

AI Brand Leader Report

Survey results for 10 AI Cyber Risk Management Products

itbrandpulse.com

ITBRAND PULSE

Table of Contents

The November 2026 AI Brand Leader survey results for 10 AI Cyber Risk Management Products are on the following pages:

AI Cyber Risk Management 2027 Brand Leaders	3
Executive Summary	4
Summary Analysis	5
Brand Leadership Defined	6
AI Product Taxonomy and Security Stack	7-8
Category Definitions	9
Survey Results: Cyber Risk Management	
1. Cybersecurity Risk Ratings Platforms	10-11
2. Supply Chain Cyber Risk Monitoring and Response Platforms	12-13
3. Third-Party Risk Management Platforms (TPRM)	14-15
4. External Attack Surface Management Platforms (EASM)	16-17
5. Cyber Threat Intelligence Platforms (CTI)	18-19
6. Cyber Risk Quantification Platforms (CRQ)	20-21
7. Governance, Risk, and Compliance Platforms (GRC)	22-23
8. Exposure Management Platforms	24-25
9. Vulnerability Management Platforms	26-27
10. Security Compliance Automation and Trust Management Platforms	28-29
Looking Forward and Predictions	30
About the Author	31

AI Cyber Risk Management 2027 Brand Leaders

Product Category	Market Leader	Innovation Leader
Cyber Risk Management		
Cybersecurity Risk Ratings	**SecurityScorecard**	**SecurityScorecard**
Supply Chain Cyber Risk Monitoring and Response	**SecurityScorecard**	**SecurityScorecard**
Third-Party Risk Management (TPRM)	**ServiceNow**	**ProcessUnity**
External Attack Surface Management (EASM)	**Palo Alto Networks**	**Palo Alto Networks**
Cyber Threat Intelligence (CTI)	**Recorded Future**	**Recorded Future**
Cyber Risk Quantification (CRQ)	**SAFE Security**	**SAFE Security**
Governance, Risk, and Compliance (GRC)	**ServiceNow**	**Diligent**
Exposure Management	**Tenable**	**CrowdStrike**
Vulnerability Management	**Tenable**	**Tenable**
Compliance Automation and Trust Management	**Vanta**	**Vanta**

© 2026 IT BRAND PULSE

Executive Summary

Responses to the 2027 AI Cyber Risk Management Products Brand Leader Surveys revealed who the security community perceives as the Market Leaders and Innovation Leaders in 10 product categories that identify, assess, prioritize, monitor, and reduce cyber risk across an organization and its third-party ecosystem.

SecurityScorecard led voting by being selected as the Market and Innovation Leader in the Cybersecurity Risk Ratings and in Supply Chain Cyber Risk Monitoring and Response categories. Tenable was picked as Market Leader in Vulnerability Management and Exposure Management, while ServiceNow garnered the most votes for Market Leader in both Third-Party Risk Management and GRC. Palo Alto Networks, Recorded Future, SAFE, and Vanta each were selected as a leader in one category. The most dominant brands, defined as the widest margins between first and second place, were SAFE and Vanta.

In seven of the ten categories the same vendor was selected Market and Innovation Leader, signaling alignment between brand trust and perceived technical advancement.

In the other three, innovation votes went to a different vendor: ProcessUnity in Third-Party Risk Management, Diligent in GRC, and CrowdStrike in Exposure Management.

The results suggest this market is moving from periodic assessment toward continuous, AI-driven risk management. As the market evolves, IT professionals will reward vendors that connect exposure data, threat intelligence, and supplier monitoring to measurable risk decisions.

Prepared by
Frank Berry
Frankie Berry



© 2026 IT BRAND PULSE

Summary Analysis

The 2027 AI Cyber Risk Management Products Brand Leader Survey reveals a market in transition. Security and risk teams are consolidating onto platforms they already trust, yet they are also looking for vendors that use AI to shorten the time between identifying a risk and acting on it. The brands that led voting are those perceived as closing that gap.

Third-party and supply chain risk produced some of the closest races in the survey, and one vendor swept both. SecurityScorecard led voting for Market and Innovation Leader in Cybersecurity Risk Ratings, edging Bitsight by 3.5 points on market, and won both in the Supply Chain Cyber Risk Monitoring and Response category, narrowly on market and decisively on innovation. Four of the five finalists appear in both categories, and voters appear to credit SecurityScorecard with moving from rating a vendor to responding when that vendor is breached. In Third-Party Risk Management, ServiceNow led voting for Market Leader on the strength of its workflow platform, while ProcessUnity was voted the Innovation Leader.

The survey shows the most movement in the Exposure & Attack Surface group of products where Tenable led Market Leader voting in both Vulnerability Management and Exposure Management, while CrowdStrike led voting for Innovation Leader. Palo Alto Networks was selected Market and Innovation Leader for External Attack Surface Management with Cortex Xpanse. These results suggest that IT professionals reward vendors that connect exposure data to real attacker behavior.

In the intelligence and governance groups of products, Cyber Threat Intelligence was a near three-way tie, with Recorded Future, Google, and CrowdStrike within about two points of each other in voting for Market Leader and Innovation Leader. SAFE led voting for Market Leader in Cyber Risk Quantification by the widest margin in the survey, and Vanta posted a similarly decisive win in Security Compliance Automation and Trust Management. In contrast, voting for GRC leaders was close. ServiceNow led voting for Market Leader, Diligent led voting for Innovation Leader, while Optro, formerly AuditBoard, and Vanta finished close behind.

Overall, the survey points to a cyber risk market where trust is still earned through installed base and platform breadth, while innovation leadership is moving toward vendors that apply AI to prioritization, quantification, and continuous monitoring. Security pros perceive different Market and Innovation Leaders In three of ten categories, and in several others the innovation race was far closer than the market vote.

Brand Leadership Defined

Infrastructure and security surveys measure two of the Five Pillars of AI brand leadership. IT professionals vote for the Market Leader and the Innovation Leader in each product category.



Market Leader

What it means. Market leadership is not simply about size or revenue. In the AI world, it signals a brand's ability to set direction for the industry. A market leader defines categories, influences standards, attracts ecosystems, and becomes the default choice for buyers who want confidence and continuity.

Why it matters. AI buyers, especially enterprise buyers, want stability as much as innovation. They want to know the product they invest in today will exist, grow, and be supported tomorrow. In a market where technology leaps and pricing shifts happen at breakneck speed, market leadership becomes a stabilizing force and a strategic moat that can outlast technological cycles.



Innovation Leader

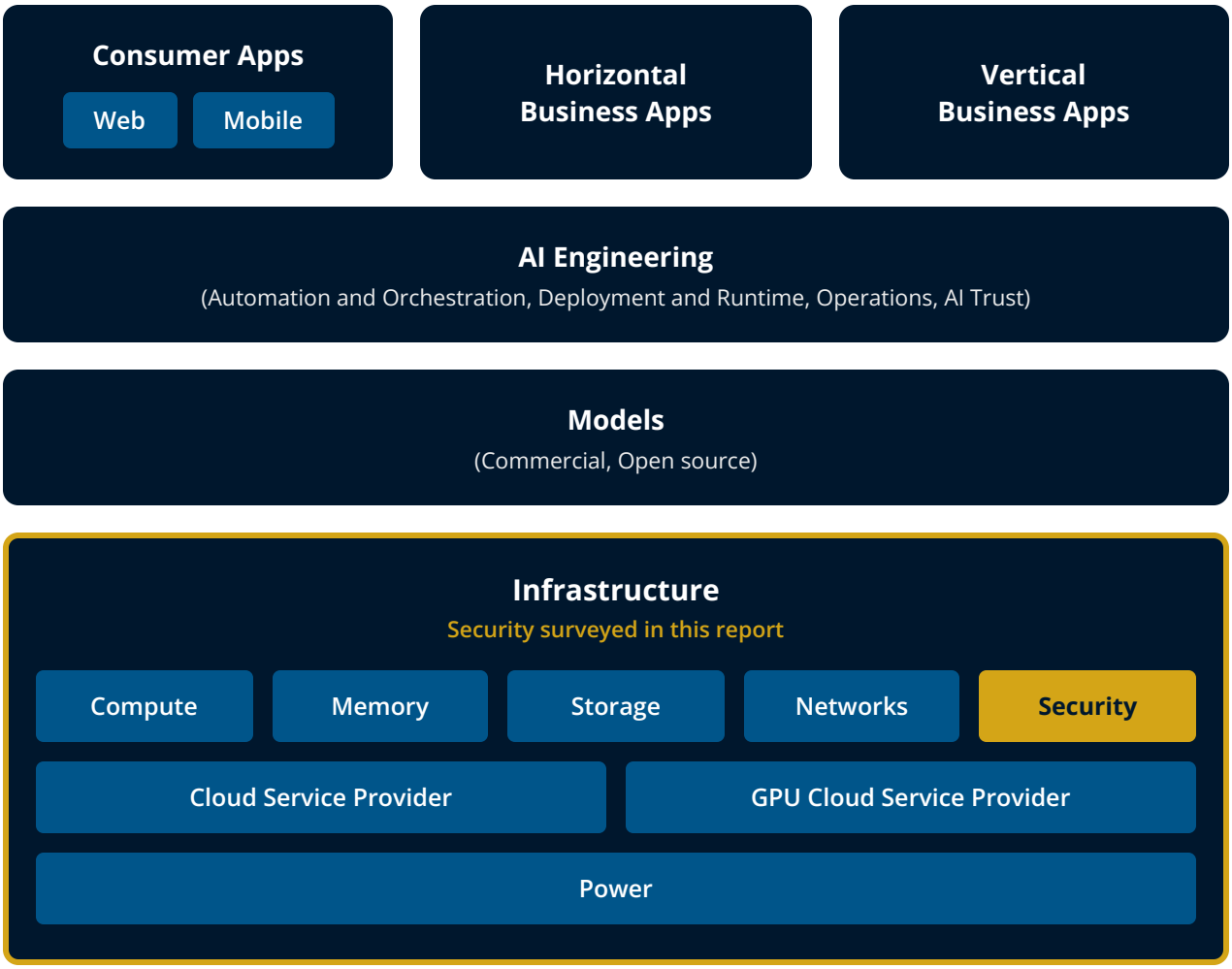
What it means. In AI, innovation is not optional. It is survival. Innovation leadership represents a brand's ability to push boundaries, pioneer new capabilities, and deliver meaningful advancements before competitors. It is about consistently releasing smarter systems, improving performance, speed, and efficiency, and solving previously unsolved problems.

Why it matters. AI companies are judged by their rate of progress. Buyers want assurance that a brand's solutions will not fall behind as models and threats evolve. Innovation leadership attracts engineering talent, fuels investor confidence, and signals that the brand is shaping the future rather than reacting to it. Buyers are not just evaluating what a brand can do today; they are evaluating whether it will still be leading tomorrow.

© 2026 IT BRAND PULSE

AI Product Taxonomy

The product categories covered in this survey are part of the Security segment of the Infrastructure layer in the IT Brand Pulse AI Product Taxonomy. AI Brand Leader surveys are based on the product groupings below with shared characteristics, intended use, target customer, and other criteria.



Enterprise AI Security Stack

The Enterprise AI Security stack has three layers, 10 segments, and 38 product categories. This survey covers the 10 Cyber Risk Management categories shown in blue.

Govern and Identify

Understand, measure, and prioritize cyber risk

Cyber Risk Management

- Cybersecurity Risk Ratings
- Supply Chain Cyber Risk Monitoring and Response
- Third-Party Risk Management (TPRM)
- External Attack Surface Management (EASM)
- Cyber Threat Intelligence (CTI)
- Cyber Risk Quantification (CRQ)
- Governance, Risk, and Compliance (GRC)
- Exposure Management
- Vulnerability Management
- Compliance Automation and Trust Management

Protect

Controls organized by attack surface

Identity and Access Security

- Identity and Access Management (IAM)
- Privileged Access Management (PAM)
- Identity Governance and Administration (IGA)
- Identity Threat Detection and Response (ITDR)

Endpoint Security

- Endpoint Protection Platforms (EPP)
- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Mobile Threat Defense

Network Security

- Next-Generation Firewalls (NGFW)
- Secure Access Service Edge (SASE)
- Zero Trust Network Access (ZTNA)
- Network Detection and Response (NDR)

Cloud Security

- Cloud-Native Application Protection (CNAPP)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWPP)

Data Security

- Data Security Posture Management (DSPM)
- Data Loss Prevention (DLP)
- Encryption and Key Management

Application Security

- Application Security Testing (AST)
- Software Supply Chain Security
- API Security

Email and Collaboration Security

- Email Security
- Security Awareness Training

AI Model and Agent Security

- AI Security Posture Management (AI-SPM)
- AI Runtime Protection and Guardrails
- AI Agent Identity and Access

Detect and Respond

Monitor and respond across the whole stack

Security Operations

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

■ Surveyed in this report ☐ Planned for future surveys

© 2026 IT BRAND PULSE

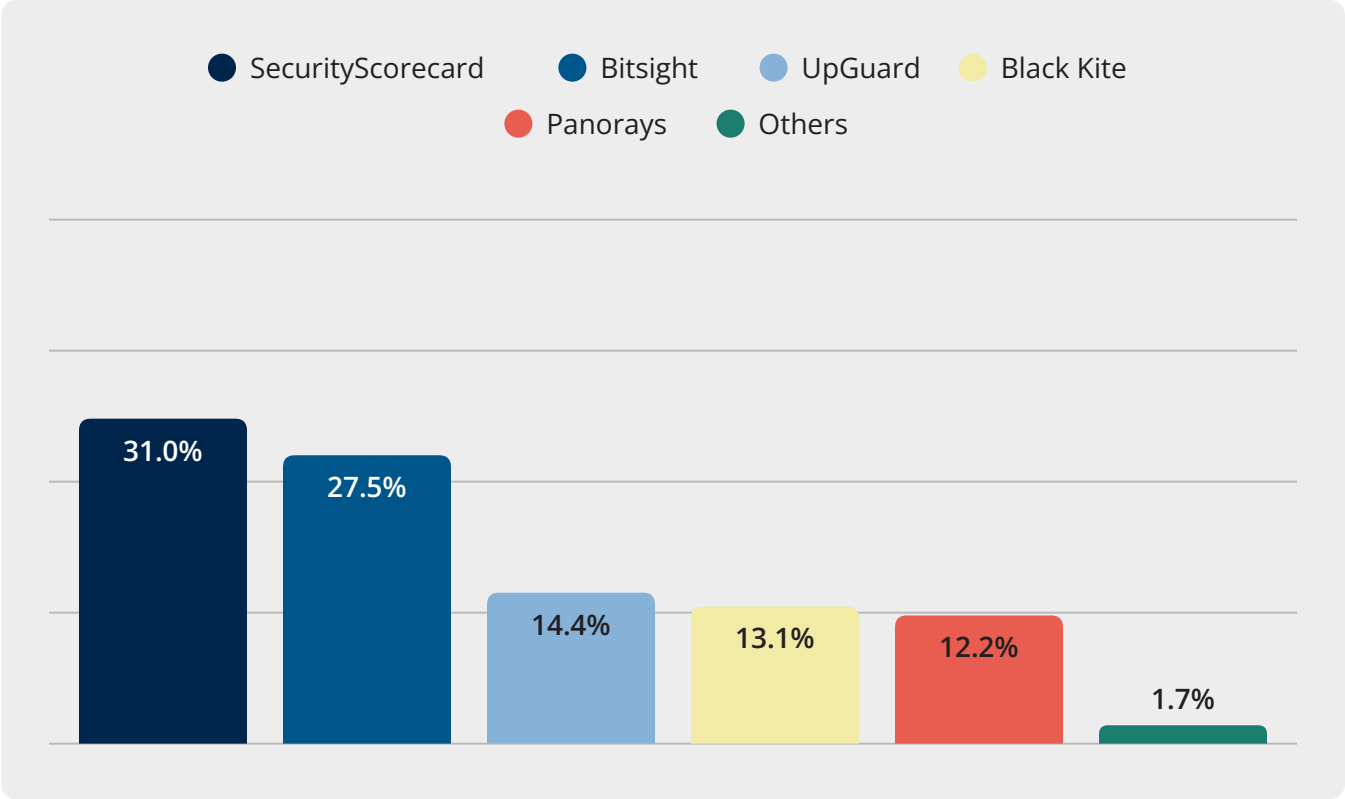
Category Definitions

Cyber Risk Management	
Cybersecurity Risk Ratings Platforms	Platforms that continuously assess organizations and vendors using external security signals, translating findings into comparable ratings and prioritized risks.
Supply Chain Cyber Risk Monitoring and Response Platforms	Platforms that continuously monitor vendors and fourth parties for breaches and exposures across the supply chain, and coordinate detection, response, and remediation with suppliers.
Third-Party Risk Management Platforms (TPRM)	Platforms that manage vendor onboarding, due diligence, assessments, monitoring, and remediation across cyber, operational, financial, and compliance risks.
External Attack Surface Management Platforms (EASM)	Platforms that discover and monitor internet-facing assets, exposed services, misconfigurations, and vulnerabilities, including unknown or unmanaged systems.
Cyber Threat Intelligence Platforms (CTI)	Platforms that provide intelligence about threat actors, attack campaigns, ransomware, exploited vulnerabilities, and compromised credentials to guide defense.
Cyber Risk Quantification Platforms (CRQ)	Platforms that estimate cyber incident likelihood and financial impact to support security investment, insurance, and risk acceptance decisions.
Governance, Risk, and Compliance Platforms (GRC)	Platforms that centralize risk registers, policies, controls, audit evidence, compliance obligations, and executive oversight, including cyber risk.
Exposure Management Platforms	Platforms that consolidate security findings across assets, identities, cloud environments, and attack paths to prioritize and coordinate risk reduction.
Vulnerability Management Platforms	Platforms that discover, assess, prioritize, and track remediation of vulnerabilities across systems, applications, and infrastructure.
Security Compliance Automation and Trust Management Platforms	Platforms that automate control monitoring, evidence collection, audit preparation, security questionnaires, and sharing of security assurance documentation.

Cybersecurity Risk Ratings Platforms



In Market Leader voting, 31.0% of IT professionals selected SecurityScorecard, followed by Bitsight (27.5%), UpGuard (14.4%), Black Kite (13.1%), and Panorays (12.2%). SecurityScorecard edged Bitsight by 3.5 points, and the two category pioneers captured nearly 59% of the vote between them, a sign that IT professionals still associate security ratings with the brands that created the market.



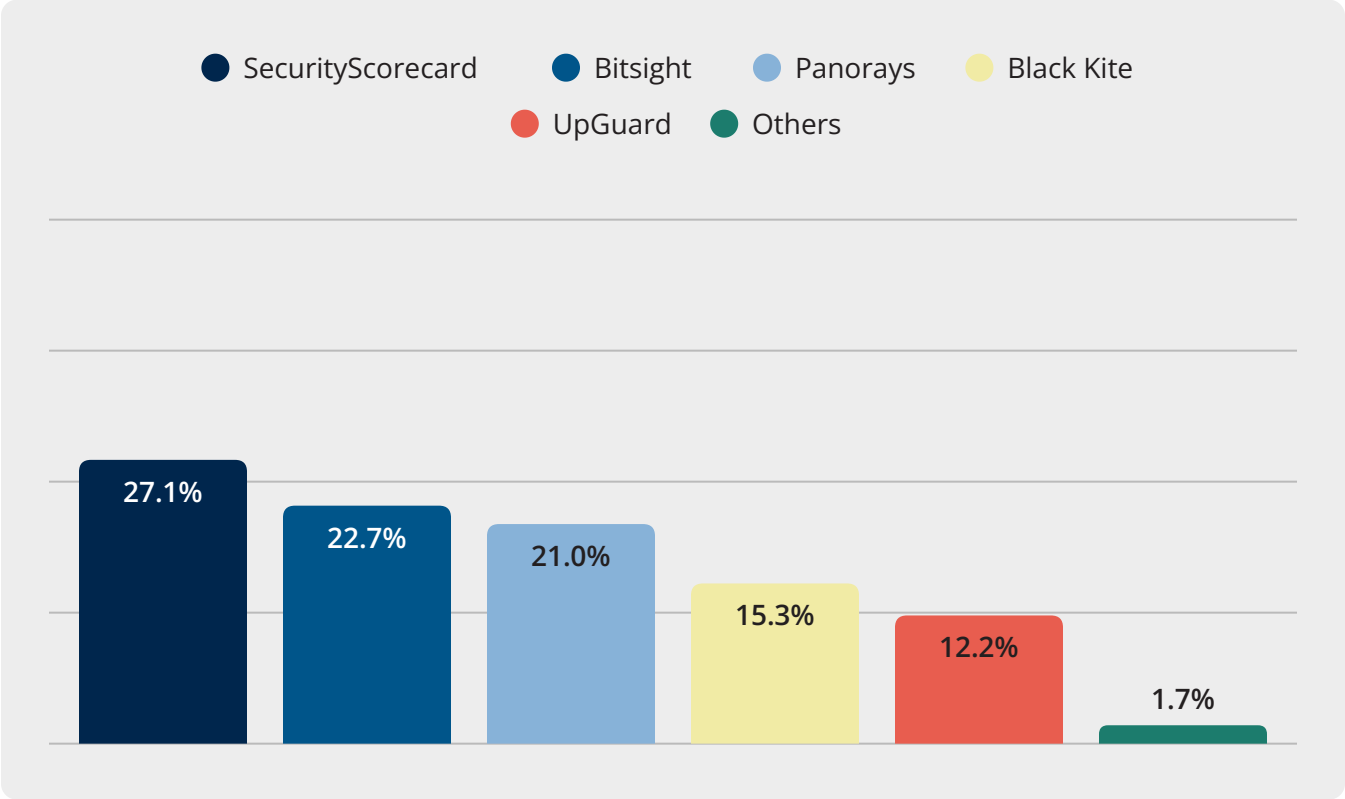
SecurityScorecard

SecurityScorecard's lead reflects a brand closely tied to security ratings, broad free access to its scores, steady research and marketing, and a platform that now extends ratings into supplier detection and response. Bitsight's close second shows the strength of one of the largest ratings datasets in the market and its standing with insurers and boards.

Cybersecurity Risk Ratings Platforms



In Innovation Leader voting, 27.1% of IT professionals selected SecurityScorecard, followed by Bitsight (22.7%), Panorays (21.0%), Black Kite (15.3%), and UpGuard (12.2%). SecurityScorecard also led Innovation Leader voting, about four points ahead of Bitsight, with Panorays a close third.



SecurityScorecard

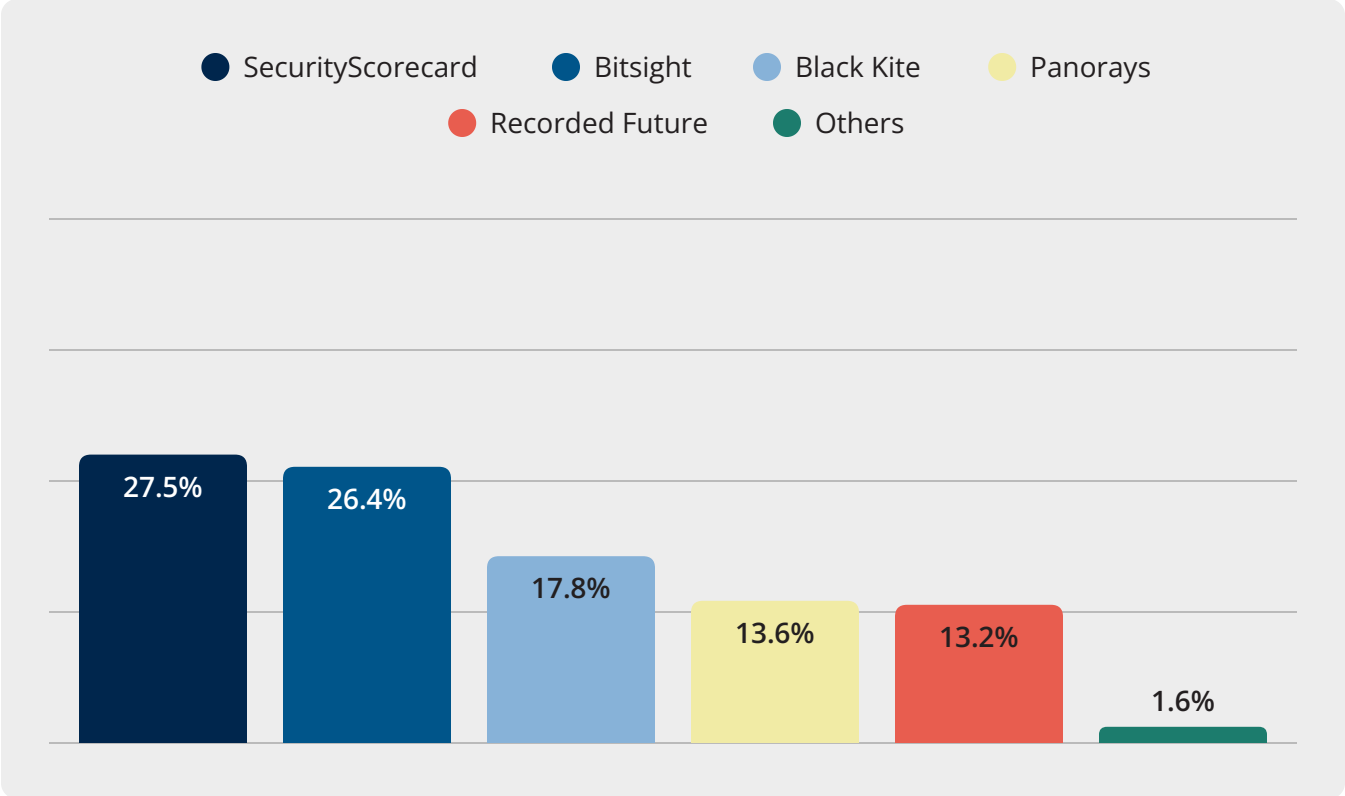
Votes for SecurityScorecard as Innovation Leader suggests the voters like the use of AI and its MAX service to turn ratings into detection, response, and remediation with suppliers. Bitsight, which added threat intelligence through its Cybersixgill acquisition, and Panorays remain close behind in the race to make ratings actionable.

AI Cyber Risk Management Products Brand Leader Report © 2026 IT BRAND PULSE 11

Supply Chain Cyber Risk Monitoring and Response Platforms



In Market Leader voting, 27.5% of IT professionals selected SecurityScorecard MAX, followed by Bitsight (26.4%), Black Kite (17.8%), Panorays (13.6%), and Recorded Future (13.2%). SecurityScorecard edged Bitsight by just over one point, the closest Market Leader race in the survey, while Black Kite placed a clear third.



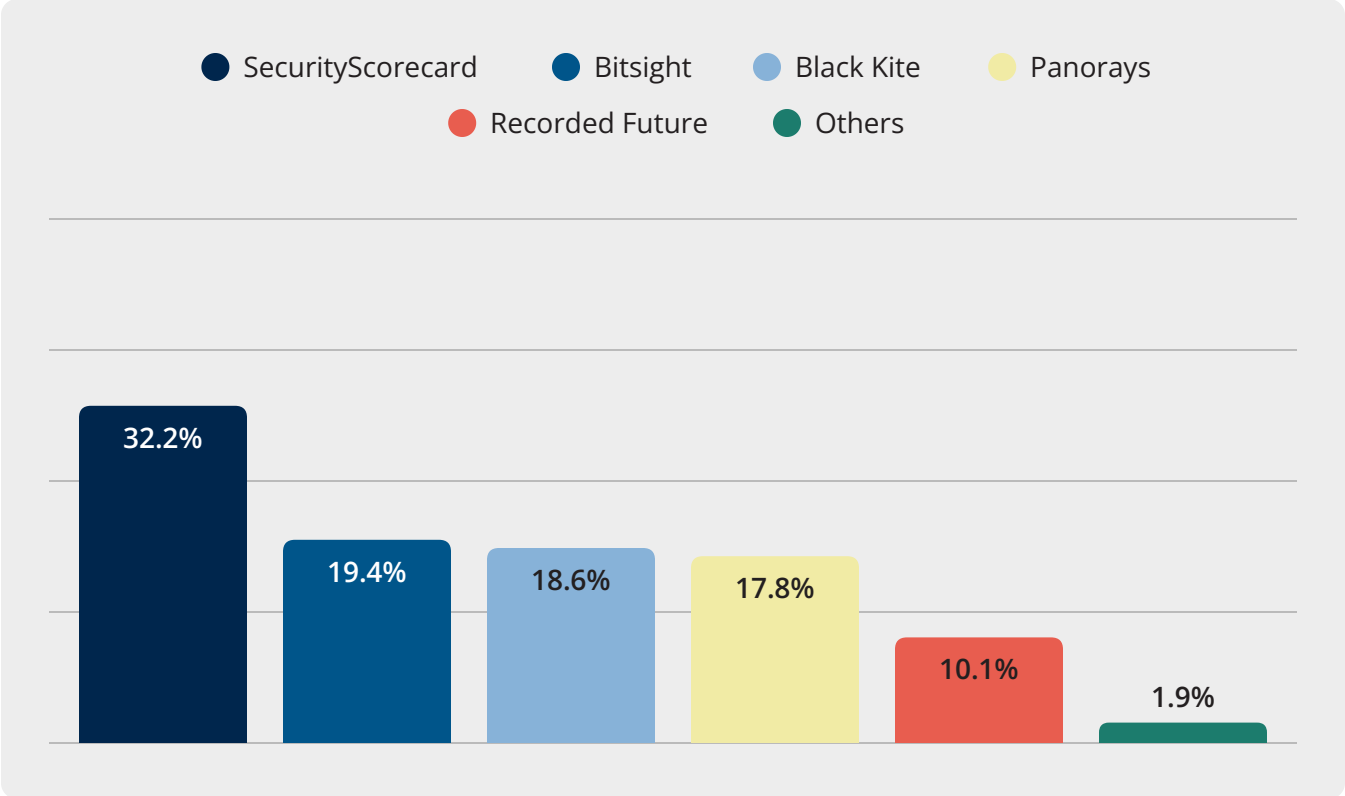
SecurityScorecard

SecurityScorecard's narrow win likely reflects how closely its brand is tied to supply chain detection and response, an approach it popularized with its MAX managed service, which pairs continuous monitoring with remediation work alongside suppliers. Bitsight's near tie shows how far its ratings footprint carries into supply chain use cases.

Supply Chain Cyber Risk Monitoring and Response Platforms



In Innovation Leader voting, 32.2% of IT professionals selected SecurityScorecard MAX, followed by Bitsight (19.4%), Black Kite (18.6%), Panorays (17.8%), and Recorded Future (10.1%). SecurityScorecard's margin widened in Innovation Leader voting, where it led Bitsight by nearly 13 points, with Black Kite and Panorays close behind in a young category.



SecurityScorecard

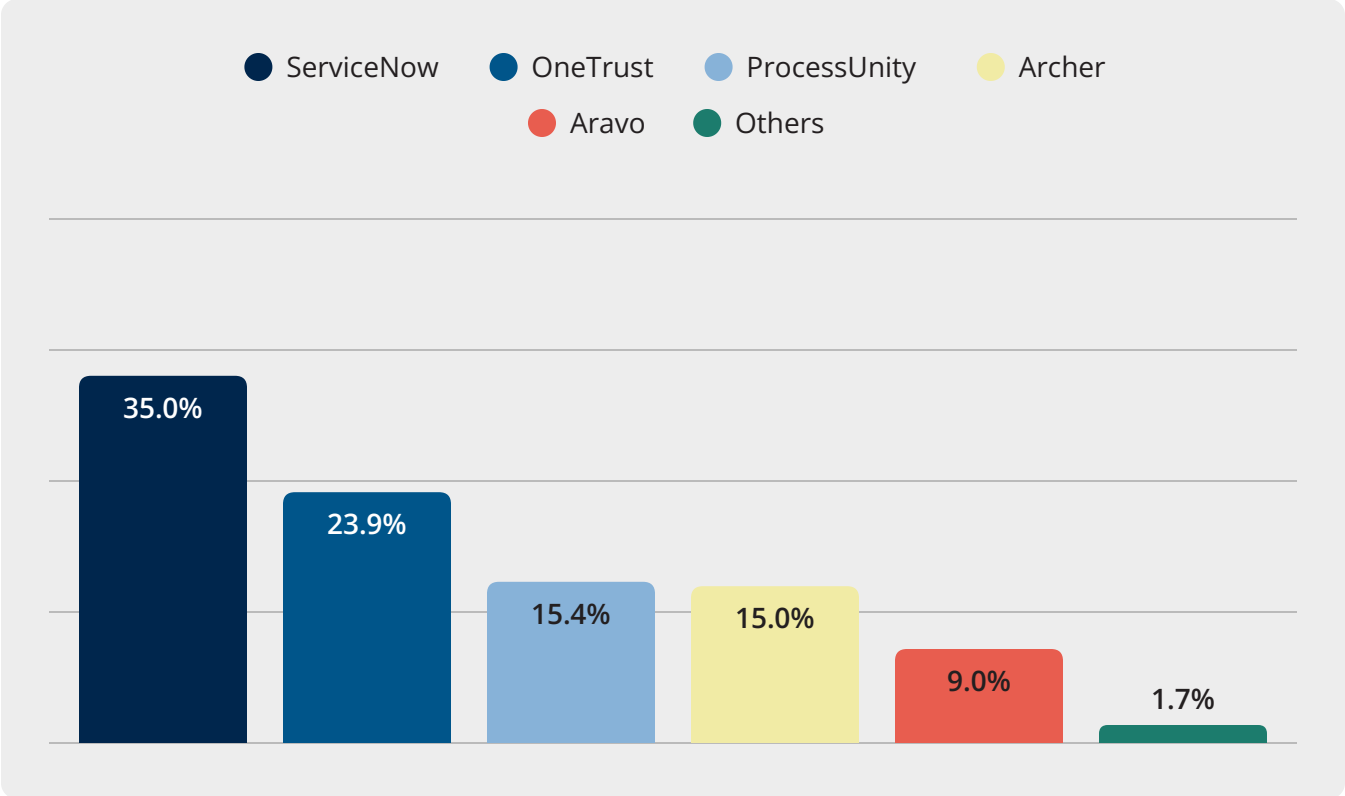
Voters appear to credit SecurityScorecard with treating third-party risk as an operational problem that needs detection and response, not just periodic assessment. Its focus on finding supplier breaches early and driving remediation with the affected vendor gives it a clear identity as the category's innovator.

© 2026 IT BRAND PULSE

Third-Party Risk Management Platforms (TPRM)



In Market Leader voting, 35.0% of IT professionals selected ServiceNow Third-Party Risk Management, followed by OneTrust (23.9%), ProcessUnity (15.4%), Archer (15.0%), and Aravo (9.0%). ServiceNow finished more than 11 points ahead, reflecting the pull of an enterprise workflow platform in a category that spans risk, procurement, and security teams.

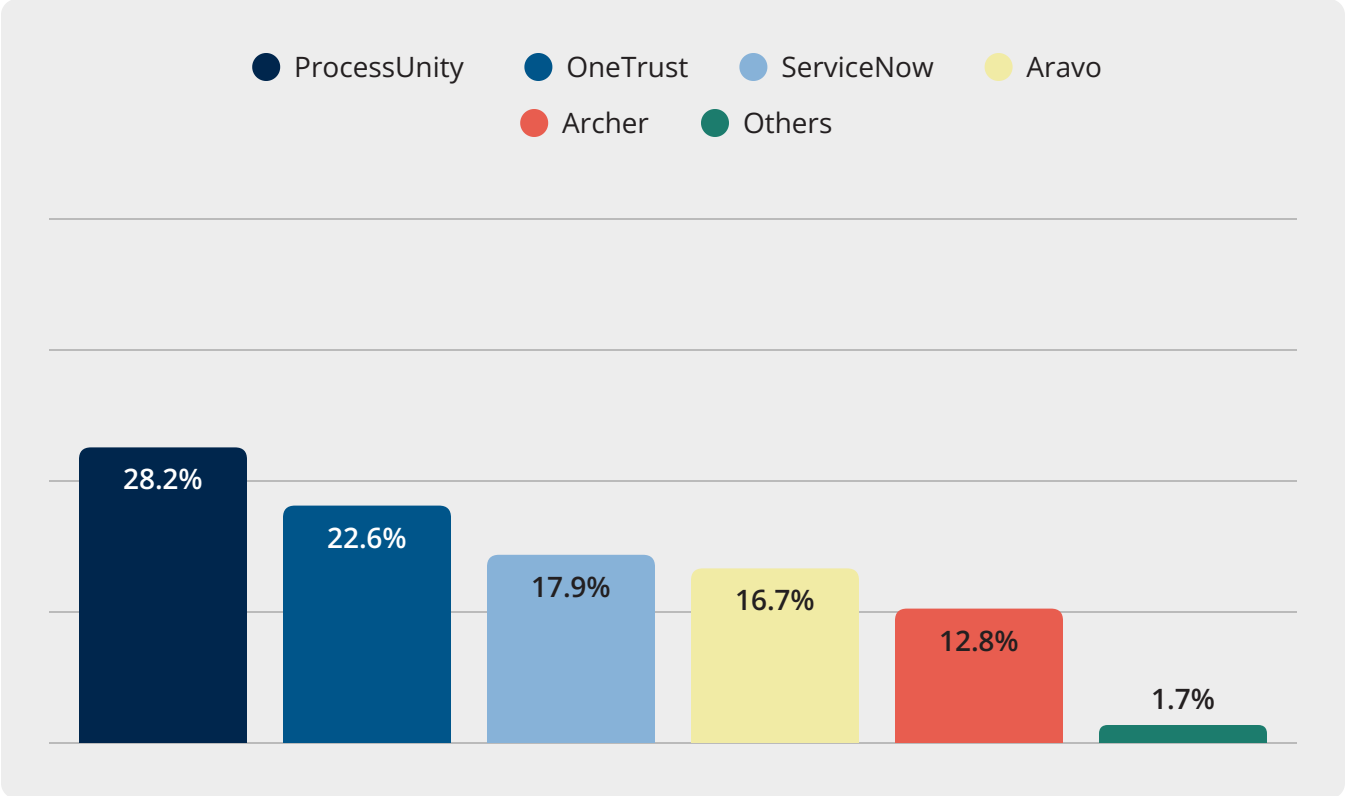


servicenow

ServiceNow's showing reflects the advantage of running third-party risk on the platform many enterprises already use for IT, security operations, and integrated risk management. Consolidating vendor risk workflows onto an established platform reduces integration work and gives risk, procurement, and security teams a shared system of record.

Third-Party Risk Management Platforms (TPRM)

In Innovation Leader voting, 28.2% of IT professionals selected ProcessUnity, followed by OneTrust (22.6%), ServiceNow Third-Party Risk Management (17.9%), Aravo (16.7%), and Archer (12.8%). ProcessUnity won Innovation Leader voting while ServiceNow fell to third, a sign that IT professionals credit the specialist with moving faster than the platform players.

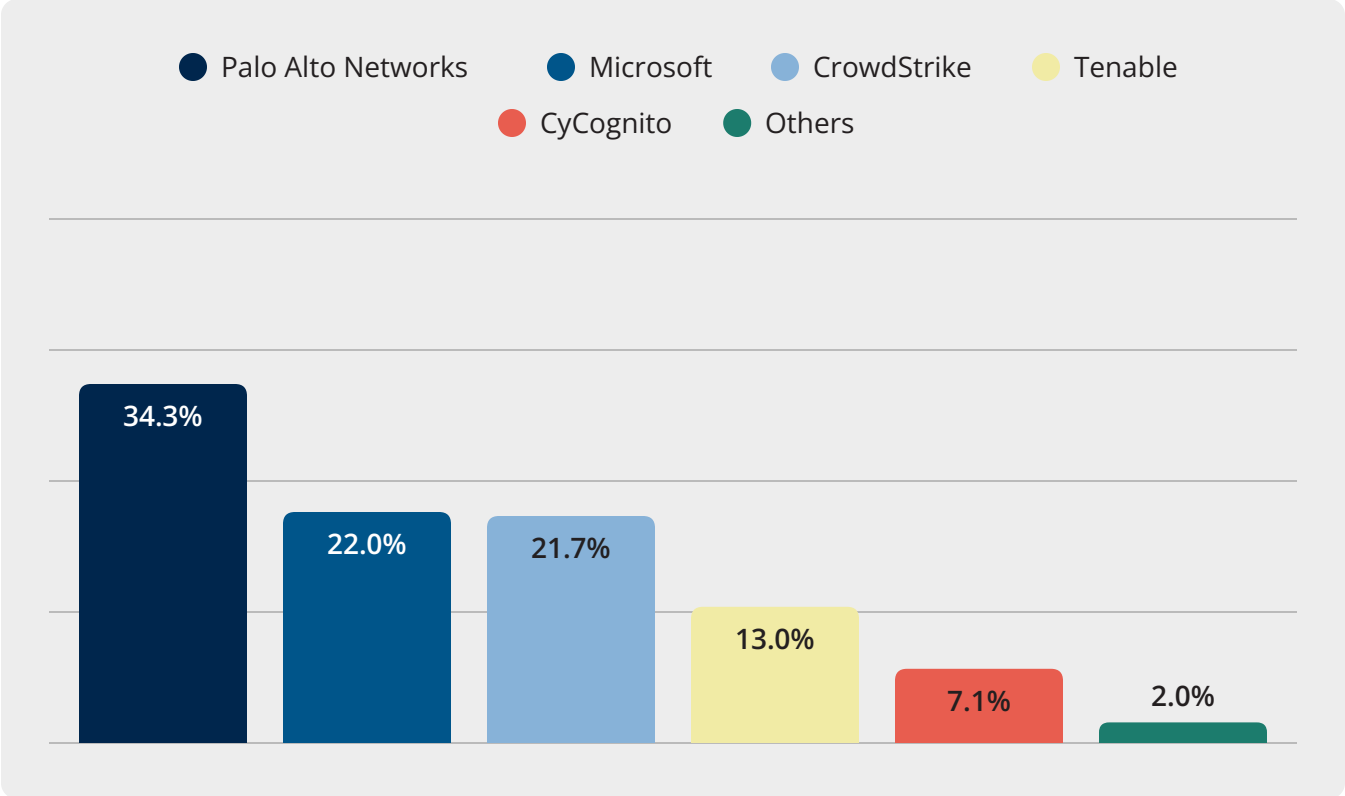


ProcessUnity's innovation lead suggests voters value its focus on TPRM as a dedicated discipline, with automated assessments, continuous monitoring, and AI-assisted review of vendor evidence. Specialists that shorten the path from vendor onboarding to a risk decision are earning recognition against much larger platform vendors.

External Attack Surface Management Platforms (EASM)



In Market Leader voting, 34.3% of IT professionals selected Palo Alto Networks Cortex Xpanse, followed by Microsoft Defender EASM (22.0%), CrowdStrike Falcon Surface (21.7%), Tenable (13.0%), and CyCognito (7.1%). Palo Alto Networks led by more than 12 points, while Microsoft and CrowdStrike finished in a virtual tie for second as platform vendors absorb attack surface discovery.



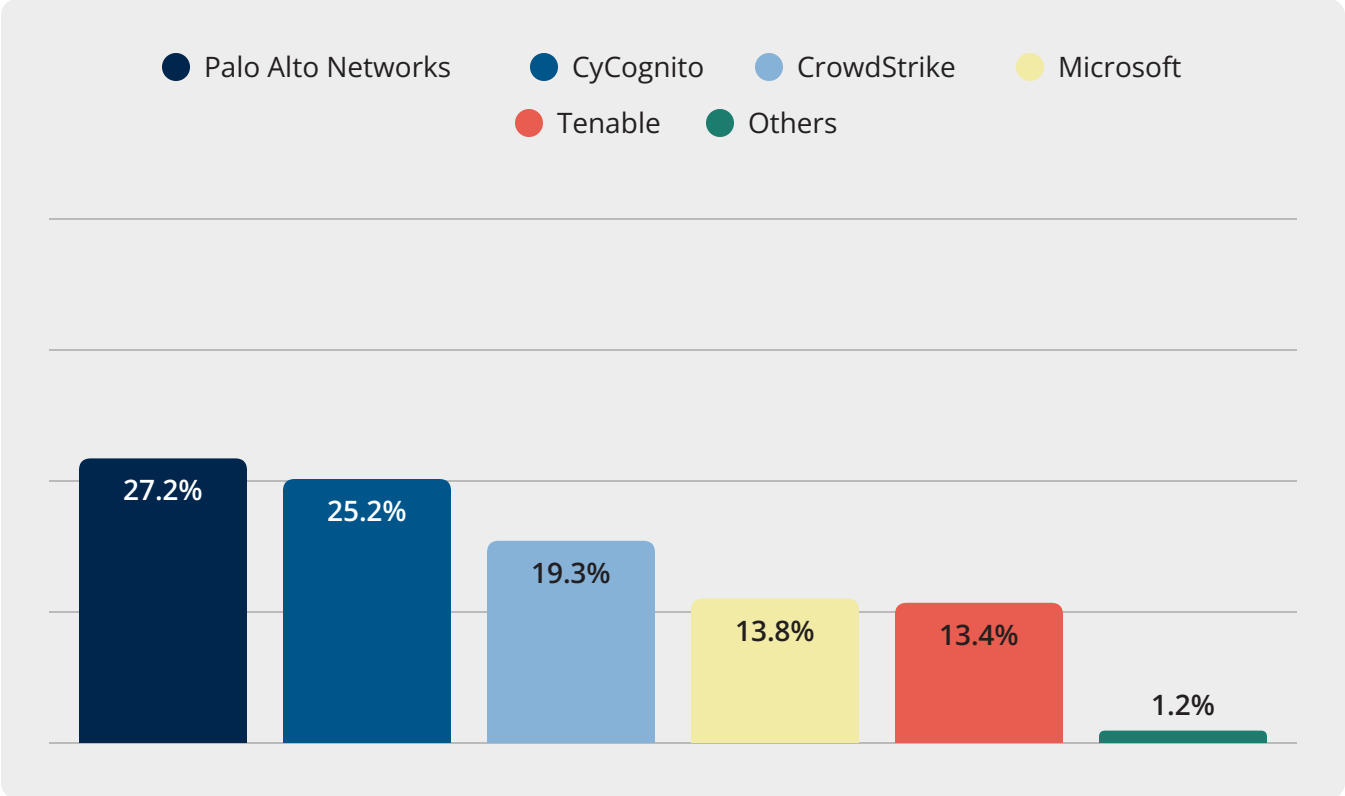
paloalto NETWORKS

Cortex Xpanse helped define external attack surface management, and Palo Alto Networks has since folded it into Cortex as part of a broader exposure management strategy. IT professionals appear to reward that combination of an early, recognized EASM product and a platform that connects internet-facing discovery to detection and response.

External Attack Surface Management Platforms (EASM)



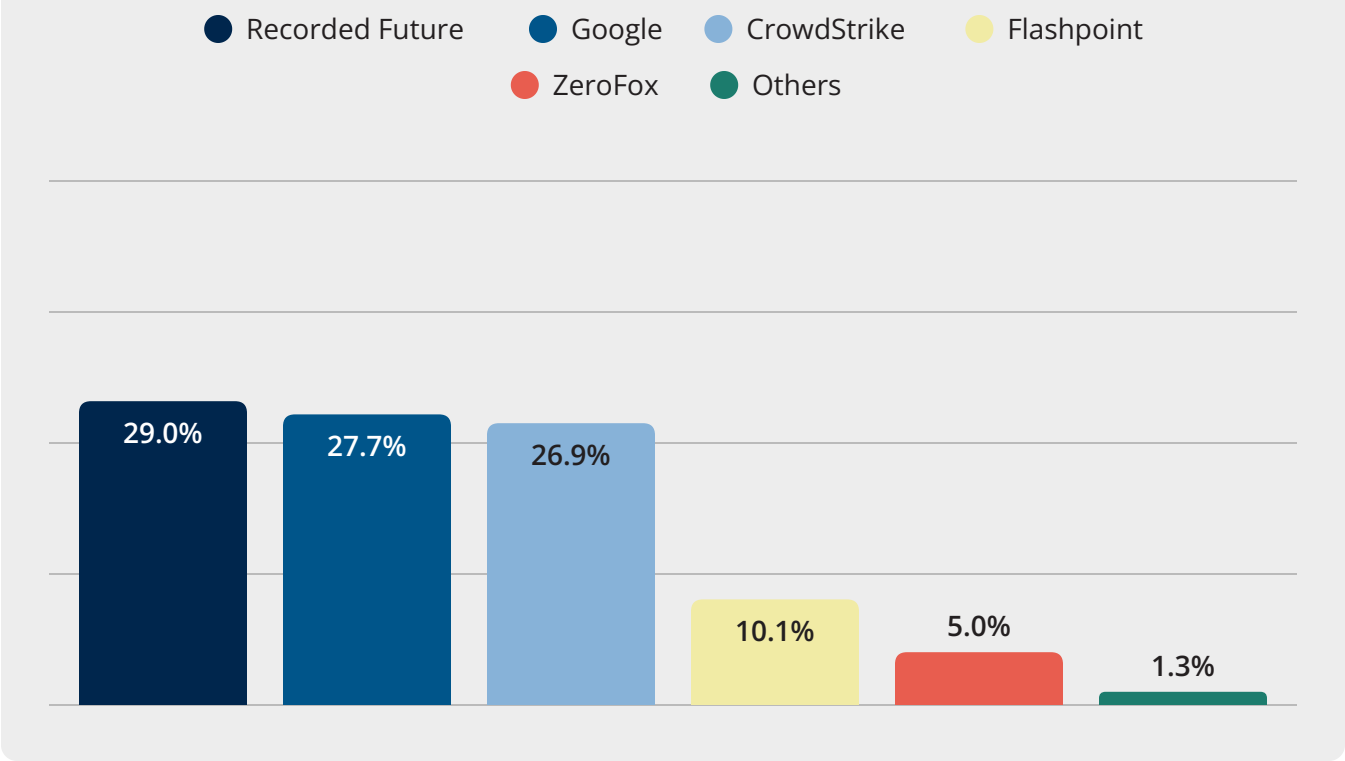
In Innovation Leader voting, 27.2% of IT professionals selected Palo Alto Networks Cortex Xpanse, followed by CyCognito (25.2%), CrowdStrike Falcon Surface (19.3%), Microsoft Defender EASM (13.8%), and Tenable (13.4%). Palo Alto Networks also led Innovation Leader voting, but CyCognito finished about two points behind, a far stronger showing than its fifth-place market result.



Palo Alto Networks' innovation win reflects continued investment in automated discovery, attribution, and remediation of internet-facing assets inside Cortex. CyCognito's close second shows that voters also recognize specialists that use automation and AI to map and test the attack surface the way an adversary would.

Cyber Threat Intelligence Platforms (CTI)

In Market Leader voting, 29.0% of IT professionals selected Recorded Future, followed by Google Threat Intelligence (27.7%), CrowdStrike Falcon Adversary Intelligence (26.9%), Flashpoint (10.1%), and ZeroFox (5.0%). The top three finished within about two points of each other, one of the tightest races in the survey, showing that IT professionals see several intelligence brands as credible defaults.



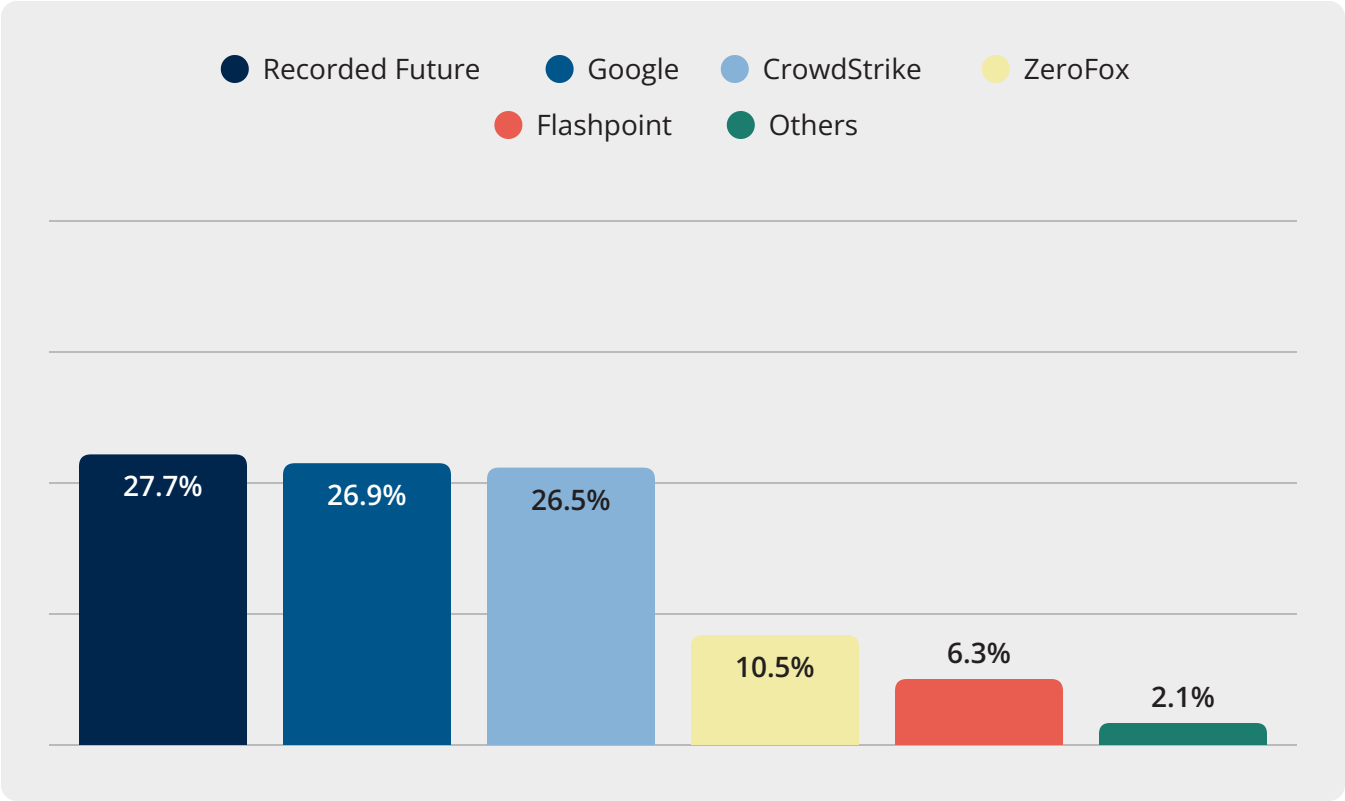
Recorded Future's narrow win reflects its long-standing position as one of the best-known pure-play intelligence brands and the breadth of its Intelligence Cloud. Now part of Mastercard, it competes with Google and CrowdStrike, which pair intelligence with their own security platforms, and that competition kept the margin close.

© 2026 IT BRAND PULSE

Cyber Threat Intelligence Platforms (CTI)



In Innovation Leader voting, 27.7% of IT professionals selected Recorded Future, followed by Google Threat Intelligence (26.9%), CrowdStrike Falcon Adversary Intelligence (26.5%), ZeroFox (10.5%), and Flashpoint (6.3%). Innovation Leader voting was even closer, with little more than a point separating the top three, while ZeroFox moved ahead of Flashpoint for fourth place.



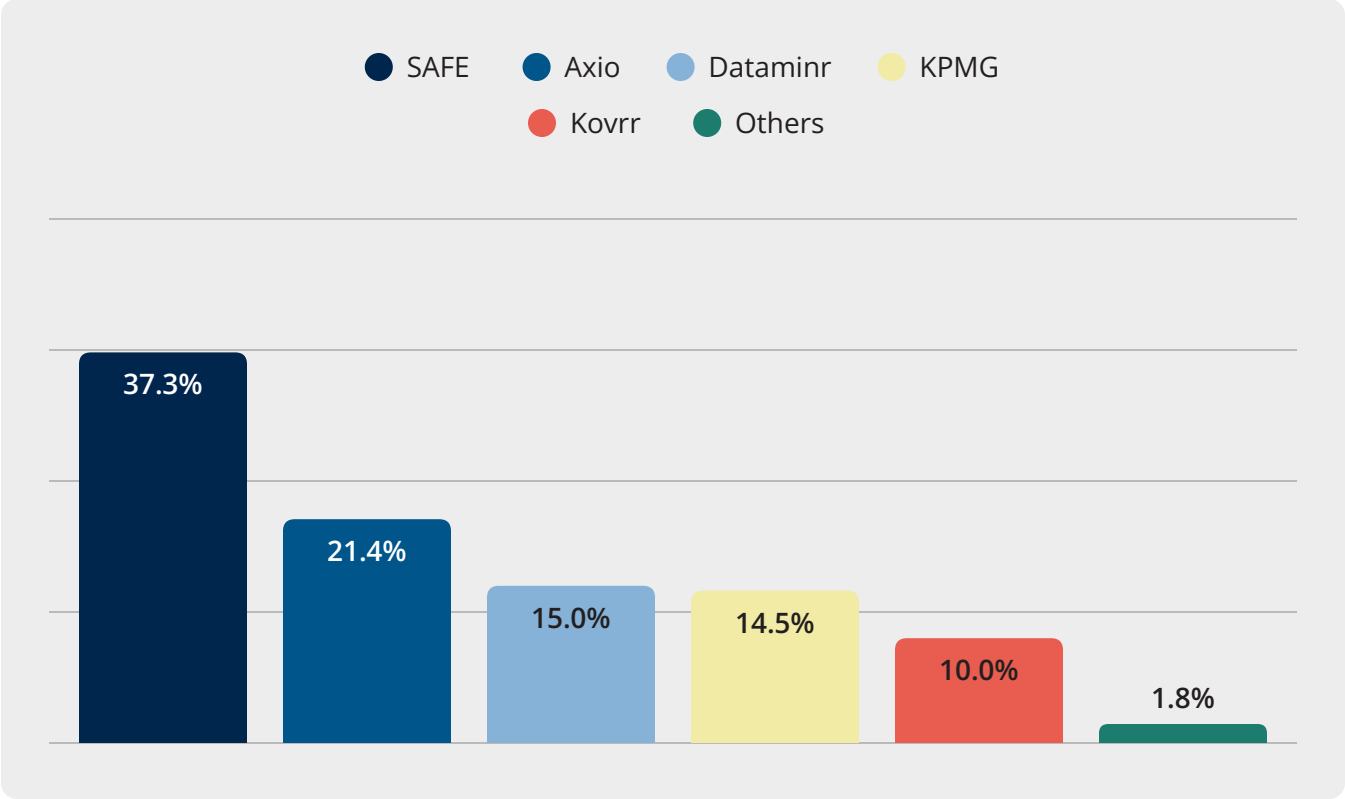
Recorded Future®

Voters credited Recorded Future with innovation by a slim margin, likely reflecting its use of AI to turn large volumes of threat data into prioritized, actionable intelligence. Google, which combines Mandiant expertise with VirusTotal, and CrowdStrike, with adversary intelligence built into Falcon, remain right behind it.

Cyber Risk Quantification Platforms (CRQ)



In Market Leader voting, 37.3% of IT professionals selected SAFE One, followed by Axio360 (21.4%), Dataminr ThreatConnect Risk Quantifier (15.0%), KPMG (14.5%), and Kovrr (10.0%). SAFE won by nearly 16 points, the widest Market Leader margin in the survey, marking it as the clear reference brand for cyber risk quantification.

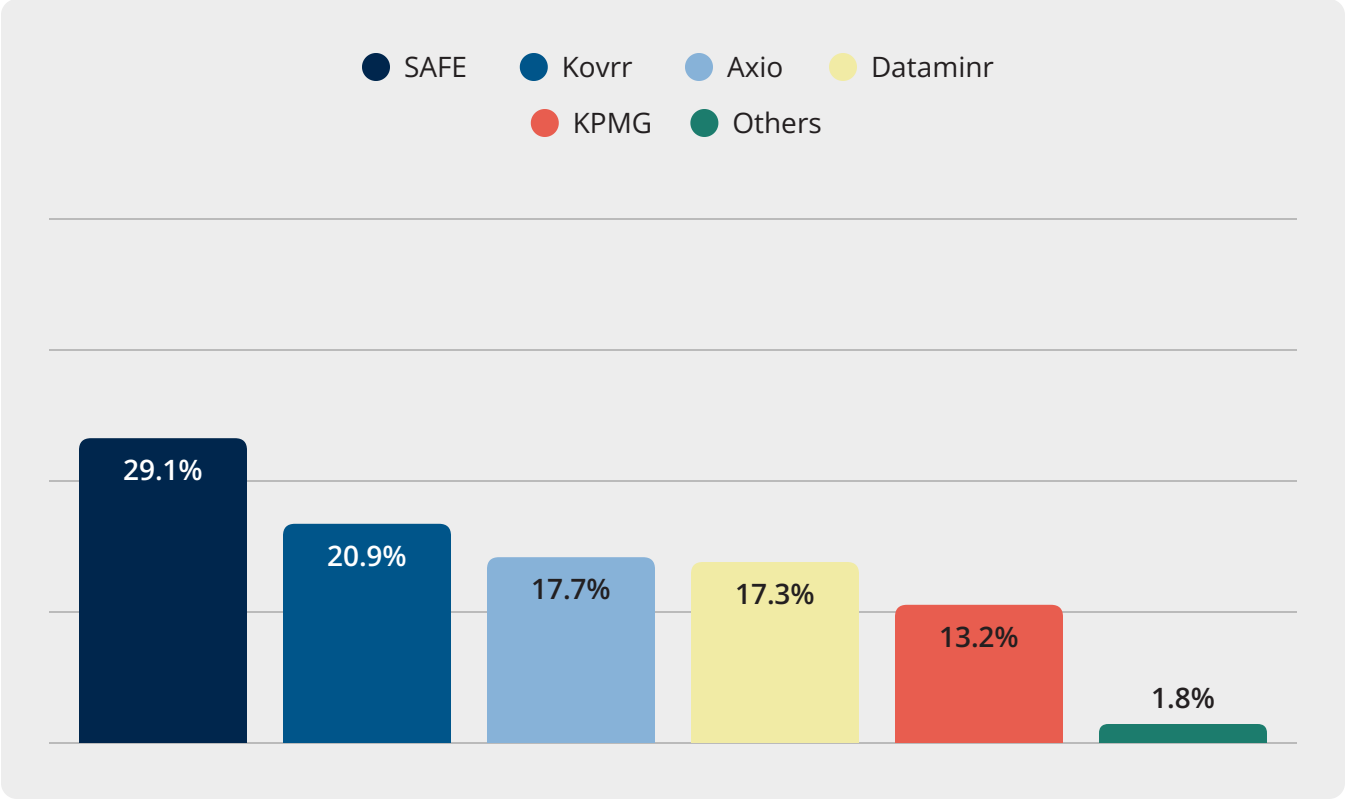


SAFE's lead reflects a focused bet on expressing cyber risk in financial terms, strengthened by its acquisition of RiskLens, one of the early names in risk quantification. Boards and CISOs increasingly want risk stated in dollars, and SAFE has become closely associated with that conversation.

Cyber Risk Quantification Platforms (CRQ)



In Innovation Leader voting, 29.1% of IT professionals selected SAFE One, followed by Kovrr (20.9%), Axio360 (17.7%), Dataminr ThreatConnect Risk Quantifier (17.3%), and KPMG (13.2%). SAFE also led Innovation Leader voting, while Kovrr climbed from fifth in market voting to second, suggesting IT professionals see the specialist as one of the more inventive CRQ vendors.

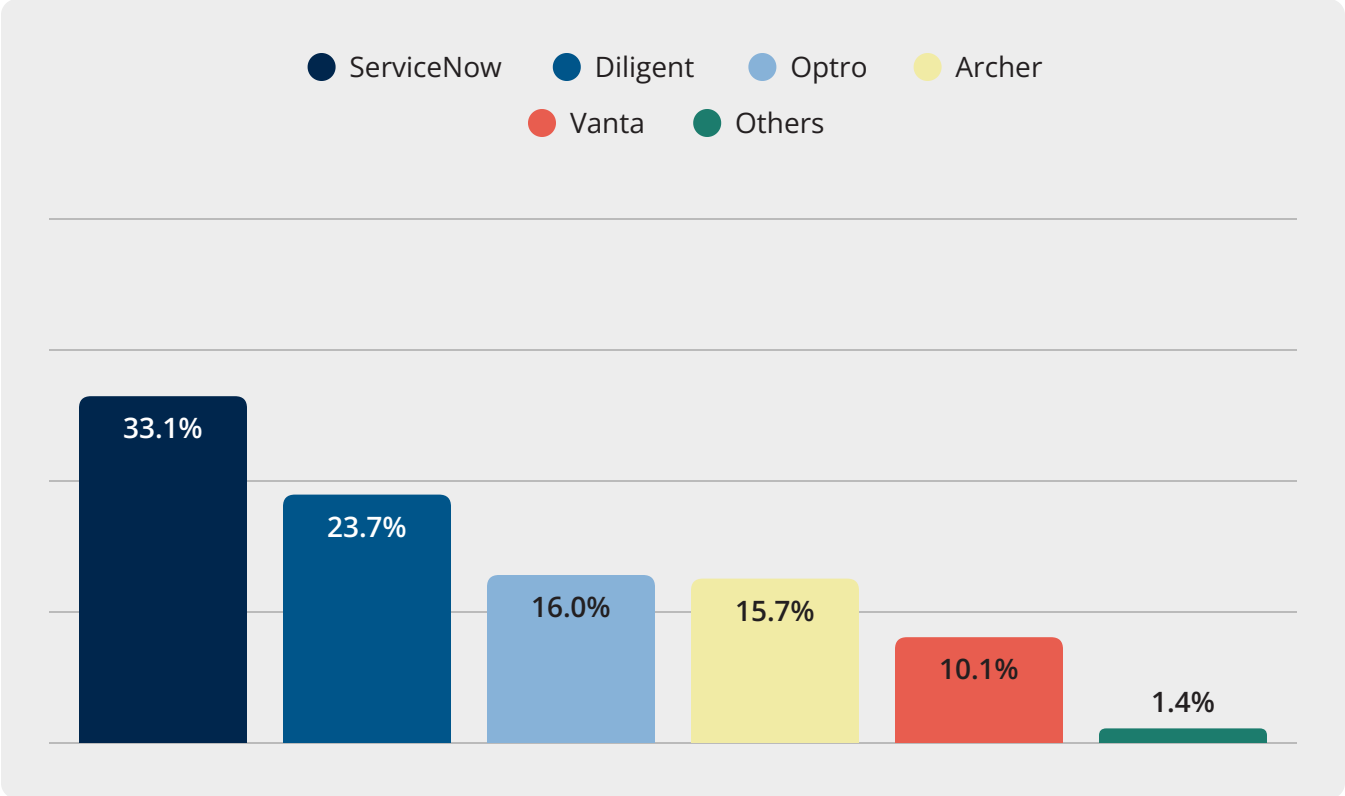


SAFE's innovation win suggests voters credit its AI-driven approach, which combines internal telemetry, external signals, and threat data to model loss scenarios continuously rather than in periodic workshops. The result is risk quantification that can keep pace with a changing attack surface.

Governance, Risk, and Compliance Platforms (GRC)



In Market Leader voting, 33.1% of IT professionals selected ServiceNow Integrated Risk Management, followed by Diligent One (23.7%), Optro (16.0%), Archer (15.7%), and Vanta (10.1%). ServiceNow finished more than nine points ahead of Diligent, with Optro and Archer close behind in a near tie for third.



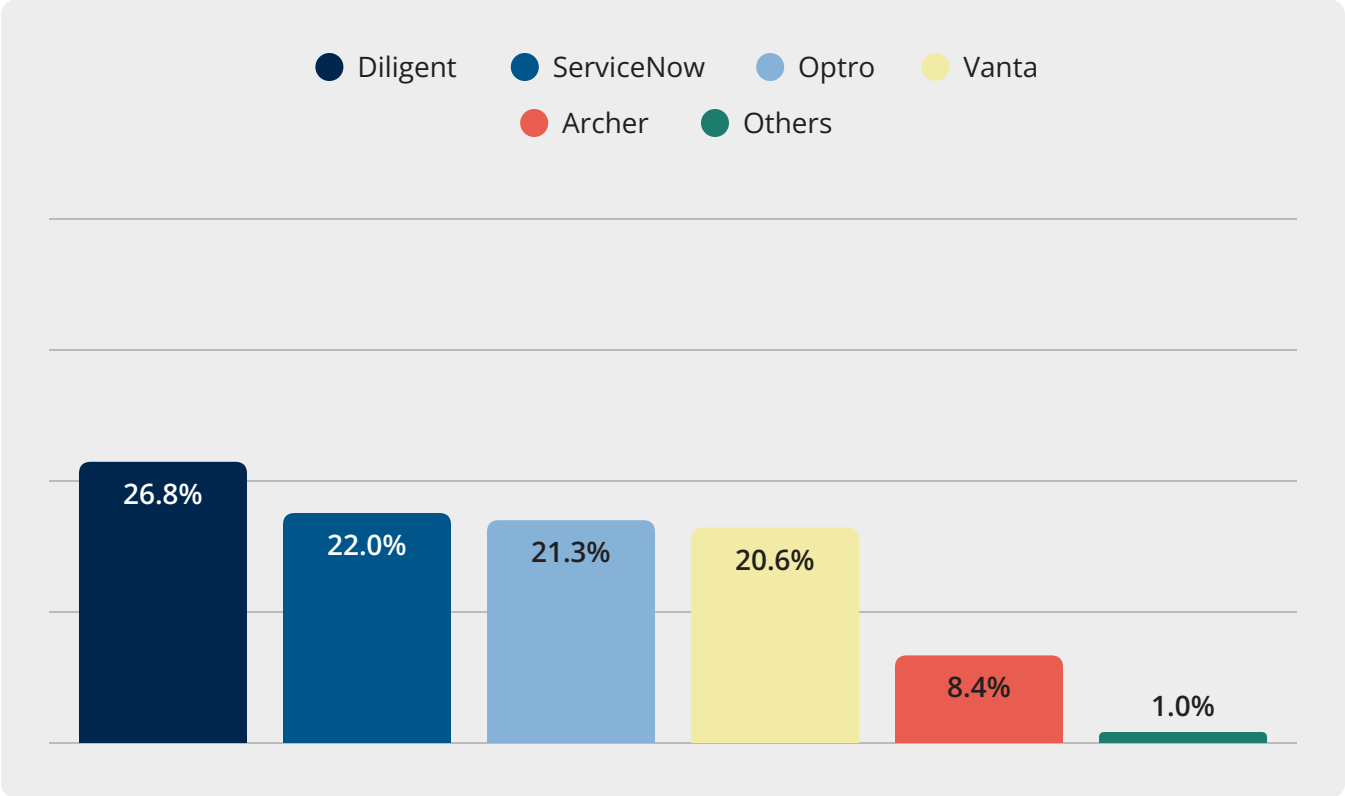
servicenow

ServiceNow's lead reflects the reach of its platform among IT professionals and the appeal of managing risk, policy, audit, and compliance on the same system as IT and security workflows. For many enterprises, integrated risk management is a natural extension of a platform they already run.

Governance, Risk, and Compliance Platforms (GRC)



In Innovation Leader voting, 26.8% of IT professionals selected Diligent One, followed by ServiceNow Integrated Risk Management (22.0%), Optro (21.3%), Vanta (20.6%), and Archer (8.4%). Diligent led Innovation Leader voting, with ServiceNow, Optro, and Vanta separated by less than two points behind it in an open race for GRC innovation.



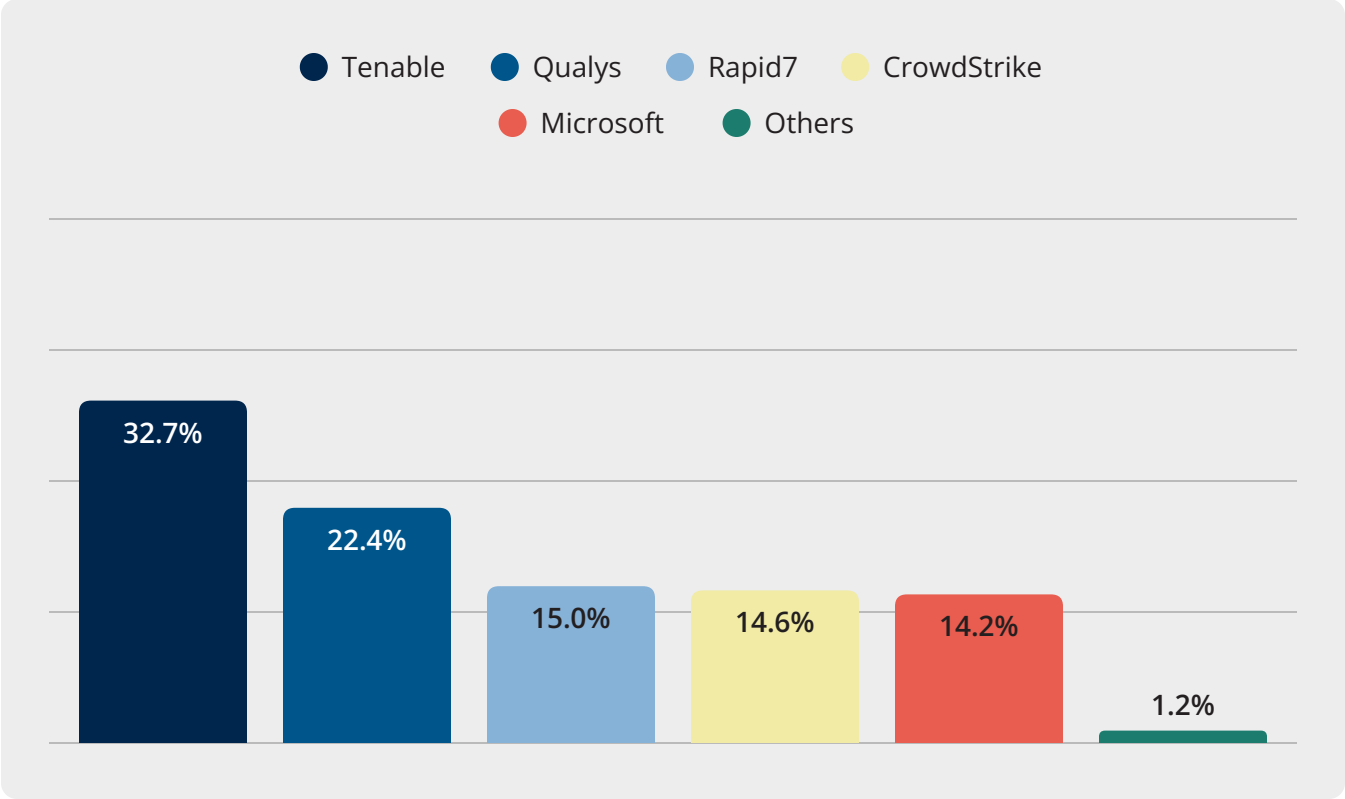
Diligent

Diligent's innovation win likely reflects its push to connect board governance, risk, audit, and compliance on one platform, with AI that helps leaders see and report on risk. Vanta's strong showing, from a company better known for compliance automation, signals that voters expect GRC to become more automated and continuous.

Exposure Management Platforms



In Market Leader voting, 32.7% of IT professionals selected Tenable One, followed by Qualys Enterprise TruRisk Management (22.4%), Rapid7 Exposure Command (15.0%), CrowdStrike Falcon Exposure Management (14.6%), and Microsoft Security Exposure Management (14.2%). Tenable led by more than ten points, while Rapid7, CrowdStrike, and Microsoft finished within a point of each other, leaving the race behind the two incumbents wide open.



tenable

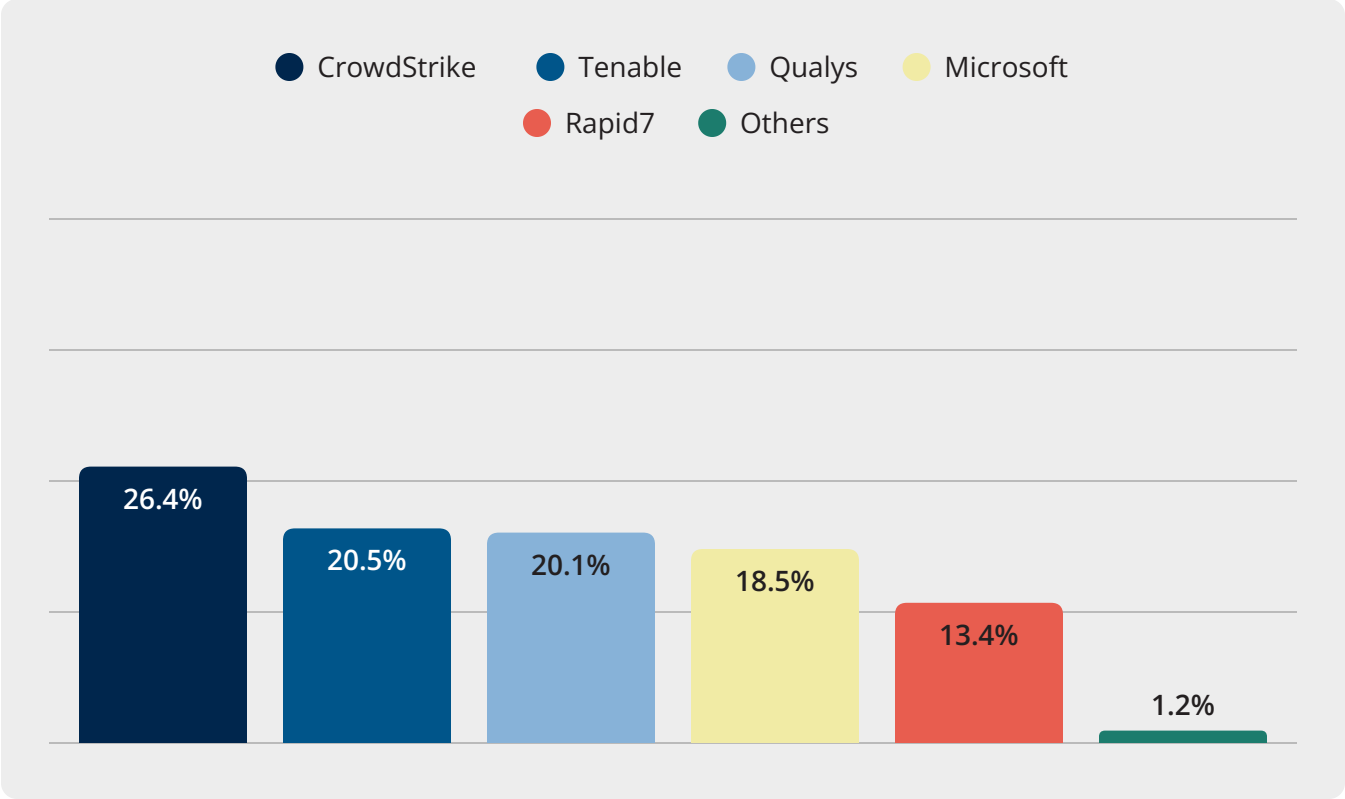
Tenable's lead reflects the strength of its vulnerability management heritage and its early move to unify assets, vulnerabilities, identities, and cloud exposures in Tenable One. IT professionals appear to see Tenable as the natural default as exposure management grows out of vulnerability management.

© 2026 IT BRAND PULSE

Exposure Management Platforms



In Innovation Leader voting, 26.4% of IT professionals selected CrowdStrike Falcon Exposure Management, followed by Tenable One (20.5%), Qualys Enterprise TruRisk Management (20.1%), Microsoft Security Exposure Management (18.5%), and Rapid7 Exposure Command (13.4%). CrowdStrike led Innovation Leader voting by nearly six points after placing fourth in market voting, one of the clearest market and innovation splits in the survey.



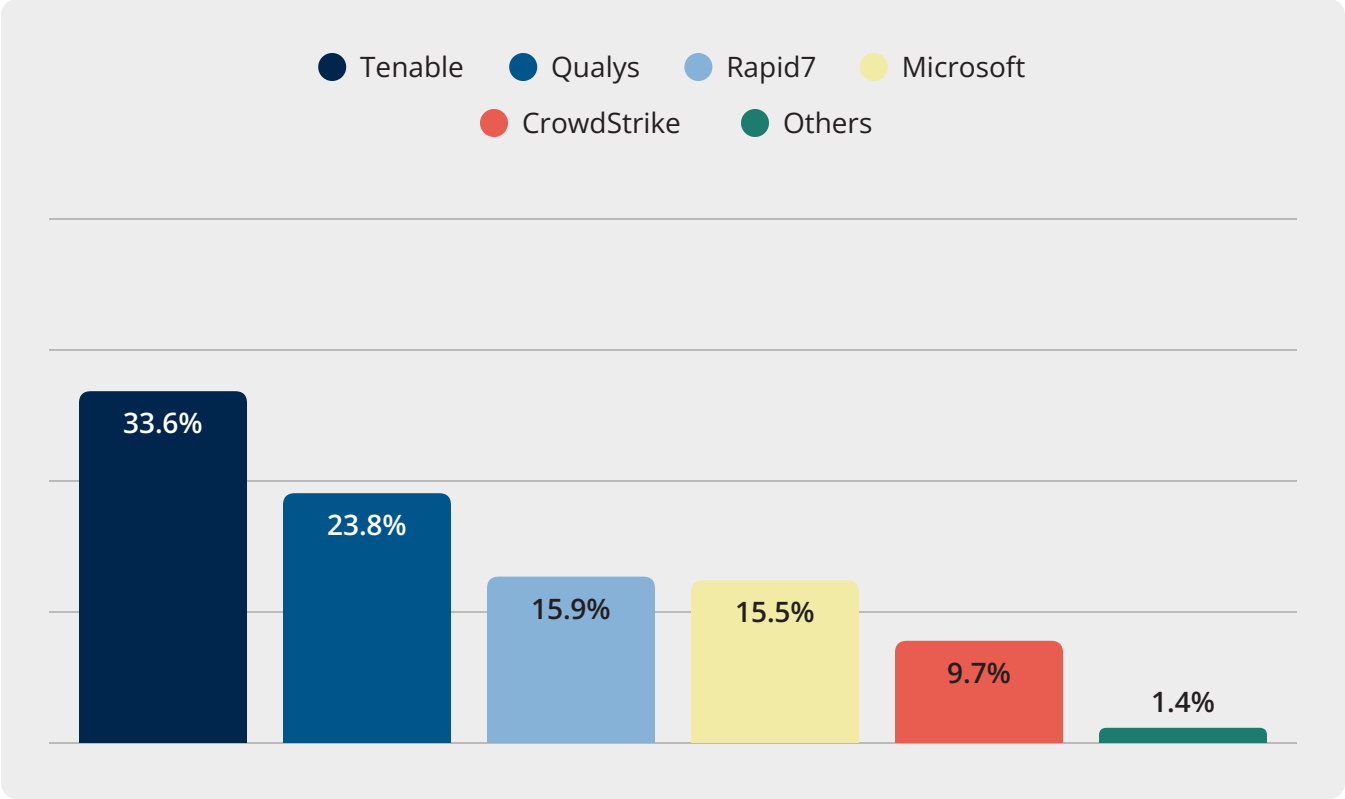
CROWDSTRIKE

CrowdStrike's innovation win suggests voters credit its approach of building exposure management into the Falcon platform, using the same agent and threat intelligence to prioritize the exposures adversaries are most likely to exploit. That link between exposure data and real attacker behavior is reshaping how buyers judge innovation.

Vulnerability Management Platforms



In Market Leader voting, 33.6% of IT professionals selected Tenable Vulnerability Management, followed by Qualys VMDR (23.8%), Rapid7 InsightVM (15.9%), Microsoft Defender Vulnerability Management (15.5%), and CrowdStrike Falcon Exposure Management (9.7%). Tenable won by nearly ten points over Qualys in a mature market where long-established scanners remain the default choice.



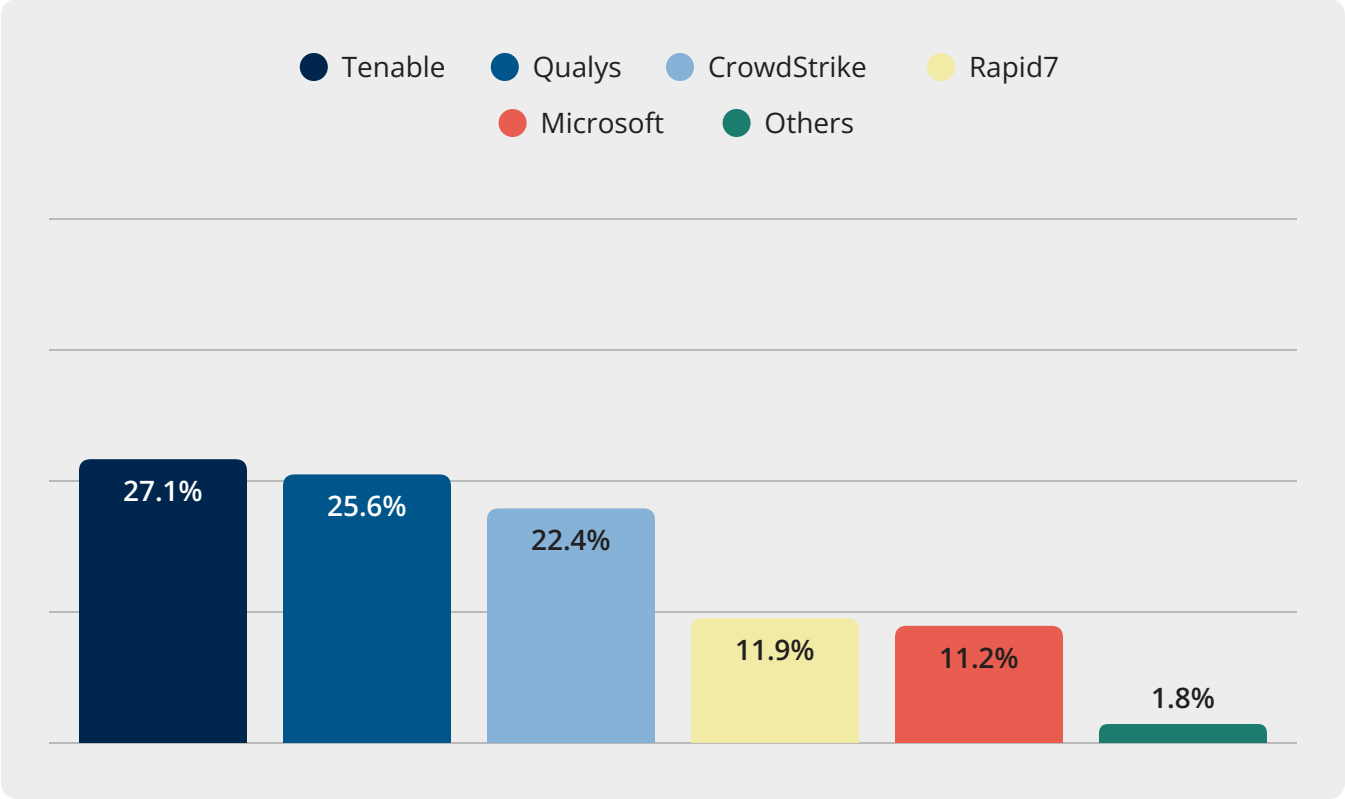
Tenable's lead reflects more than two decades of brand recognition built on Nessus, one of the most widely used vulnerability scanners, and the continued strength of Tenable Vulnerability Management in enterprise environments. For many IT professionals, Tenable remains the brand most closely associated with finding vulnerabilities.

© 2026 IT BRAND PULSE

Vulnerability Management Platforms



In Innovation Leader voting, 27.1% of IT professionals selected Tenable Vulnerability Management, followed by Qualys VMDR (25.6%), CrowdStrike Falcon Exposure Management (22.4%), Rapid7 InsightVM (11.9%), and Microsoft Defender Vulnerability Management (11.2%). Tenable also led Innovation Leader voting, but Qualys finished about 1.5 points behind and CrowdStrike placed third, well ahead of its fifth-place market result.

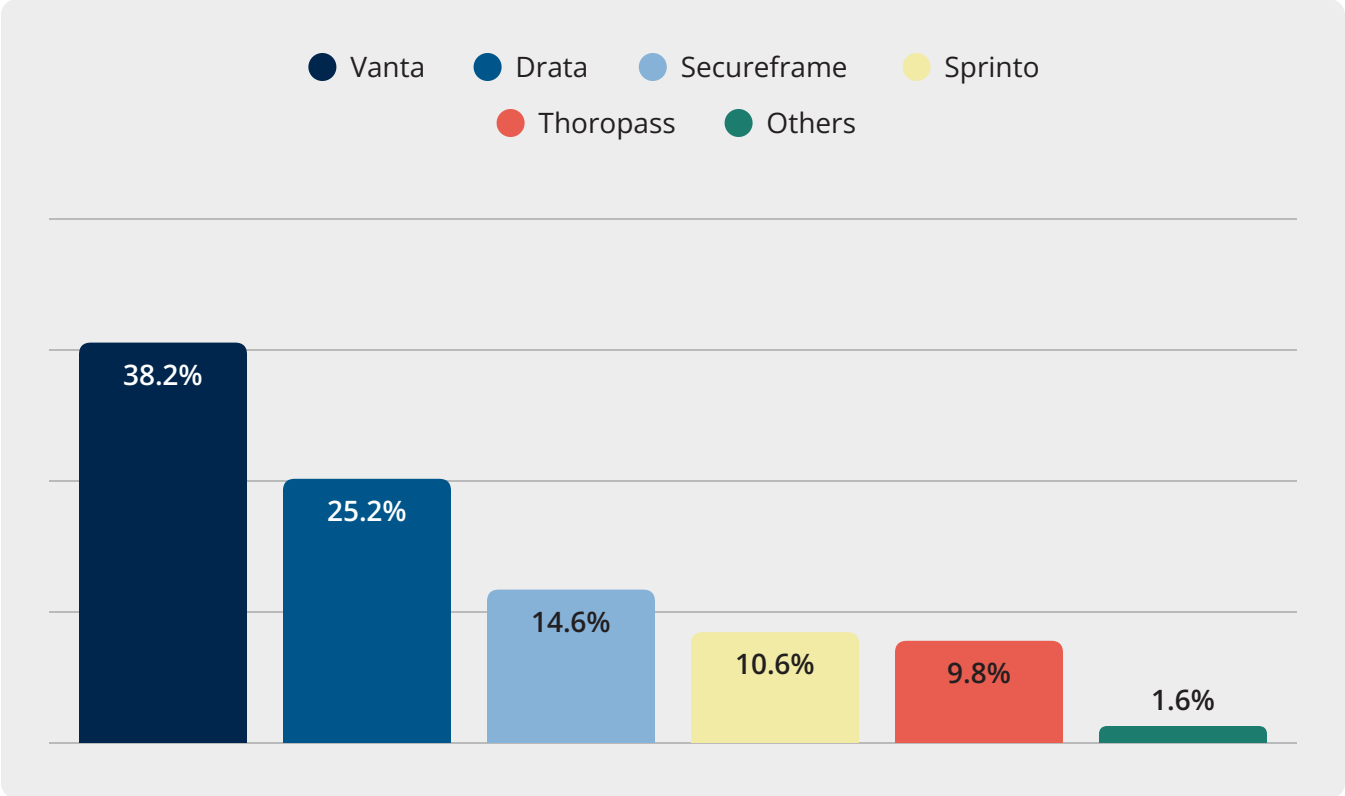


Tenable's innovation win suggests voters credit its work on risk-based prioritization, which uses threat context and AI to show which vulnerabilities matter most. Qualys, with TruRisk scoring, and CrowdStrike, with agent-based assessment, show that innovation in this category now centers on prioritization rather than discovery.

© 2026 IT BRAND PULSE

Security Compliance Automation and Trust Management Platforms

In Market Leader voting, 38.2% of IT professionals selected Vanta, followed by Drata (25.2%), Secureframe (14.6%), Sprinto (10.6%), and Thoropass (9.8%). Vanta won by 13 points, one of the widest Market Leader margins in the survey, reflecting the scale it has built in compliance automation.

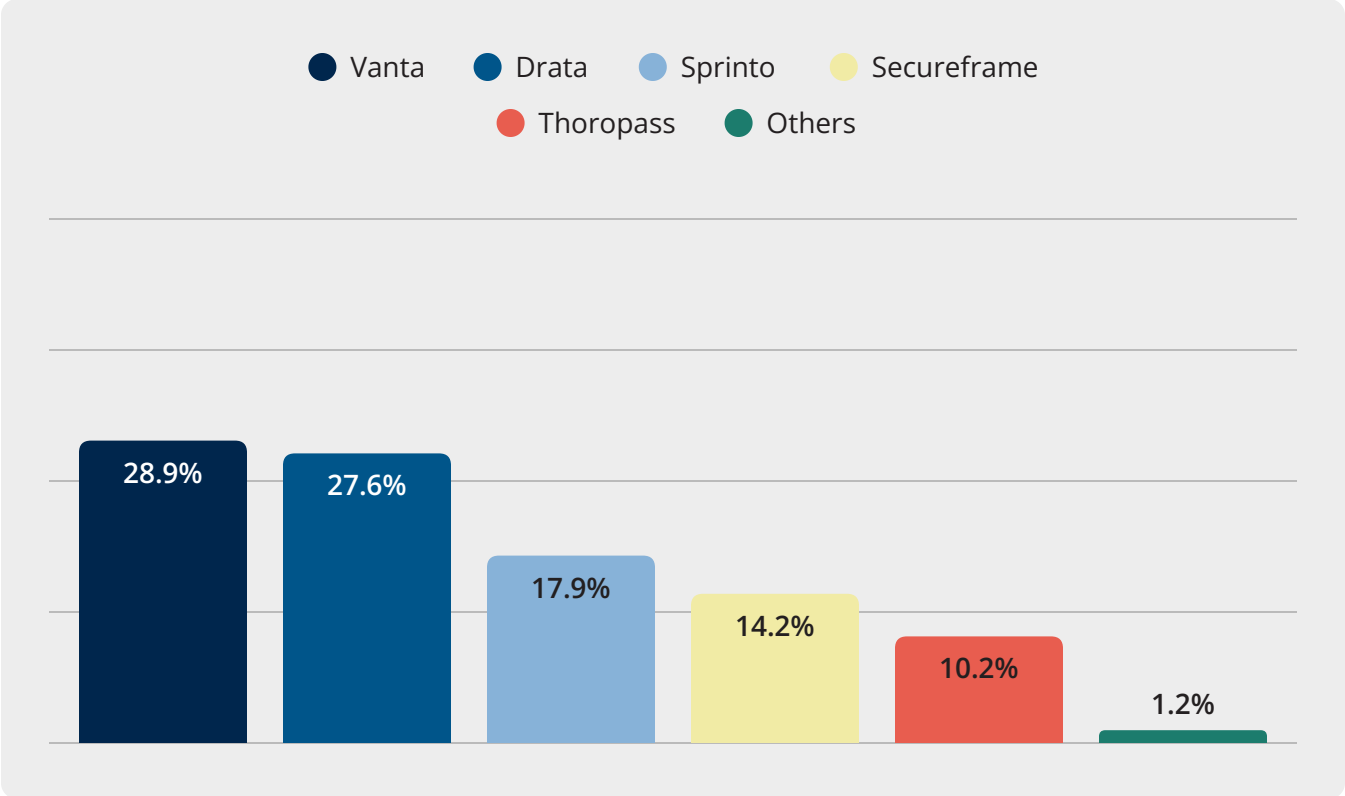


Vanta's lead reflects how quickly it has scaled, with reported annual recurring revenue passing $300 million in 2026, and its broad adoption among companies preparing for SOC 2, ISO 27001, and other audits. Its trust management platform has made it the brand most associated with automating compliance.

Security Compliance Automation and Trust Management Platforms



In Innovation Leader voting, 28.9% of IT professionals selected Vanta, followed by Drata (27.6%), Sprinto (17.9%), Secureframe (14.2%), and Thoropass (10.2%). Innovation Leader voting was much closer, with Vanta leading Drata by just over one point and Sprinto moving ahead of Secureframe into third.



Vanta

Vanta's narrow innovation win suggests voters credit its use of AI agents to automate evidence collection, security questionnaires, and continuous control monitoring. Drata's close second shows the two vendors are seen as pushing each other to make compliance continuous rather than an annual scramble.

© 2026 IT BRAND PULSE

Looking Forward

Cyber risk management is entering an AI-driven phase. The first generation of tools produced scores, scan results, and questionnaires that teams reviewed on a periodic cycle. Over the next three to five years, differentiation will shift toward platforms that monitor continuously, use AI to prioritize what matters, and connect findings directly to remediation and executive decisions.

As attack surfaces expand across cloud services, identities, suppliers, and AI systems themselves, buyers will place greater value on measurable risk reduction than on the volume of findings a product produces. Brand leadership will increasingly be defined by a vendor's ability to show that its platform reduces risk, not just reports it.

IT Brand Pulse expects consolidation to continue as exposure, vulnerability, and attack surface management converge, and as ratings, third-party risk, and supply chain monitoring move closer together. At the same time, specialists in risk quantification, supply chain response, and compliance automation have an opportunity to establish leadership before that consolidation is complete.

Predictions

1. Exposure and vulnerability management will converge.
Vulnerability scanning, attack surface management, and cloud posture findings will increasingly be managed as one exposure program, prioritized by business impact and real attacker behavior. Analyst firms have already begun evaluating the market as exposure assessment rather than vulnerability assessment. Vendors that unify discovery, prioritization, and remediation across assets, identities, and suppliers will strengthen both their market and innovation leadership.

2. Third-party risk will shift from assessment to continuous response.
Within the next three years, periodic vendor questionnaires and static ratings will give way to continuous monitoring of suppliers and fourth parties, with coordinated detection and remediation when a supplier is breached. Ratings, third-party risk management, and supply chain monitoring will increasingly be bought together, and the strong innovation vote for SecurityScorecard suggests IT professionals already see the shift underway.

3. Cyber risk will be managed in financial terms.
Boards, regulators, and insurers will expect security leaders to express cyber risk in dollars and to show how investments reduce it. Risk quantification, GRC, and compliance automation will become tightly linked, and AI agents will take on much of the evidence collection and reporting work, giving vendors that connect technical findings to business risk a growing role in executive decisions.

About the Author

Frank Berry, Founder and Senior Analyst, IT Brand Pulse

Frank Berry is one of the technology industry's earliest advocates for AI Memory as a foundational layer of the AI stack. He is the former Vice President of Marketing at MemVerge, where he helped pioneer industry awareness around memory-centric computing, software-defined memory, and emerging AI memory architectures.

Since 2022, Frank has led the AI Memory Forum community, bringing together AI developers, infrastructure architects, researchers, startups, and enterprise technology leaders focused on the future of memory-enabled AI systems. Under his leadership, the community has hosted 16 AI Memory Forum events and Frank has moderated the popular AI Memory Forum LinkedIn Group with over 2,000 members and growing.

As an industry analyst, Frank is researching and writing extensively on Personal AI Memory, AI agent memory, multimodal memory, enterprise memory architectures, and memory infrastructure platforms. His work explores how persistent memory may become a foundational component of future AI systems, enabling context awareness, cognitive orchestration, and personalized AI experiences across models, agents, applications, and devices.

About IT Brand Pulse

Since 2008, IT Brand Pulse has conducted the industry's only brand leader research voted by IT Pros. Today, we combine customer research with independent analysis to measure customer perceptions of AI product brands, identify market leaders, evaluate emerging technologies, and provide insight into the products, companies, and trends shaping the future of AI.

AI Brand Leader Program

IT Brand Pulse Brand Leader Awards are voted by thousands of IT professionals, not algorithms or small judging panels. Our surveys measure brand perception across the Five Pillars of AI brand leadership, giving winners credible, third-party validation that resonates with customers, analysts, and investors.

Infrastructure and security surveys vote the Market Leader and the Innovation Leader in each category. Every voter chooses from a randomized vendor list with a write-in option, one vote per verified IT professional. Readers never pay, and vendors never touch the vote.

See the latest survey results at:
https://itbrandpulse.com/brand-leader-program







© 2026 IT BRAND PULSE



Industry First Program

IT Brand Pulse's Industry First Program provides independent, third-party validation that you were first to deliver a meaningful AI innovation. Our analysts verify your timeline, technical claims, and market precedence, then publish a comprehensive validation article documenting your achievement.

See the latest industry firsts and nominate your product at: itbrandpulse.com/industry-first

---

Voted by humans, not algorithms.

IT Brand Pulse analyzes the market, measures who leads it, and convenes the people who decide. Readers never pay. Vendors never touch the vote.

info@itbrandpulse.com
itbrandpulse.com
1895 Avenida Del Oro #4683
Oceanside, CA 92052

© 2026 IT Brand Pulse