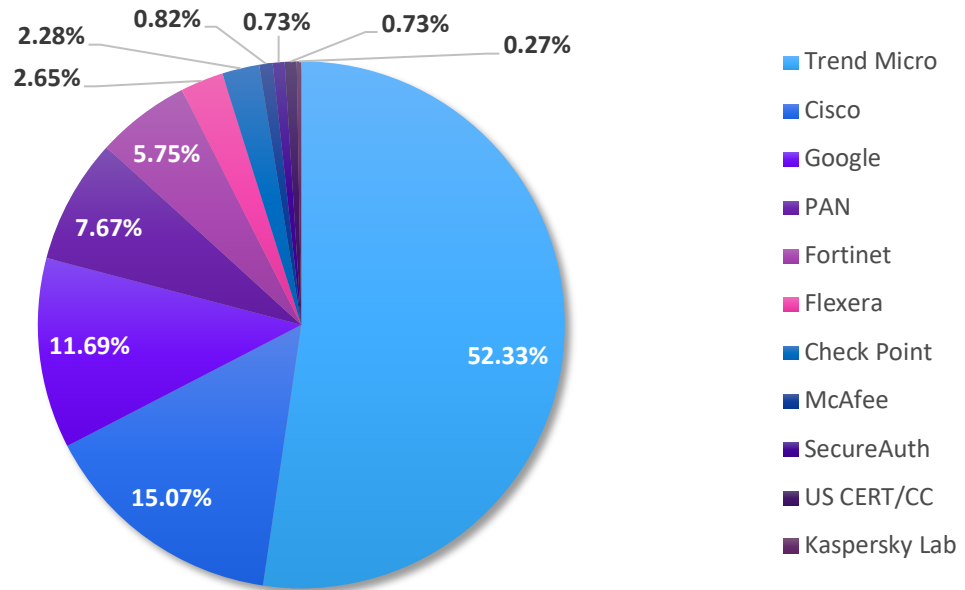


### VULNERABILITY MARKET COVERAGE - 2020



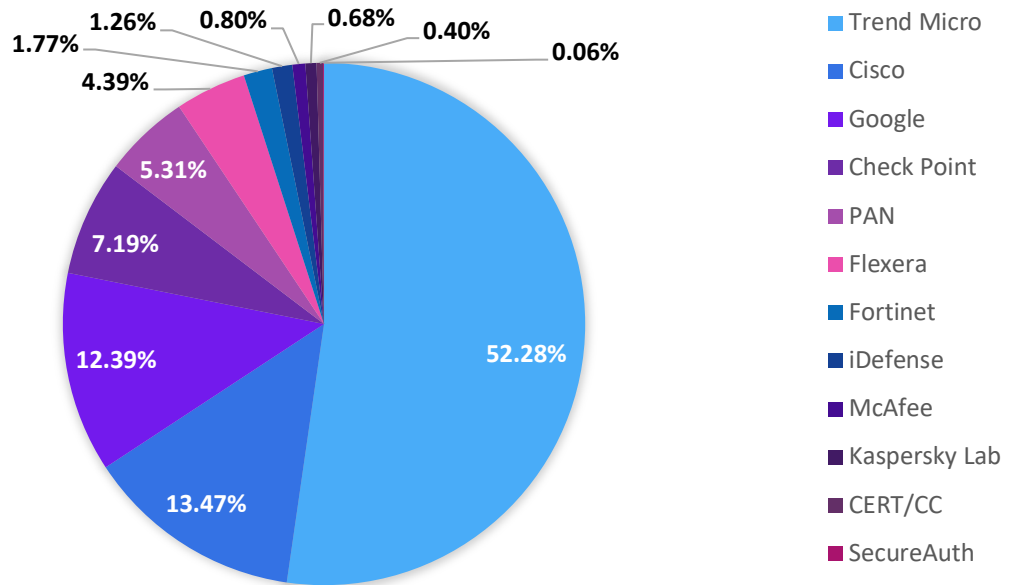
Omdia Research - 2020	Vulnerabilities Managed	Average of Base Score	Average of Exploitability Score	Average of Impact Score
Trend Micro	825	7.64	2.47	5.05
Cisco	242	7.96	2.62	5.18
Google	100	7.53	2.25	5.15
Fortinet	79	7.80	2.17	5.54
McAfee	63	5.91	1.95	3.83
PAN	33	7.24	1.80	5.34
Check Point	16	8.41	2.74	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
<b>Grand Total</b>	<b>1378</b>	<b>7.62</b>	<b>2.42</b>	<b>5.07</b>

### VULNERABILITY MARKET COVERAGE - 2019



Omdia Research - 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
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	2.60	4.14
US CERT/CC	8	7.73	2.33	5.33
Kaspersky Lab	3	7.80	1.80	5.90
<b>Grand Total</b>	<b>1095</b>	<b>7.76</b>	<b>2.66</b>	<b>4.99</b>

### VULNERABILITY MARKET COVERAGE - 2018



IHS Markit Research - 2018	Vulnerabilities Managed	Average of Base Score	Average of Exploitability Score	Average of 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	7.10	2.70	4.31
Fortinet	31	7.81	2.19	5.50
iDefense	22	7.70	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	7.80	1.80	5.90
<b>Grand Total</b>	<b>1752</b>	<b>7.45</b>	<b>2.40</b>	<b>4.95</b>



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

## Author

Tanner Johnson, Principal Analyst, Data Security

[tanner.johnson@omdia.com](mailto:tanner.johnson@omdia.com)

## 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”) 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 and agents, 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.



## CONTACT US

[omnia.com](https://www.omnia.com)

[askananalyst@omnia.com](mailto:askananalyst@omnia.com)