OMDIA

Brought to you by Informa Tech

2023 Cybersecurity Horizon: Near-Term Trends

2022 Omdia

Omdia's cybersecurity analyst team – trend authors, market experts, and influencers

Maxine Holt
Senior Director
Cybersecurity

Eric Parizo
Managing Principal Analyst
Cybersecurity

Rik Turner
Senior Principal Analyst
Emerging Cybersecurity

Fernando Montenegro
Senior Principal Analyst
Infrastructure Security

Andrew Braunberg
Principal Analyst
Security Operations

Don Tait
Senior Analyst
Identity, Authentication, Access

Ketaki Borade
Senior Analyst
Security Operations

Hollie Hennessy
Senior Analyst
IoT Cybersecurity

Elvia Finalle
Senior Analyst
Security Operations

Curtis Franklin
Senior Analyst
Enterprise Security Management

Welcome

Welcome to this 2023 Cybersecurity Horizon report, where we explore key trends identified by Omdia's cybersecurity analyst team.

2022 has seen the pandemic wind down in many parts of the world, with travel returning. We are seeing no signs of a slow down in the desire or plans for organizational innovation. Indeed, much of the frenetic activity since the start of 2020 has continued unabated through 2022 and although there are more signs of fiscal prudence for 2023, the need to stay "ahead of the game" and take advantage of digital opportunities continues.

Digital opportunities bring digital dependence. Digital dependence brings the need for digital resilience. And cyber-resilience is a core component of digital resilience. It ensures that the organization continuously operates despite security incidents and breaches.

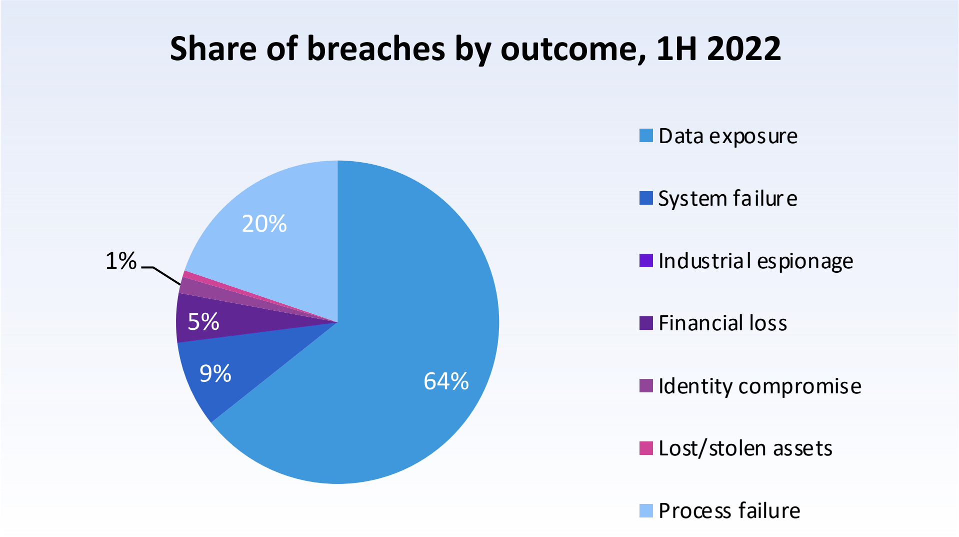
Maxine Holt
Senior Director
Cybersecurity

"Cyber-resilience is a core component of digital resilience - yet 40% of organizations still have significant gaps in their security controls"

To this end, 2023 will bring increased scrutiny of today's cybersecurity controls and the ability to withstand security incidents and breaches. According to Omdia's IT Enterprise Insights, although around 60% of organizations believe that they are currently advanced in their ability to manage security, identity, and privacy, this leaves the remainder of 40% with significant gaps in their security controls. These organizations are not resilient. They may fail if hit by ransomware, business email compromise, supply chain attacks, and so much more. Even temporary failure can significantly impact the ability to do business or service citizens.

Data exposure was the leading outcome of security breaches during the first half of 2022

Omdia’s security breaches tracker shows that data exposure was the leading outcome of security breaches during the first half of 2022 (see opposite). Consistently, since 2019, data exposure accounts for around two-thirds of breach outcomes. Healthcare was the biggest sector to be impacted by security breaches in 1 H22; government and healthcare have interchanged “top spot” over the preceding three years.



As part of the need to address cyber-resilience and minimize breaches, over 60% of organizations are planning to invest in cybersecurity products and services across the board during 2023 – making strategic or minor investment. Cybersecurity is a huge growth area.

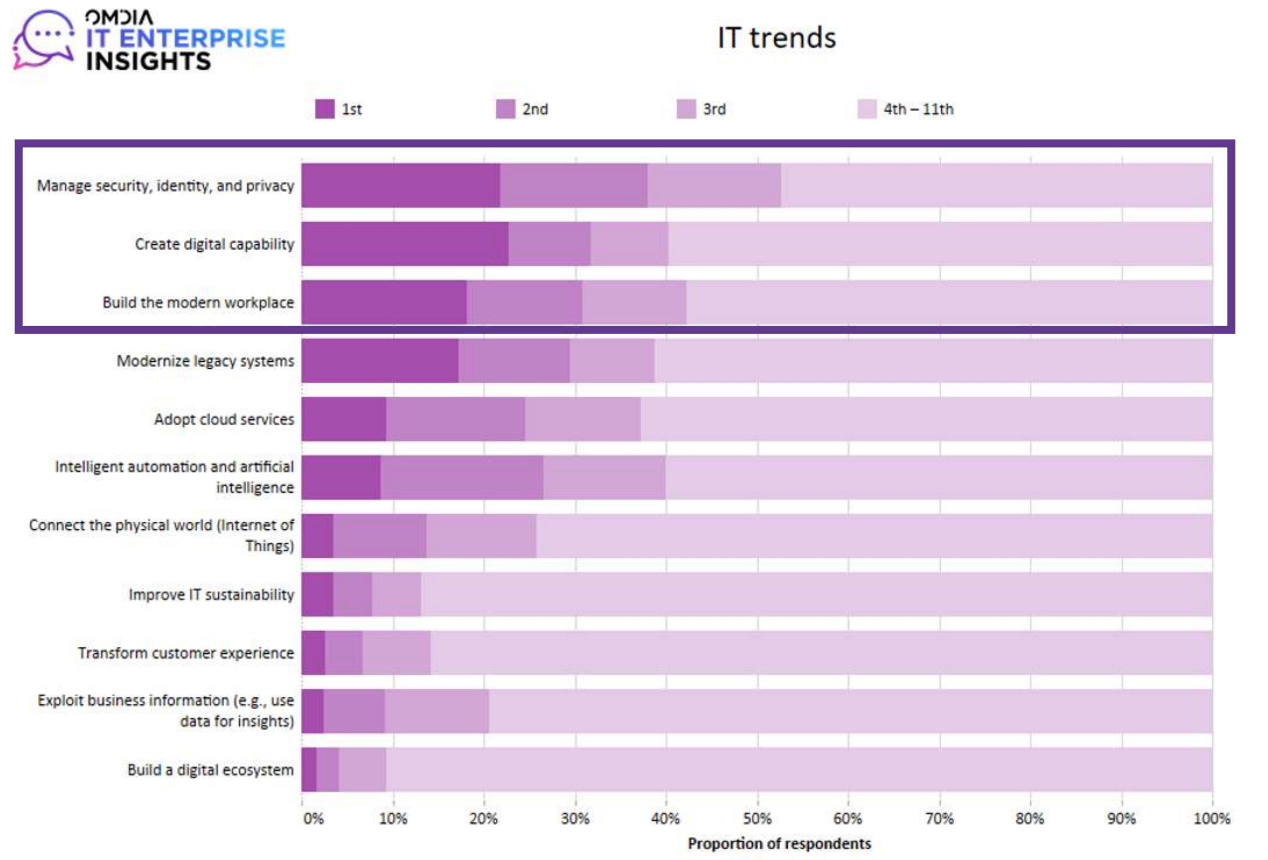
Omdia’s extensive cybersecurity research portfolio includes market sizing, competitive insights, market predictions & trends, emerging technologies, and more. This Omdia Predicts report scratches the surface of our research across data security, identity, authentication, access, infrastructure security, security operations, IoT cybersecurity, enterprise security management, and more.

I hope you enjoy this report!

Maxine

Turbo-charged 2022

Innovation continues to be turbo-charged, with security included



© Omdia 2022. All rights reserved.

Sample size: 4,769
Question: How important are the above technology areas to your organization?
Vertical: All. Subvertical: All. Country: All. Enterprise size: All.

Manage security, identity, privacy

22% Top priority

16% Second-highest priority

15% Third-highest priority

Create digital capability

23% Significantly more important

9% More important

8% Third-highest priority

Build the modern workplace

18% Significantly more important

13% More important

11% Third-highest priority

Trends overview

Top-level trends across the Omdia Cybersecurity Ecosystem

Data Security	Identity, Authentication, Access	Infrastructure Security	Security Operations	Enterprise Security Management	IoT Cybersecurity	Emerging Cybersecurity
Organizations will continue to fail customers' data privacy expectations	Decentralized identity gaining traction	Continued evolution of network security functionality into services drives SASE adoption	Risk-based vulnerability management (RBVM) makes inroads to reduce attack surface	COVID-19 hangover leaves enterprise security headaches	Regulation puts pressure on IoT manufacturers	Data becomes the latest area for the application of security posture management
Data becomes the latest area for the application of security posture management	Identity detection and response gathers momentum	Cloud security offerings go beyond the purpose-built cloud-security platform	Identity detection and response (IDR) provide additional security to an organization's identity architecture	Security executives find themselves in legal crosshairs	Top priority for OT and healthcare alongside IoT	SaaS security becomes more complex; enter CSAPP
The race is on to provide quantum-safe encryption algorithms	Continued market consolidation despite economic uncertainty	Security interest in 5G grows as 5G-enabled business initiatives increase in 2023	The interoperability of extended detection and response (XDR) to improve to drive adoption	Cyber-risk metrics push toward portability	5G connectivity highlights the need to secure IoT	XDR moving beyond identity – bringing in data detection and response

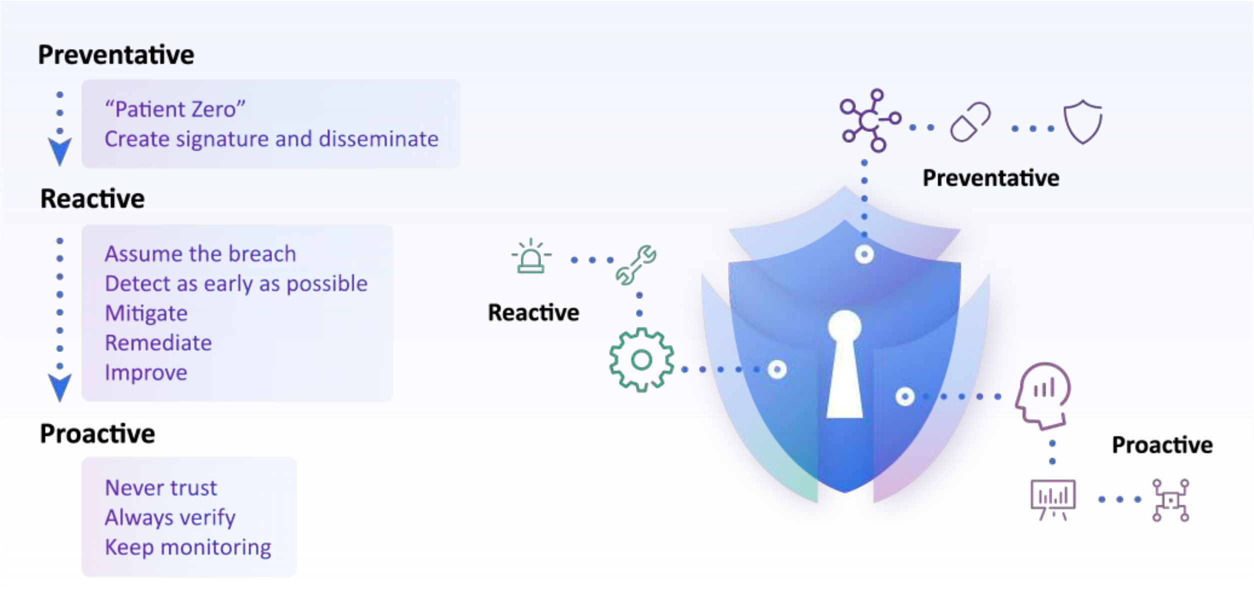
Data security: Data is the latest area for security posture management (SPM)

In 2022 Omdia has introduced the third “era” of cybersecurity technology – that of proactive security (see diagram opposite). This era is not a replacement for preventative and/or reactive, but instead is a complement.

Security posture management (SPM) has been a growing trend for proactive security in the cloud era. It started with cloud security posture management (CSPM), seeking misconfigurations in IaaS and PaaS environments that can result in vulnerabilities.

In the last couple years it has expanded into SaaS security posture management, doing essentially the same thing for SaaS apps. Now we are seeing the emergence of data security posture management (DSPM), with firms such as Cyera, Laminar, Uptycs, Veza, and Xage are all vying for visibility in this expanding segment.

The three “eras” of cybersecurity technology



Preventative

“Patient Zero”
Create signature and disseminate

Reactive

Assume the breach
Detect as early as possible
Mitigate
Remediate
Improve

Proactive

Never trust
Always verify
Keep monitoring

Source: Omdia

© 2022 Omdia

Identity, Authentication, Access: Continued market consolidation despite economic uncertainty

In 2022 there was a considerable amount of market consolidation in the form of mergers and acquisitions. Some of the more notable acquisitions in 2022 included:

- Thoma Bravo acquired Sailpoint (April 2022), Ping Identity (August 2022), and ForgeRock (October 2022)
- OpenText acquired Micro Focus (August 2022)
- Thales acquired OneWelcome (July 2022)

Despite the global economic slowdown, Omdia believes that there will still be market consolidation and M&A activity in the IAA market in 2023.

Some companies will struggle during this period and will be more prone to takeover bids. Companies that have large cash reserves may want to increase their presence in the IAA market by acquiring struggling companies.

Microsoft’s decision to go bigger on identity and access capabilities with the launch of its Entra product family in June 2022 shows that the identity space is becoming more popular and strategic with large cybersecurity and IT players.

Source: Freepik and Omdia

@ 2022 Omdia

Identity, Authentication, Access: Continued market consolidation despite economic uncertainty

Player type	What will the impact be?	Impact rating	How should players respond?
Vendors	As the market consolidates through merger and acquisition activity, vendors that play in this space will see stronger competition. This will come from vendors that have increased their market share through M&A activity.	+2 +1 – ◄ -1 -2	Companies that plan on acquiring other vendors must be in a strong financial position with good cash reserves. As global economic conditions worsen, companies on a strong financial footing will be able to take advantage of companies that are struggling.
Service providers	With an increase in M&A activity and market consolidation, service providers may find that there is less choice in terms of IAA products and solutions.	+2 +1 – ◄ -1 -2	Service providers that can handle decentralized identity and IDR should scope out business opportunities in this area.
Enterprises	Market consolidation within the identity, authentication, and access space may lead to less choice in terms of the number of products/solutions that an enterprise could potentially purchase.	+2 +1 ◄ – -1 -2	Enterprises need to make sure that the vendors that they plan to use for decentralized identity and IDR solutions are financially secure.

Source: Omdia

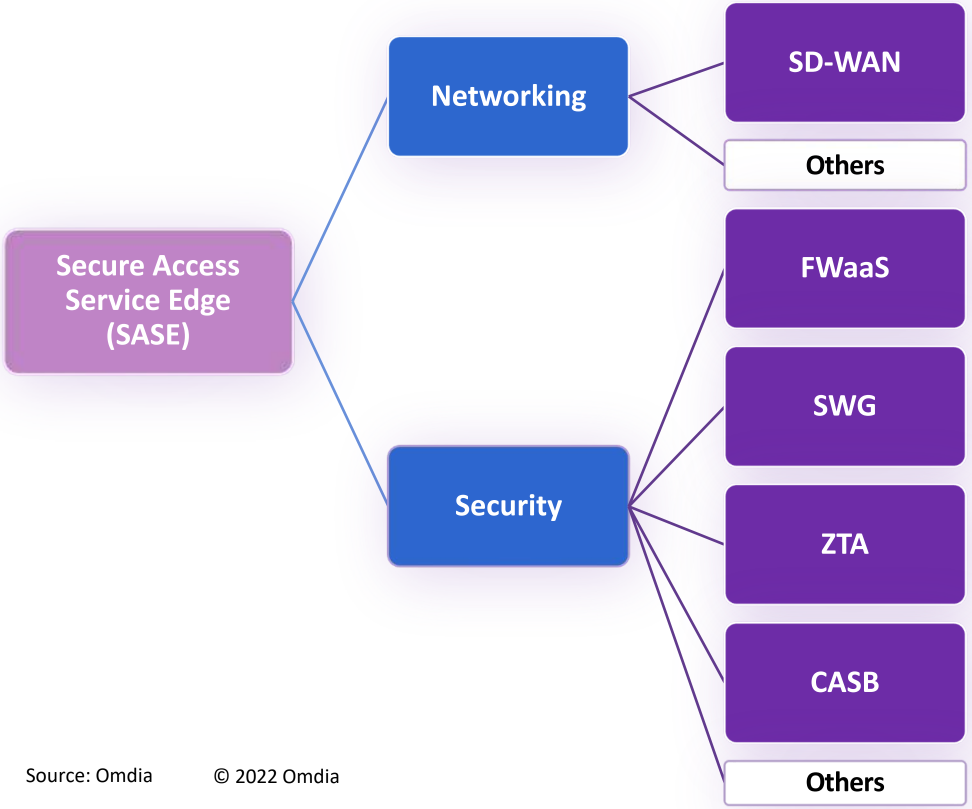
Infrastructure Security: Continued evolution of network security functionality into services drives SASE adoption

Secure Access Service Edge (SASE) has been around as a concept for a few years: the idea being that a "service edge," typically defined as a set of network endpoints between end users or branches on one side and the rest of the corporate network on the other, includes both networking and security functionality that would otherwise be deployed by the organization either directly at the endpoints or inside corporate data centers. Key use cases include software-defined WAN (SD-WAN) for optimized networking, and Secure Web Gateway, Zero Trust Access, and Firewall-as-a-Service as key security functions offered by SASE (see diagram opposite).

The benefits of SASE include optimized delivery of networking and security functionality: lower latency for end users, simplified footprint at the branch/end user location, and centralized upgrades and management for the equipment responsible for key functionality. To that, one can add the ease with which SASE can be consumed "as a service" from your friendly neighborhood security vendor or service provider.

Omdia had already called out SASE as a key trend for 2022 and we expect his trend to continue into 2023: the evolution of how technology has responded to the COVID-19 pandemic includes a more complex scenario where the workforce becomes hybrid, which demands lots of flexibility. At the same time, the digital value chains on which the organization depend get more complex, and more important for the survival of the organization itself.

Key SASE use cases across security and networking



Source: Omdia

Infrastructure Security: Continued evolution of network security functionality into services drives SASE adoption

Player type	What will the impact be?	Impact rating	How should players respond?
Vendors	Enterprise customers will continue to seek SASE deployments, with all or most of their technological components residing in the cloud, to support their WAN, WAN security, and hybrid workforce requirements. Tech vendors who cannot deliver a reasonable SASE story—either as a provider of SASE or offering meaningful integration—will likely face headwinds.	[✓ +2] +1 – -1 -2	Security vendors that offer functionality that would fit into a SASE model—SWG, CASB, ZTA, and others—need to clearly articulate to both end-user organizations as well as to service providers how their offering can fit into a SASE story, be it via integration, partnership, or evolution. They should also be proactive in describing how their offering fits into broader security architecture.
Service Providers	SASE remains an approach to consuming network-centric security functionality that is particularly well aligned to being offered by service providers, particularly network service providers, as a value-add offering. We expect increased demands from customers on how a service provider can fulfill needs around SASE, both for initial planning and deployment as well as ongoing operations.	[✓ +2] +1 – -1 -2	Service providers should make sure they have a robust SASE message, covering a wide spectrum of use cases and able to accommodate customer needs for seamless deployments, smooth operations, and integration with other aspects of security architecture. This will likely require multiple partnerships with security vendors.
Enterprises	Organizations are looking at ways to optimize the delivery of networking and security services. As interest in SASE grows, organizations will have to clearly understand the underlying use cases, migration paths, and requirements for how initiatives may align to a broader SASE framework.	[✓ +2] +1 – -1 -2	Security teams should be ramping up on how their existing networking and security initiatives could align to SASE. They should also be speaking with their strategic security vendors and service providers about how they currently support SASE or plan to do so in the future.

Security Operations: Risk-based vulnerability management (RBVM) makes inroads to reduce attack surface

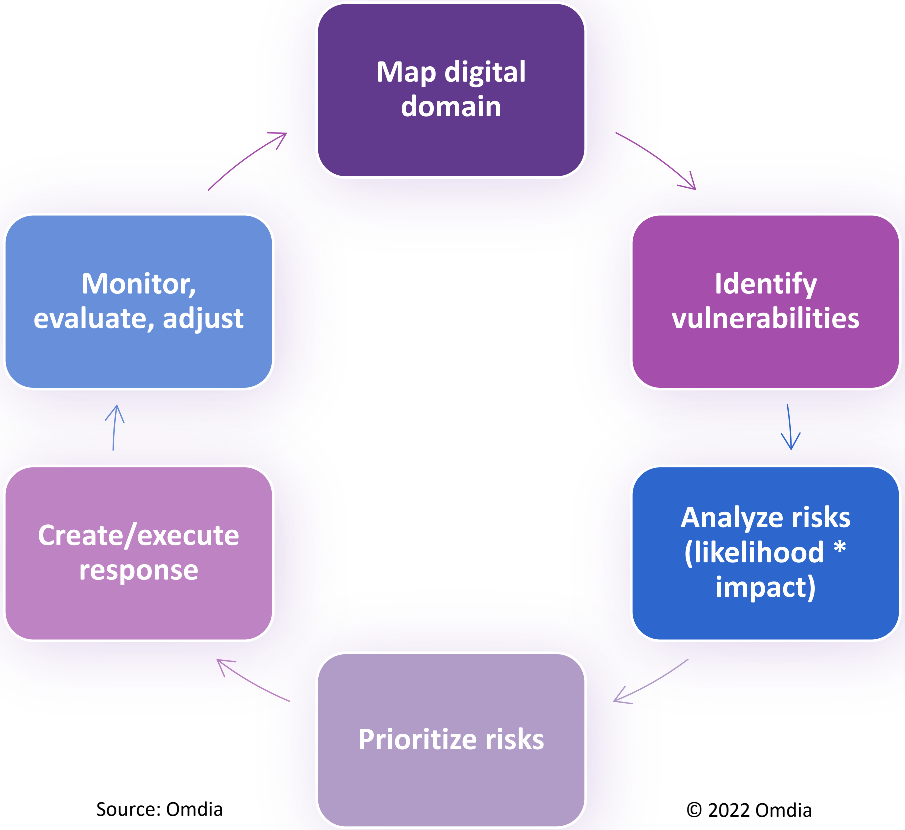
Risk-based vulnerability management is an important component of any proactive risk reduction strategy. All vulnerability management products will eventually be risk based, and RBVM is fast becoming a foundational element of broader proactive enterprise risk reduction strategies.

The three fundamental capabilities of an RBVM are complete asset visibility, accurate creation of a risk register for vulnerability-related risk, and orchestration of mitigation and remediation recommendations.

Omdia defines RBVM as delivering the following functionality:

- Asset inventory
- Vulnerability data collection
- Vulnerability scanning
- Vulnerability assessment and prioritization
- Temporary vulnerability mitigation
- Patch management
- Vulnerability operations management

Understanding the RBVM lifecycle



Source: Omdia

Security Operations: Risk-based vulnerability management (RBVM) makes inroads to reduce attack surface

Player type	What will the impact be?	Impact rating	How should players respond?
Vendors	Proactive security tools are beginning to come together into more comprehensive bundles, for example, the inclusion of external attack surface management (EASM) capabilities in RBVM solutions. There is also a trend, however, to include proactive features into TDIR offerings.	+2 [✓ +1] – -1 -2	Omdia has been an early advocate for better integration and bundling of detection and response tools but is less enthusiastic regarding the inclusion of proactive tools into XDR suites. The use of reactive and proactive tools generally have different drivers, cadence, and personnel mixes.
Service providers	The integration of risk management with proactive tools such as vulnerability management is increasingly becoming the norm, and the risk scores derived from these systems will inform broader risk management strategies, including the issuance of cyber insurance.	+2 [✓ +1] – -1 -2	Much of the data that informs a risk score is threat intelligence that is globally sourced; large service providers are in an advantageous position to collect, analyze, and push that intelligence to RBVMs. Additionally, service providers should consider integration of RBVMs with their existing MDR solutions to enable vulnerability mitigation recommendations.
Enterprises	If there is one constant in security, it is the perennial shortage of talent. Priorities must be established with respect to what can get done on any given day, and those priorities should be determined based on risk.	[✓ +2] +1 – -1 -2	The heart of any RBVM is its analytic capabilities. Is it transparent in how risk models are created and applied? Transparency builds trust, and trust in risk scores will be an important determinant of willingness to automate remediation.

Source: Omdia

Enterprise Security Management: Cyber-risk metrics push toward portability

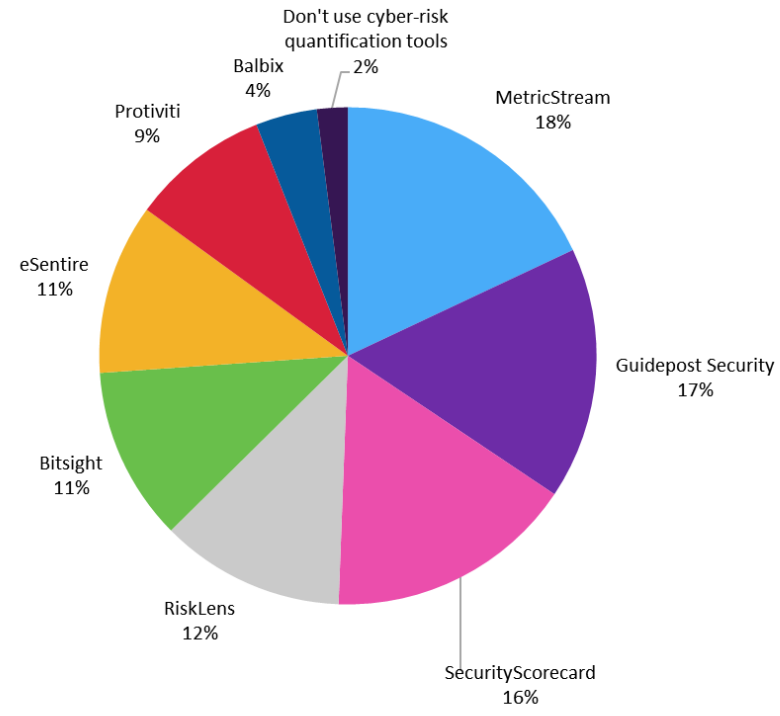
Quantifying risk will grow in importance during 2023. More than that, the ability to compare one organization's risk posture to those of another will see a push from executives across many different industries and markets.

Several competing risk quantification frameworks are available. Though several have significant populations of users, none has taken hold as a genuine market leader. Enterprises will work to determine which framework best suits their needs and then struggle to compare their results with those of organizations that chose a different framework.

More than frameworks, organizations will want to know that the risk quantification tools they choose can provide results useful to their cyber-insurance provider, their internal risk committee, and to their cybersecurity staff, to effectively benchmark their risk performance against corporate peers.

The multiple applications of a risk metric will be important as risk quantification becomes an accepted part of the cybersecurity group's portfolio. Once the data is available, cybersecurity professionals will seek new ways to use it to improve overall threat posture and increase the organization's cybersecurity.

Which cyber-risk quantification tool does your organization use?



Note: n=187
Source: Omdia

Enterprise Security Management: Cyber-risk metrics push toward portability

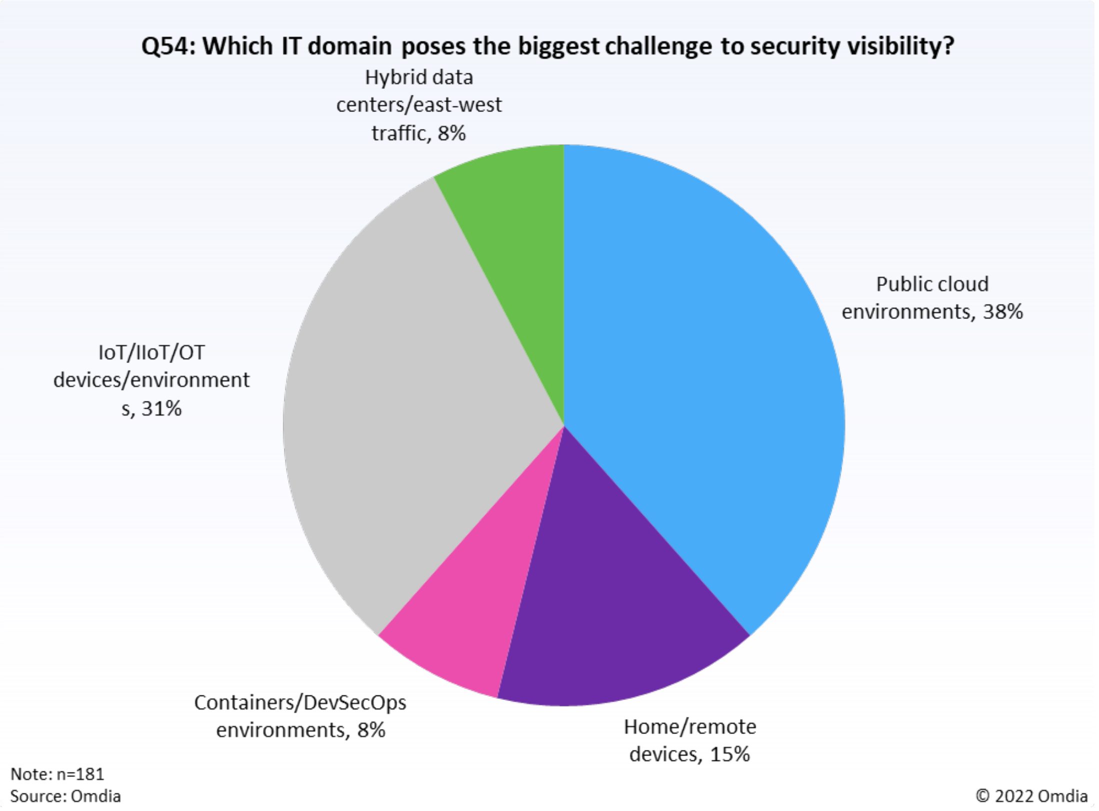
Player type	What will the impact be?	Impact rating	How should players respond?
Vendors	Enterprise customers will look for risk quantification metrics that can be given to critical partners, such as cyber-insurance providers, and used to compare the organization's risk posture with those of its enterprise peers. Metrics that are severely limited will be severely questioned by customers that are eager to get the most out of their quantified risk landscape.	+2 [✓ +1] – -1 -2	Risk metrics that can be compared with the metrics produced by other vendors' products are not easy to generate. Vendors will need to talk about how they are making progress toward that metric portability and, if necessary, the frameworks and intermediary measurements that they are using to provide a facsimile of portability, even while true portability and interoperability remains a work in progress.
Enterprise	The possibilities of risk metrics that can be compared with those of other companies within an industry and used to reduce costs such as cyber-insurance premiums will explode in 2023. Once the exercise of quantifying risk has been conducted, enterprise customers will look for the various ways in which that measurement can be used to continuously improve their risk posture and prove to stakeholders that the risk is improving, not just within the organization but in comparison with other organizations.	[✓ +2] +1 – -1 -2	Enterprise cybersecurity teams and executives must decide which industry framework they will use for their risk metrics. Cyber-insurance carriers may be able to offer significant assistance in understanding the relative advantages of the different systems and frameworks. The real key is to use 2023 as a year to begin employing risk metrics as widely as possible, to afford the basis on which to judge the effectiveness of various security efforts. "Lack of disaster" is no longer a sufficient metric; genuine measurement progress is possible.

IoT Cybersecurity: Top priorOTy for OT and healthcare alongside IoT

IoT continues to be broadly deployed. The IoT Enterprise Survey 2022 revealed 90% of respondents said IoT was core to digital transformation or was being deployed across multiple areas. However, security for IoT environments is still lacking.

Throughout this past year there has been increasing development and acquisition activity among vendors who market themselves, or marketed themselves, as IoT cybersecurity vendors – shifting into the OT space. This looks to continue as IoT cybersecurity solutions vendors start to consolidate and OT and IoMT are pulled into the equation.

Omdia's Decision Makers Survey 2022 suggested that IoT, IIoT and OT devices and environments were one of CISOs and VPs biggest challenges to security visibility. In addition, these environments require a unique balance between IT and OT, security and safety, something which the IoT cybersecurity industry is familiar with given the nature of securing devices and networks that transcend in the physical world, as opposed to just IT networks.



Note: n=181
Source: Omdia

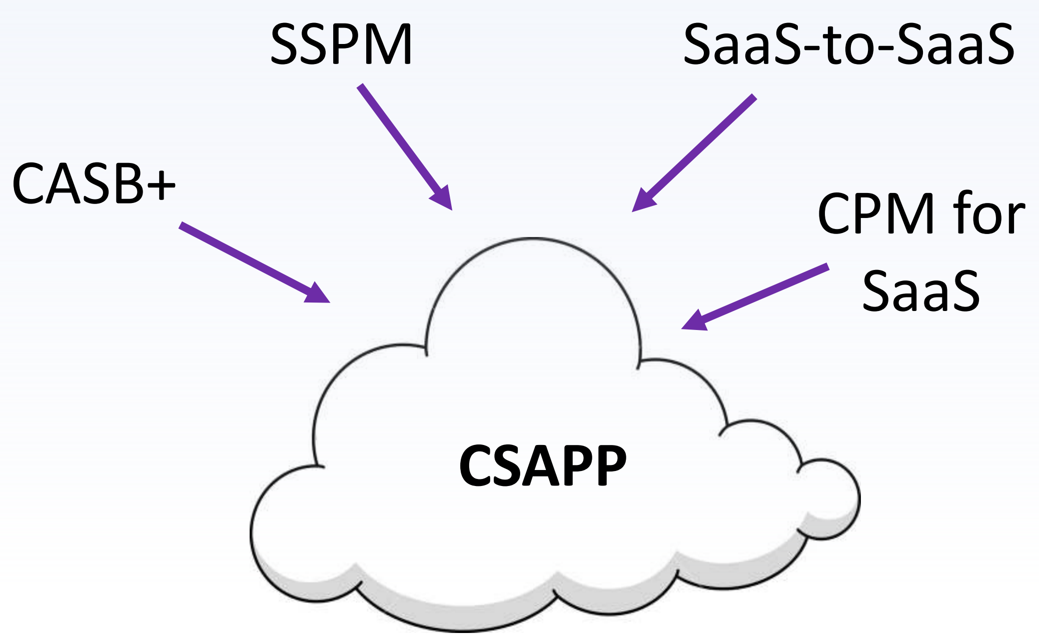
Emerging cybersecurity: SaaS security becomes more complex; enter CSAPP

Security for IaaS and PaaS environments has grown increasingly complex, with household names such as CSPM and cloud workload protection platforms (CWPPs) being joined by cloud permissions management (CPM), infrastructure-as-code (IaC) checking, and API security as necessary complements for a complete cloud security offering. Indeed, a bundle of all these capabilities now has its own acronym, namely cloud-native application protection platform (CNAPP).

However, SaaS security is also moving on from the days when it was essentially circumscribed to cloud access security brokers (CASBs). More proactive capabilities are being introduced, such as SSPM, permissions management for SaaS (probably an extension of CPM platforms), and what some are calling SaaS-to-SaaS security, i.e. monitoring and, where appropriate, curtailing one SaaS app’s ability to communicate and interact with others.

In a non-too-subtle nod to CNAPPs, Omdia posits the emergence of product offerings combining all these elements, called comprehensive SaaS app protection platforms, or CSAPPs.

Comprehensive SaaS Application Protection Platform



SSPM

SaaS-to-SaaS

CASB+

CPM for SaaS

CSAPP

Source: Omdia

© 2022 Omdia

Appendix

Omdia Cybersecurity – Intelligence Service products and ecosystem

Cybersecurity Service Area

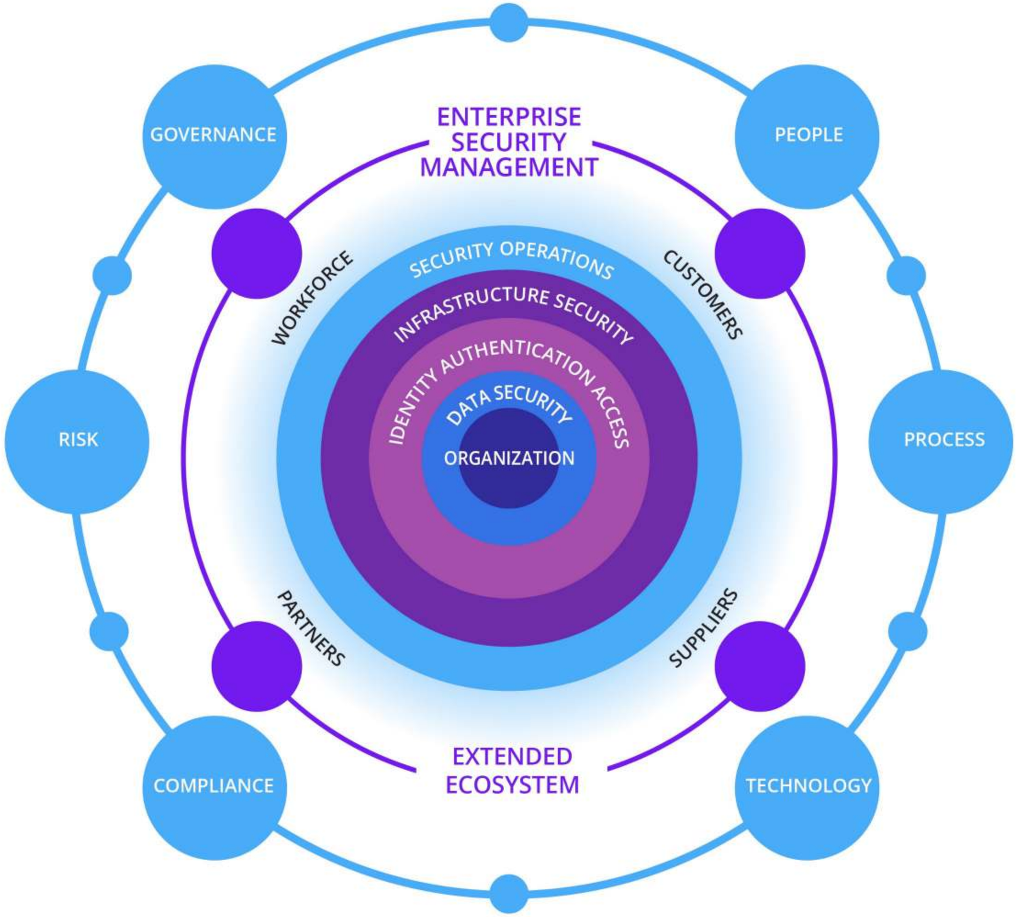
Cybersecurity Viewpoint Service

Data Security Intelligence Service	Identity, Authentication, Access Intelligence Service
Infrastructure Security Intelligence Service	Security Operations (SecOps) Intelligence Service
IoT Cybersecurity Intelligence Service	Enterprise Security Management Intelligence Service
DDoS Prevention Intelligence Service	Emerging Cybersecurity Intelligence Service

Upcoming coverage

- Managed Security Services
- SASE
- Cloud Security

Omdia Cybersecurity Ecosystem



Get in touch!

✉ askananalyst@omdia.com

in @Omdia

🐦 @OmdiaHQ

OMDIA

Thank you

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.

Get in touch!

✉ customersuccess@omdia.com

in @Omdia

@OmdiaHQ