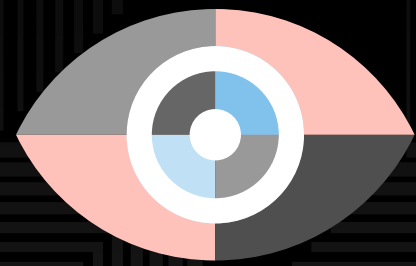


ARROW

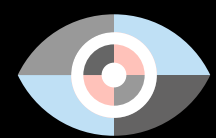


Opportunity Watch

Industry research to
supercharge your strategy

THE CYBERSECURITY IMPERATIVE





Opportunity
Watch

The
cybersecurity
imperative

2

Building trust starts with cybersecurity

Cyberattacks are getting more sophisticated and moving with acceleration, with the rampant proliferation of AI and emergence of quantum being highly influential factors. The timeline of attack has been dramatically compressed — and it doesn't take long for serious damage.

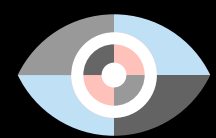
The cybersecurity landscape is shifting from reactionary and tool-heavy programs toward more proactive approaches that encompass security posture management, outcome-based managed services, unified platforms and identity-first control models.

DID YOU KNOW?

91.7%

of cybersecurity
revenue is sold
through or
with channel
partners.

SOURCE: OMDIA



Opportunity
Watch

The
cybersecurity
imperative

3

What's one of the fastest growing enterprise technology areas? Cybersecurity.

Estimated at \$311B and growing at 12.1%, the cybersecurity market is vast — and fast-growing.¹ Budgets are increasing by 5% or more over the next 12 months, according to 60% of security decision-makers.² Services and partner ecosystems are driving how cybersecurity is bought, implemented and operated. In fact, 91.7% of cybersecurity revenue is sold through or with channel partners.¹

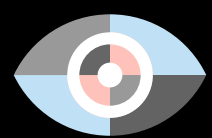
Omdia estimates that the channel sells \$204.8B in cyber services compared to \$106.4B in products this year.¹ That's \$2 in cyber services for every \$1 in product. Cloud-delivered software is increasing as a share of spend, as public cloud-delivered cybersecurity software rose to 80.0% of total spending in 2025.³

Your customers are facing increasing pressure around regulations, compliance and cyberinsurance and are looking for channel partner guidance interpreting, implementing and adhering to requirements.



The channel
sells **\$2** in
cyber services
for every **\$1** in
product.

SOURCE: OMDIA



Opportunity
Watch

The
cybersecurity
imperative

4

Why the urgency?

Serious, long-term and costly consequences are just one cyberattack away. And that attack can happen in a flash.

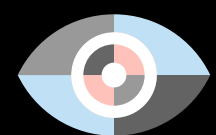
Phishing-driven compromises can occur in under 60 seconds.⁴ The average data exfiltration time has dropped from days to mere hours,⁵ as ransomware operations now have the means to accelerate like never before. The median ransom is reported at \$1M — but the cost of recovery exceeds that at \$1.53M on average.⁶

What's more, the incident response process takes 270 days to move through, according to security decision-makers across organizations worldwide. And organizations in financial services and insurance, government, education, social services and healthcare take even longer — at 285 days on average.⁷

The incident response process takes **270 days** to move through, according to security decision-makers across organizations worldwide.

SOURCE: FORRESTER





What's today's perimeter for protection? Identity.

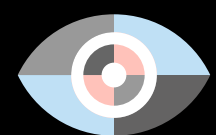
While physical network locations were once the first line of defense, the responsibility rests on an identity-first approach. Day in and day out, decisions and accessibility depend on who or what is requesting access. Identity is the primary control for securing users, devices, workloads and AI. Identity, cloud security, data protection and security analytics need to be tightly integrated.

Passwords are the source of 97% of identity attacks.⁸ Passkey and quantum-safe PKI-based password authentication are replacing legacy password-based authentication.² Identity threat detection and response should be incorporated into organizations' identity lifecycle and risk management efforts to protect against human and non-human identities.



Passwords
are the source
of **97%** of
identity
attacks.

SOURCE: MICROSOFT



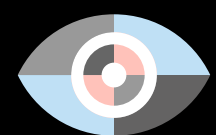
AI security

While AI is giving attackers the horsepower to move with speed and sophistication, there are more layers to the AI story that impact you as channel partners. AI is being embedded into vendor workflows, tools and solutions to strengthen protection and combat new AI-driven attack surfaces. At the same time, AI is also creating a new form of identity — agents — that can be difficult for organizations to govern if not constantly and properly managed. Incredibly, agents are beginning to outnumber humans, and the number of agents is growing by the day. They're more autonomous than traditional machine identities, making these controls more critical than ever.²

Platform consolidation

Tool sprawl is a real problem — and technology buyers are tired of too many disparate systems and tools. Platform consolidation helps organizations streamline and optimize security investments. Vendors are building and offering broader platforms with more capabilities rolling into one centralized hub. With security tools in a single place, organizations can eliminate redundancies, reduce complexity from tool sprawl and save money by divesting standalone external attack management and retiring data pipeline management tools that are no longer necessary.





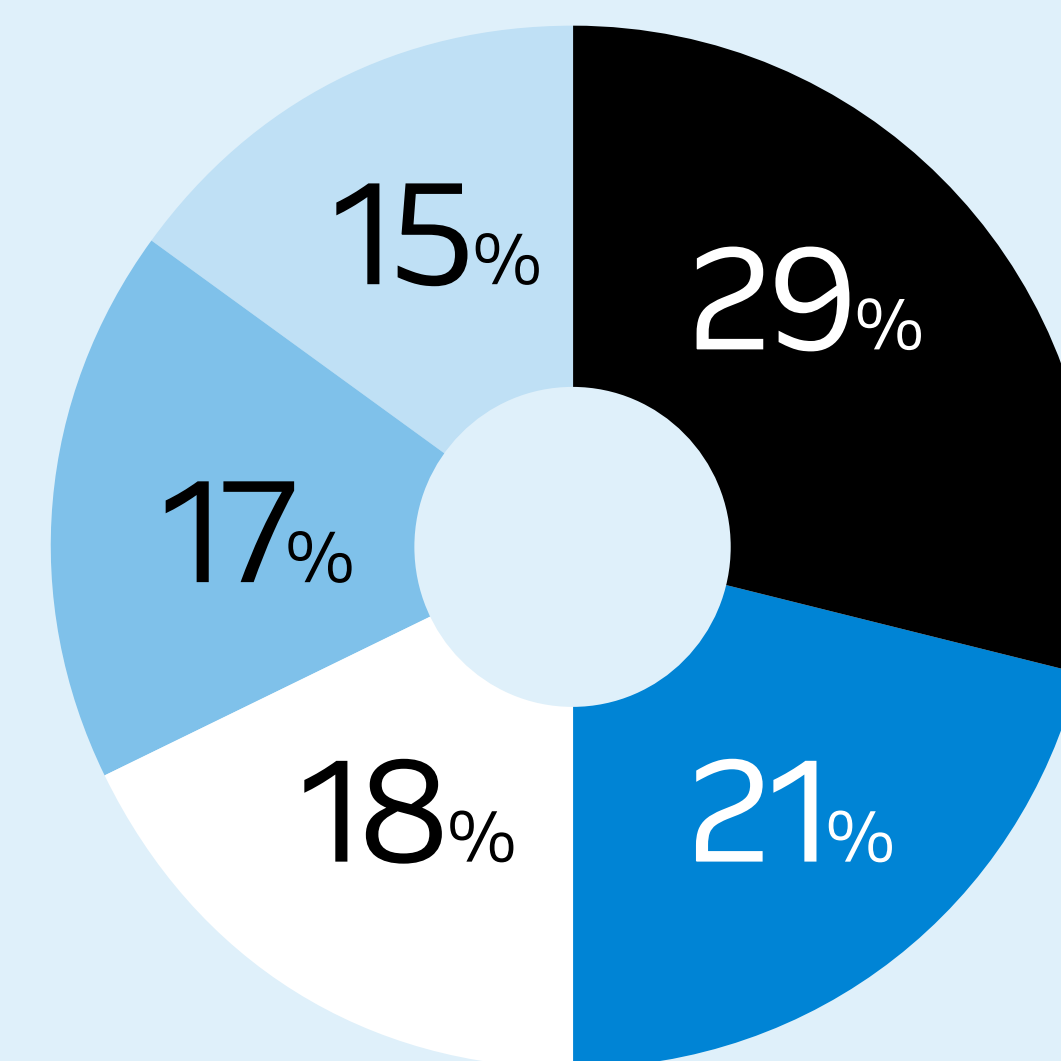
Proactive services

As organizations continue adopting new capabilities and implementing more AI, security services become an increasingly attractive growth opportunity. Internal teams are stretched — and there's a demand for services to help fill in the gaps and proactively combat threats, as the risk landscape continues to intensify.

End customers are moving toward outcome-based services and unified platforms to reduce risk and simplify operations. Large enterprises are investing in scalable services to support efforts around managed detection and response (MDR), cloud security, identity and access management (IAM). Smaller enterprises are drawn to subscription-based managed security bundles with endpoint and cloud security as priority focus areas.⁹

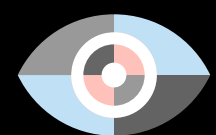
Offering technical services is one approach to expand your capabilities and support your customers' cybersecurity needs, even when teams are short on skills and time. You can help improve customers' security posture by offering services that support areas like exposure management and attack surface management. The chart on the right shows how the global managed security services market share is segmented, according to Fortune Business Insights.⁹

Segmentation of global
managed security
services market share



- Managed detection & response (MDR)
- Managed identity and access management (IAM) services
- Managed vulnerability management
- Managed firewall services
- Managed compliance services

SOURCE: FORTUNE BUSINESS INSIGHTS



Opportunity
Watch

The
cybersecurity
imperative

8

Accelerate your cybersecurity growth

With so much growth, cybersecurity is an attractive area to land or expand your business. And it isn't going anywhere, making it a desirable area to pursue into the future. Yet the complexities of a constantly evolving threat landscape paired with a skill shortage can make it difficult to break into if it isn't your primary focus. Don't tackle cybersecurity challenges and opportunities alone. Take your security practice to the next level.

Here's a few ways we can help you:



1. Dedicated teams & cybersecurity prowess. You have access to Arrow's teams of dedicated technical engineers, sales and marketing professionals. Work directly with our technical teams who monitor the threat landscape and offer cybersecurity expertise as well as guidance on vendor technologies that meet your customers' needs.



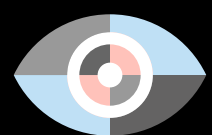
2. Technical expertise. Work directly with our technical teams who offer AI, data, cloud and cybersecurity expertise and are closely following the AI landscape.



3. Immersive experiences. Demo, test and prove cybersecurity solutions in Arrow's experience centers. Collaborate with technical experts and simulate a real-world environment so you can build cybersecurity solutions that align to your customers' requirements. Arrow channel partners achieve a 90% close rate when using the experience centers. Why not give it a try?

90%
close rate
achieved
by channel
partners when
using Arrow's
experience
centers!

[Learn more](#)



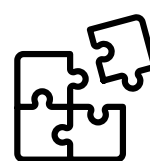
Opportunity
Watch

The
cybersecurity
imperative

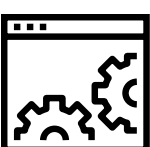
9



4. Services. Complement your in-house capabilities and offer complete solutions to your customers without the investment in additional headcount. Our services capabilities are extensive and include managed, professional, support and education services.



5. Portfolio. We're constantly evolving and enriching our portfolio to best serve you and ensure you have access to the best-fit cybersecurity solutions for your customers' environment. Offer complete solutions to help your customers protect their critical infrastructure, manage risk and meet compliance requirements.

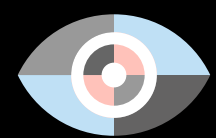


6. Platform. ArrowSphere is a single, centralized platform for accessing cybersecurity solutions from leading vendors on our portfolio. The platform's security dashboard helps you easily monitor the security score of every customer, make recommendations to strengthen their cybersecurity posture and identify cross-sell and upsell opportunities.



7. Programs. Advance your skills through specialized training opportunities. Check out security-related courses available in Arrow's AI academy, including titles like "AI and Cybersecurity," and "Cybersecurity Inflection Point: The Mythos Moment."





Opportunity
Watch

The
cybersecurity
imperative

10

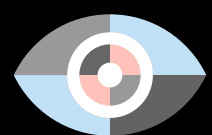
ARROW

Arrow is the leading
AI and hybrid
cloud aggregator.
**Cybersecurity is
fundamental to what
we do.**

[Discover why](#)

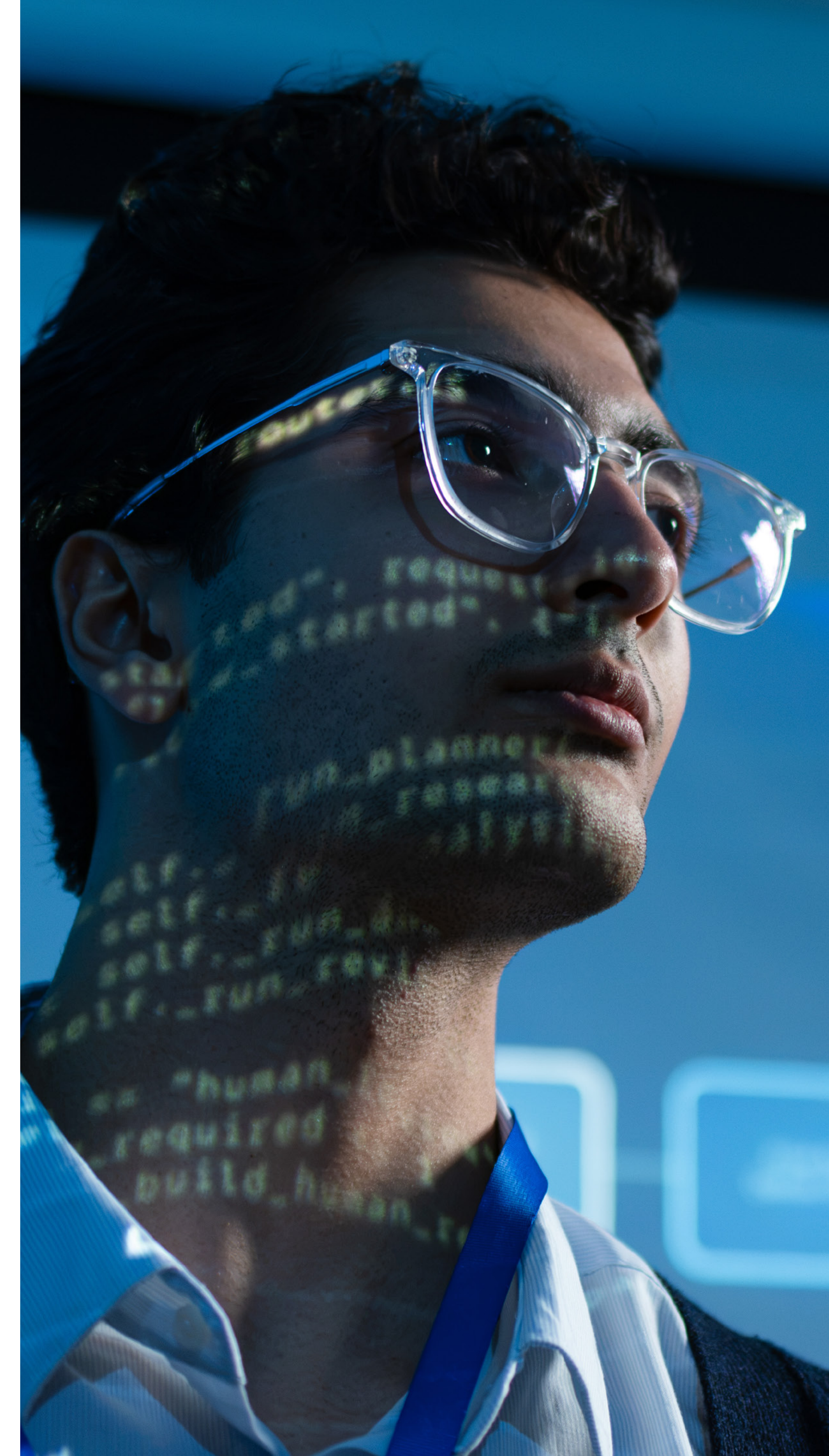
FEATURING
TOP CYBERSECURITY
VENDORS LIKE:



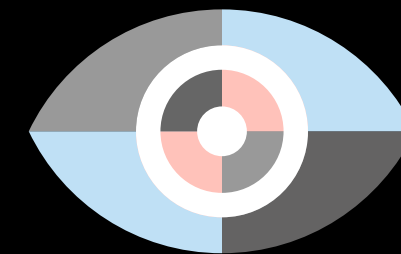


Sources

1. Omdia, The global IT market reaches \$6.2 trillion in 2026. Partners deliver 65.3% of it (and surround 96%)
2. Forrester, Budget Planning Guide 2027: Security And Risk Leaders Must Confront The AI Cost Explosion, July 2026
3. IDC, Market Share: Worldwide Cybersecurity Software Market Shares, 2025 — Market Dynamics and Vendor Share Analysis, June 2026, #US53665926
4. Verizon 2024 Data Breach Investigations Report
5. Palo Alto Networks Unit 42, "The Ransomware Speed Crisis", Sept 2025
6. Sophos State of Ransomware 2025
7. Forrester, 2026 Breach Benchmarks, By Industry, June 2026
8. Microsoft Digital Defense Report 2025
9. Fortune Business Insights



אופטו



Opportunity Watch