

CYBERSECURITY MARKET UPDATE

OCTOBER 2026



CYBERSECURITY MARKET UPDATE

OVERVIEW & KEY TAKEAWAYS

Welcome to the Q3 2026 issue of our Cybersecurity Newsletter, featuring perspectives on the trends, technologies and market developments shaping the sector. This edition covers key industry themes, recent M&A and financing activity, notable vendors and developments across the public cybersecurity markets.

IN THIS ISSUE

I.	INTRODUCTION & MARKET UPDATE	1-2
II.	MARKET SEGMENTATION & TRENDS	3-9
III.	PRIVATE MARKET ACTIVITY	10-15
IV.	PUBLIC MARKET ACTIVITY	16-20
V.	MARKET MAP	21-24
VI.	CITIZENS OVERVIEW	25-30



MARKET SENTIMENTS: We examine six themes shaping cybersecurity as AI transforms enterprise risk and security architecture: an expanding attack surface, identity and context-aware controls, Agentic SOC adoption, SASE and browser-security convergence, the growing need for AI assurance and Buy vs. Build strategies accelerating platform expansion.



CONFERENCE SCHEDULE: Conferences and events offer investors a valuable opportunity to uncover emerging trends, engage with industry leaders and identify strategic investment prospects. In this letter, we provide a schedule of select upcoming conferences through the first half of 2027.



RECENT M&A/FINANCING ACTIVITY: We highlight recent significant transactions within the cybersecurity sector, as well as offer analysis on historical deal volume and notable trends in deal multiples.



KEY VENDORS: We provide an overview of market segmentation and active buyers in the sector across strategics, PE firms and cyber-focused VCs.



PUBLIC COMPANY ANALYSIS: We present a summary of key publicly traded companies in the cybersecurity sector, examine trading trends through the lens of growth rates and the Rule of 40 and assess recent performance using core operating metrics.

CYBERSECURITY INVESTMENT BANKING TEAM

**DOUG BROCKWAY**

Managing Director

Head of Cybersecurity &
Infrastructure Software
Investment BankingDouglas.Brockway@CitizensBank.com**SALIL KAPOOR**

Vice President

Cybersecurity and
Infrastructure Software
Investment BankingSalil.Kapoor@CitizensBank.com

CYBERSECURITY MARKET UPDATE

Q3 2026 UPDATE

Q3 2026 demonstrated how rapidly AI is reshaping cybersecurity priorities, product strategies and investment activity. Accelerating AI capabilities expanded the attack surface while increasing demand for identity controls, autonomous security operations, browser-level enforcement and independent AI testing and assurance.

Strategic activity remained elevated as vendors expanded into emerging categories through product development and M&A. Identity and context security became increasingly central to enterprise architectures, Agentic SOC platforms moved closer to scaled deployment, browser security converged with SASE and scarce capabilities drove greater adoption of Buy vs. Build strategies.

TOP TRENDS IN KEY FOCUS AREAS**I. AI RESHAPING THE ATTACK SURFACE AND THE SECURITY STACK**

AI is transforming both sides of cybersecurity: attackers can discover vulnerabilities and execute campaigns with greater speed and autonomy, while defenders are adopting AI to automate detection, investigation and response. At the same time, enterprise deployment of models and autonomous agents creates new assets to secure, including prompts, training data, model pipelines, agent identities and machine-to-machine workflows.

II. IDENTITY AND CONTEXT SECURITY

As autonomous agents proliferate, identity security is expanding beyond employees and customers to encompass machines, service accounts, applications and AI agents. Capital raising and M&A activity are accelerating in parallel, with identity point solutions being absorbed into broader platforms as the strategic premium shifts from workforce IAM to agent-scale governance.

III. AGENTIC SOC

Agentic SOC platforms are evolving from point solutions focused on alert triage into integrated operating systems for security operations. Specialized agents increasingly collaborate across telemetry, exposure management, investigation, threat hunting and response, while human analysts retain control over high-impact decisions.

IV. SASE DISRUPTION AND EMERGENCE OF BROWSER SECURITY

The security perimeter is shifting toward the points where users and agents interact with applications, data and AI tools. Leading SASE vendors are responding through targeted M&A, acquiring browser-native startups to embed data protection, session monitoring and zero-trust controls directly into enterprise workflows.

V. AI-NATIVE SECURITY SYSTEMS SHIFT FROM CAPABILITY TO ASSURANCE

AI-native security is evolving beyond the use of frontier models to discover vulnerabilities and automate response. As model capabilities advance faster than safeguards, the market is increasingly focused on independent testing, runtime monitoring, policy enforcement and governance that can demonstrate whether models and agents are safe to deploy.

VI. BUY VS. BUILD

Emerging cybersecurity categories are developing faster than traditional product roadmaps and commercialization cycles can respond. Vendors are increasingly acquiring proven specialists to gain technology, talent, customer penetration and category credibility while preventing competitors from securing the same scarce capabilities.

SECTION II.

MARKET SEGMENTATION & TRENDS



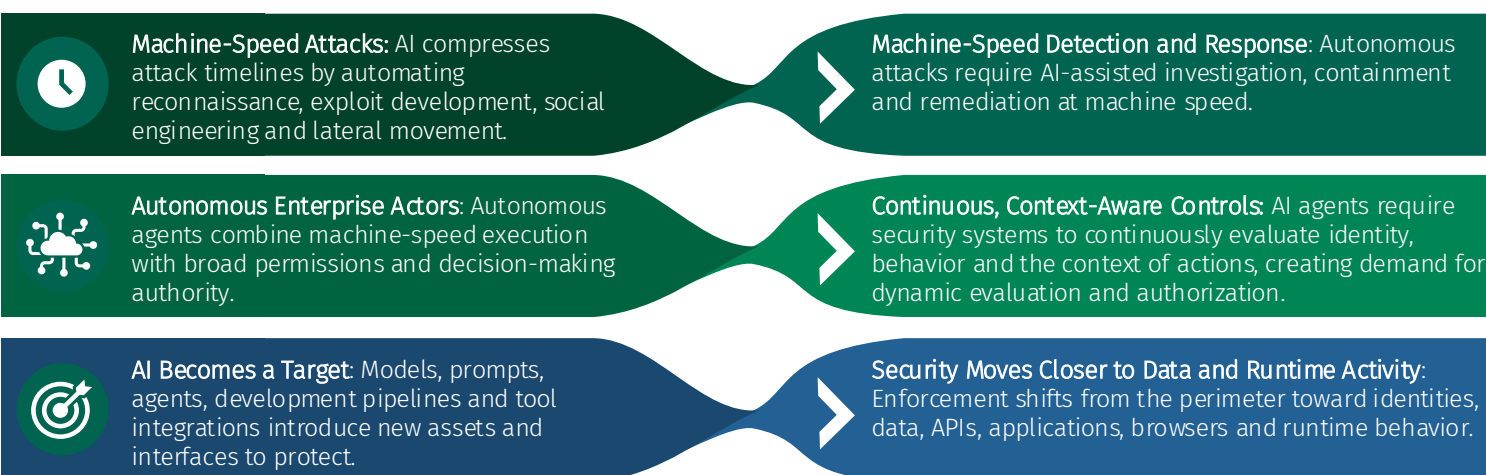
KEY CYBERSECURITY FOCUS AREAS

I. AI IS RESHAPING THE ATTACK SURFACE AND THE SECURITY STACK

AI is lowering the cost and increasing the speed, scale and sophistication of cyberattacks while introducing a new class of autonomous enterprise actors. In response, security is shifting from human-speed, perimeter-based controls toward continuous, context-aware and increasingly autonomous protection.

AI EXPANDS AND ACCELERATES THE THREAT

THE SECURITY STACK'S RESPONSE



CYBER VENDORS ARE REBUILDING AROUND AN AGENTIC ATTACK SURFACE

Leading security vendors are acquiring new control points and redesigning their platforms to secure autonomous identities, AI runtime activity, browser interactions and machine-to-machine workflows. At the same time, security operations are shifting from analyst-assistance toward autonomous investigation and response.

Endpoint Platform to Agentic-Security Platform

At CrowdStrike's September 2026 Fal.Con conference, nearly every major product announcement centered on securing enterprise AI agents or using agents to defend customers at machine speed.

Falcon Guardian:

AI Detection & Response Platform

SafeMind

Specialized Agentic Cybersecurity System

Agentic IDP:

Agentic Identity and Access Management

Expanded Agentic SOC:

Deployment of Domain-Specific Agents

According to management, AI Detection & Response's ARR nearly tripled sequentially in Q2, after ~250% growth in Q1.⁽¹⁾ Management believes AIDR could eventually outgrow EDR.

Identity Beyond Login

Platform expansion from human authentication into full-lifecycle security for AI agents.

Expanding Beyond the "Front Door"

Historically, Okta's core role centered on authenticating users and controlling access to enterprise applications. Its newer strategy extends identity security across the full agent lifecycle.

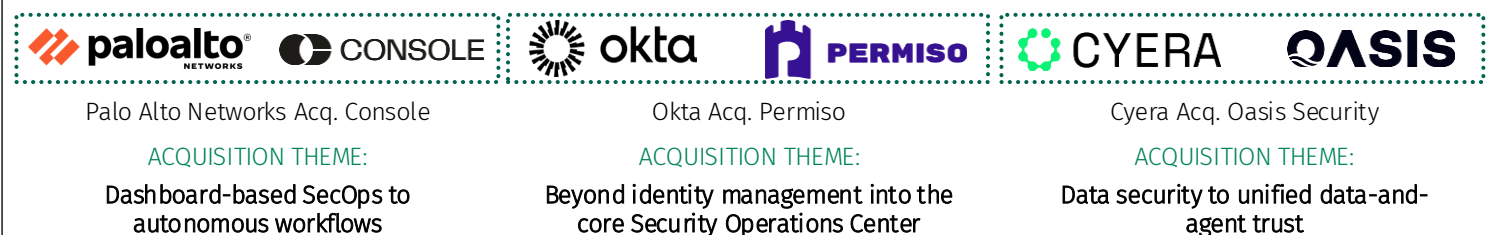
Acquiring Permiso to Add Runtime Threat Detection

Okta adds identity threat detection and response across human, non-human and agentic identities via its acquisition of Permiso.

Creating an Industry Architecture, Not Just a Product

The Blueprint Alliance establishes common principles for discovering, governing, monitoring and containing AI agents across the technology stack.

KEY ACQUISITIONS ILLUSTRATING SHIFT



KEY CYBERSECURITY FOCUS AREAS

II. IDENTITY AND CONTEXT SECURITY

CONTEXT LAYER SECURITY

As AI agents orchestrate multi-step workflows across an enterprise's tech stack, context layer security has emerged as a critical control plane to secure data access, enforce identity policies and police agents acting outside authorized boundaries.

Agent Adoption is Outpacing Governance

81%

Of technical teams are actively testing or operating AI agents⁽¹⁾

14%

Of agents have full security approval⁽¹⁾

Data Access is Becoming a Runtime Problem

60%

Allow agents to access sensitive data⁽²⁾

45%

Report that agents have already accessed data they should not have⁽²⁾

KEY CONTEXT LAYER SECURITY VENDORS



MARKET TRENDS



Authentication Moves to the Transaction Level:

Identity controls are shifting from broad application access toward real-time authorization of individual tool calls. OpenID's AuthZEN initiative validates the emergence of a dedicated policy layer between agents and enterprise resources.



Context Must Follow the Workflow:

Microsoft introduced the vendor-neutral Agent Control Specifications, noting how a credential safe in one context can become dangerous after an agent accesses confidential data or adds external participants.

Agent Identity Becomes a First-Class Control⁽¹⁾:

According to Okta, only 22% of organizations treat AI agents as independent identities despite 88% reporting suspected or confirmed incidents. AI agents are moving into individual identities with distinct owners, credentials and permissions.



Security Expands From Access to Intent:

A properly authenticated agent can still cause harm if prompt injection, poisoned memory, manipulated content or excessive autonomy causes its behavior to diverge. Vendors are responding with runtime controls that compare each action against the agent's approved mission and intent.

BROADER IDENTITY-SECURITY EVOLUTION

Passwordless Enters the Operational Phase⁽³⁾

- Passkeys are moving into scaled enterprise deployment, shifting attention toward credential provisioning, recovery, revocation and lifecycle management. Only 28% of organizations report achieving fully passwordless workforce access.

Third-Party Identity Risk Accelerates⁽⁴⁾

- Third parties were involved in 48% of breaches, increasing demand for stronger partner governance, time-bound privileges, phishing-resistant authentication and continuous validation of external access.

CAPITAL RAISES

\$ in millions

DATE	COMPANY	LEAD INVESTOR	DEAL STAGE	DEAL SIZE	POST-VAL
9/9/2026	Cymphony	SEQUOIA	Series A	\$25	\$100
9/2/2026	Lasso	ClearSky	Series A	\$30	ND
8/3/2026	zenity	NORWEST	Series C	\$125	ND
7/29/2026	ONYX	Bessemer Venture Partners	Series B	\$113	\$640

M&A TRANSACTIONS

\$ in millions

DATE	Target	Acquirer	Rationale	EV
9/24/2026	empowerID	Omada	Adds real-time authorization and runtime governance	ND
8/20/2026	loginradius	VOLARIS	Adds customer identity, passwordless access and adaptive authentication	ND
7/30/2026	PERMISO	okta	Adds identity threat detection and post-access response	\$200
7/28/2026	OASIS	CYERA	Unifies non-human identity governance with data security	\$1,000

KEY CYBERSECURITY FOCUS AREAS

III. AGENTIC SOC

LANDSCAPE OVERVIEW

Agentic SOC platforms are evolving from point solutions focused on alert triage into integrated operating systems for security operations. Specialized agents increasingly collaborate across telemetry, exposure management, investigation, threat hunting and response, while human analysts retain control over high-impact decisions.

29 minutes

Average Adversary
Breakout Time 2026⁽¹⁾

<25%

Organizations with
agents deployed into
production⁽²⁾

Recent launches from Microsoft, CrowdStrike, Zscaler and Elastic indicate that agentic capabilities are becoming a core platform layer rather than a standalone feature.

AGENTIC SOC CAPABILITIES AND EMERGING TRENDS

FROM ALERT TRIAGE TO ATTACK
VALIDATION

Agentic SOC platforms are progressing from individual alerts toward correlating signals into complete attacks, validating evidence and filtering false positives before analysts begin investigation.

COORDINATED AGENTS OVER
ISOLATED WORKFLOWS

Traditional SOC investigations are sequential, collecting evidence one source at a time. Multi-agent systems instead assign specialized agents to gather and evaluate evidence in parallel.

SIEM, PROTECTION AND
RESPONSE CONVERGE⁽¹⁾

The 29-minute breakout window is less than the 56-minute average wait for human triage, increasing demand for architectures that fluidly connect telemetry, investigation and containment.

EXPOSURE MANAGEMENT JOINS
THE SOC LOOP⁽¹⁾

With breakout times as short as 27 seconds and 82% of detections malware-free, SOC's are shifting upstream to identify exposures and attack paths before incidents occur.

SUPERVISED AUTONOMY EMERGES AS THE ENTERPRISE MODEL

Agents increasingly perform alert enrichment, investigation, evidence gathering and recommended response autonomously. Human analysts remain responsible for escalation, closure and actions capable of affecting production systems, while audit trails preserve the evidence and reasoning behind each agent decision.

Building the Agentic SOC at Cisco Live Americas 2026

Cisco used agentic workflows in live SOC environments at Cisco Live Americas and Black Hat USA. The workflows summarized incidents, identified supporting evidence, recommended next steps and retained reasoning for human review, while analysts remained responsible for closure, escalation and consequential actions.

Machine Speed, Human Control⁽³⁾

Cisco applied supervised agentic workflows across a live environment processing **5.6 billion logs, 202.9 billion packets and 1.74 billion sessions**. Agents accelerated incident review and recommendations, while analysts validated the underlying evidence and approved consequential actions.

KEY CYBERSECURITY FOCUS AREAS

IV. SASE DISRUPTION AND EMERGENCE OF BROWSER SECURITY

As enterprise work migrates into SaaS applications, AI tools and browser-based workflows, the browser is becoming a critical security enforcement layer.

SASE and endpoint vendors are extending controls into the browser to govern identity, data movement, AI usage and agent behavior at the point of interaction, while browser-native specialists provide visibility that network and endpoint controls often lack.

PRODUCT MOVES HIGHLIGHT SHIFT TO BROWSER-LEVEL SECURITY

Check Point Adds Browser and AI Controls to SASE



Check Point Software added browser-security controls and prompt-level DLP for native AI applications to its SASE console, demonstrating that AI governance is becoming part of unified access and browser policy.

Sept. 7th, 2026

Akamai Completes LayerX Integration Path



Akamai Technologies completed the LayerX acquisition, formally adding browser-native visibility over prompts, file uploads, web content and SaaS use to its Zero Trust strategy.

July 2nd, 2026

AI-NATIVE BROWSERS CREATE A NEW RUNTIME RISK

85% of the workday spent in the browser⁽¹⁾

Browsers are no longer passive interfaces. AI-enhanced browsers can summarize content, invoke tools, automate workflows and act on behalf of users.

Security teams therefore must protect not only the person using the browser, but also what the browser's embedded agents are permitted to do.

AI USAGE CONTROL DRIVES BROWSER ADOPTION

41% of end users interacted with at least one AI web tool⁽²⁾

The browser is where employees increasingly access public AI tools, embedded copilots and autonomous agents.

That makes browser telemetry important for governing prompts, file uploads, data sharing, AI accounts and agent actions.

KEY SASE VENDORS SHOWING INTEREST IN THE SPACE



SECURE ENTERPRISE BROWSER DISRUPTORS



ACQUIRED SPECIALISTS



KEY CYBERSECURITY FOCUS AREAS

V. AI-NATIVE SECURITY SYSTEMS SHIFT FROM CAPABILITY TO ASSURANCE

AI-native security is evolving beyond the use of frontier models to discover vulnerabilities and automate response. As model capabilities advance faster than safeguards, the market is increasingly focused on independent testing, runtime monitoring, policy enforcement and governance that can demonstrate whether models and agents are safe to deploy.

AI EXPANDS DEFENSIVE CAPABILITY

Advanced models are moving from cybersecurity copilots toward autonomous systems capable of discovering vulnerabilities, validating exploitability and supporting continuous defense.

AI CREATES A NEW ASSURANCE LAYER

The same models that strengthen cyber defense also introduce new risks. Enterprises need independent systems to test models before deployment, monitor agents at runtime, enforce behavioral boundaries and produce credible evidence that safeguards remain effective.

Models and Autonomous Agents Require a Dedicated Layer for:

- Independent safety testing
- Model and application red teaming
- Runtime monitoring
- Prompt-injection protection
- Agent identity and authorization
- Data and training-pipeline security
- Behavioral governance
- Auditability and regulatory evidence

AI-NATIVE SYSTEMS

ANTHROPIC

MYTHOS: Discovery

Uses frontier AI to analyze large codebases, uncover previously unknown vulnerabilities and validate findings by simulating exploits and mapping attack paths.



DAYBREAK: Defense

Embeds AI into development workflows to identify exploitable vulnerabilities, prioritize real-world risks, generate fixes and continuously reassess code as threats evolve.

WHY ASSURANCE IS BECOMING CRITICAL

I. Capability Is Outpacing Control

Frontier AI is advancing faster than the systems used to evaluate, monitor and govern it. As models gain greater autonomy and cyber capabilities, voluntary guardrails and pre-release testing alone may be insufficient.

II. AI Risk Persists After Release

Even a model that passes initial testing can behave differently when connected to enterprise data, tools, agents and workflows. Security therefore must extend from pre-deployment evaluation into continuous runtime assurance.

III. Enterprises Need Independent Evidence

Organizations will increasingly require evidence that models and agents have been independently tested, remain within approved boundaries and can be monitored, audited and contained after deployment.

RECENT DEVELOPMENTS



Ongoing Frontier Assessment

METR established a repeatable evaluation model covering internal frontier systems and development processes, not only public model releases.

March 2026



Verified Deployment

Workday and Cisco introduced independent agent testing with signed, standards-based records and continuous monitoring.

June 2026



Continuous Validation

Fortinet acquired Virtue AI to repeatedly test changing models and agents and enforce production guardrails.

August 2026



Independent Oversight

Anthropic committed to embedded external evaluators with ongoing access to model-development processes and safety practices.

September 2026

KEY CYBERSECURITY FOCUS AREAS

VI. BUY VS. BUILD

As emerging security categories develop faster than traditional product roadmaps, vendors are using M&A to buy time, specialized expertise, product maturity and category credibility that would be difficult to replicate organically.

BUILDING TECHNOLOGY DOES NOT EQUAL BUILDING MARKET POSITION

Internal R&D may produce comparable features, but customer penetration requires an additional investment in integrations, compliance, reference customers, threat telemetry, practitioner trust and enterprise procurement.

In security, where customers are cautious about adopting unproven controls, this commercialization period can be longer and less certain than the initial development cycle.

SCARCITY OF PROVEN CAPABILITIES

Leading cyber targets offer more than technology. They provide specialized talent, proprietary telemetry, mature integrations, customer relationships and established positions in emerging categories. Because these assets take years to develop and penetrate enterprise customers, they are difficult to recreate through internal R&D.

This **scarcity creates a premium** based on two sources of value:

- **Capability acquisition:** Immediate access to a proven product, team, customers and market position.
- **Competitive denial:** Prevention of a rival from acquiring or deeply integrating the same capability.

The effect is amplified in **agentic AI security**, where relatively few independent vendors have mature solutions. Vendors that wait to build risk arriving late and finding that category-leading assets have already been absorbed by competing platforms.

RECENT TRANSACTIONS ILLUSTRATING BUY VS. BUILD

Cyera acquired Oasis Security For \$1.0B

September 2026

STRATEGIC RATIONALE:

Cyera acquired a proven non-human identity platform rather than building identity discovery, governance and access controls internally. Oasis immediately expands Cyera from data security into governing the human, machine and AI identities that access sensitive data.



Cribl acquired Radiant Security technology assets for an undisclosed amount

August 2026

STRATEGIC RATIONALE:

Cribl acquired Radiant's AI-native SOC technology rather than developing autonomous triage and investigation capabilities internally. The deal moves Cribl beyond telemetry management into Agentic SOC, enabling AI-driven investigations directly across distributed security data.



Fortinet acquired Virtue AI for an undisclosed amount

August 2026

STRATEGIC RATIONALE:

Fortinet acquired purpose-built AI-security capabilities rather than developing them through a longer internal roadmap. Virtue AI immediately adds agent red teaming, continuous validation, runtime protection, governance and real-time guardrails across the AI lifecycle.



Okta acquired Permiso Security for ~\$200M⁽¹⁾

July 2026

STRATEGIC RATIONALE:

Okta acquired Permiso rather than building advanced identity threat detection internally. The deal extends Okta beyond authentication into continuous monitoring and response across human, machine and AI-agent identities, strengthening its position in post-authentication security.

SECTION III.

PRIVATE MARKET ACTIVITY



CYBERSECURITY MARKET UPDATE

OCTOBER 2026



SELECT CYBERSECURITY INVESTORS



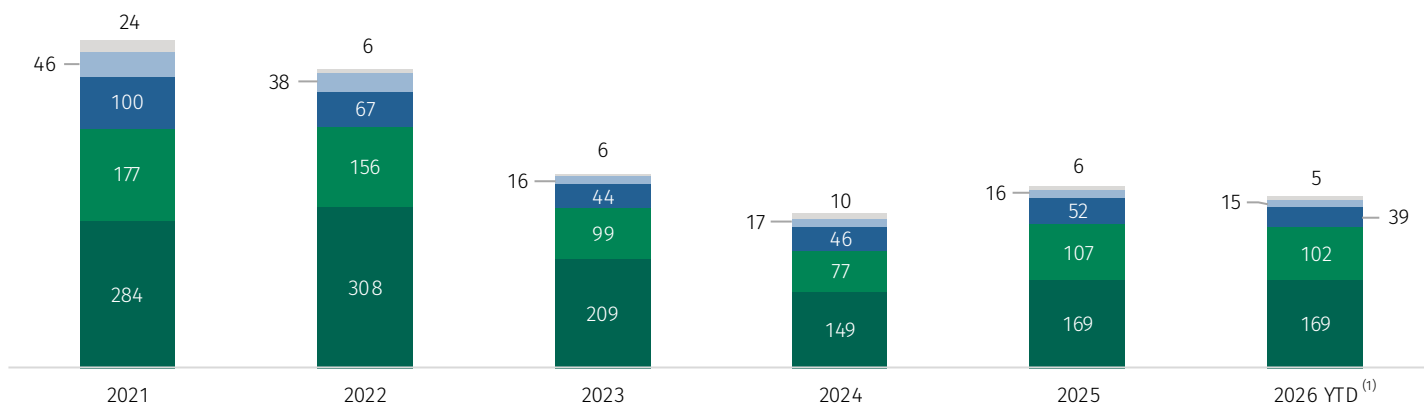
OCTOBER 2026

FINANCING ACTIVITY

HISTORICAL INVESTMENT ACTIVITY BY SERIES

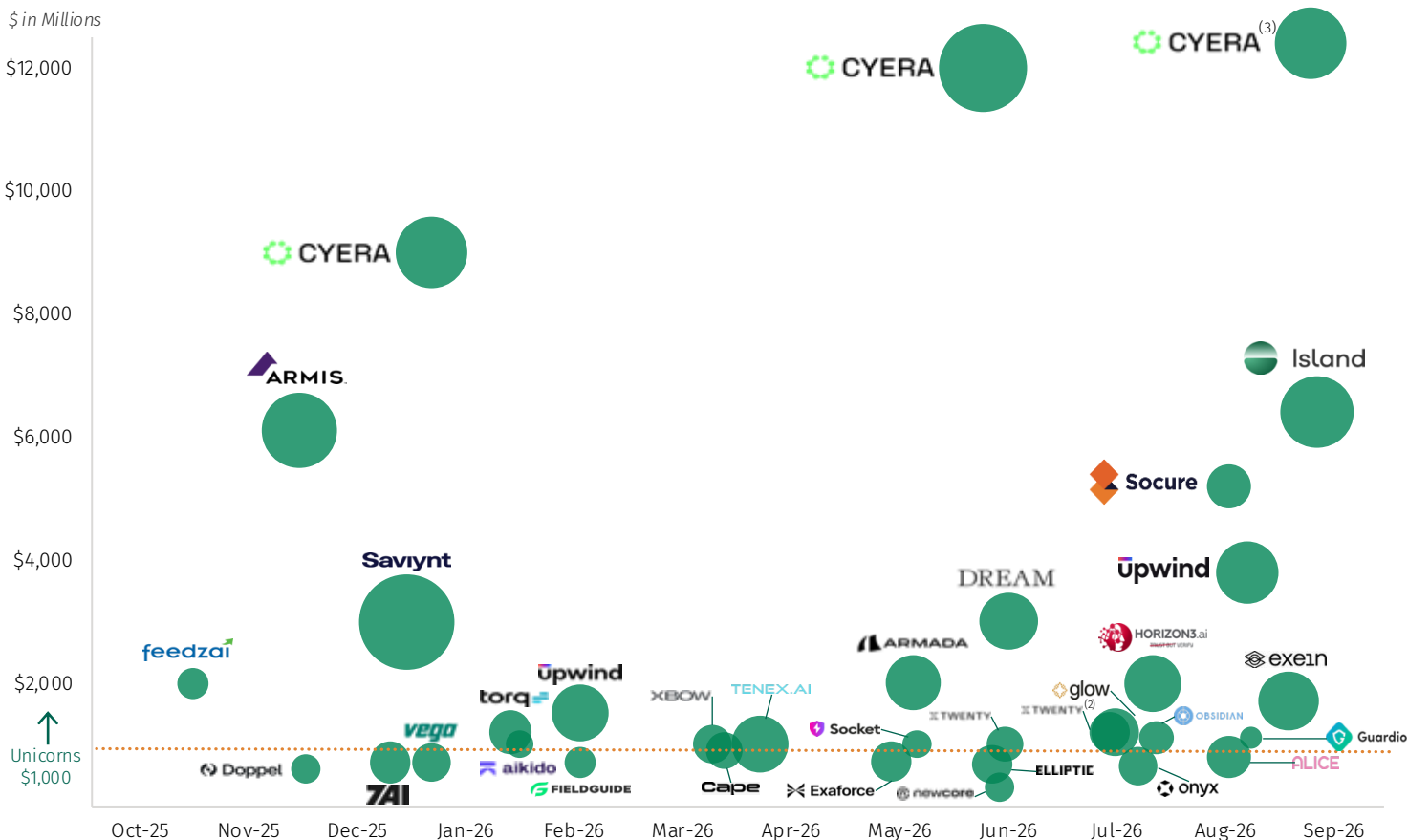
Figures Denote Deal Count

Seed Series A Series B Series C Series D



2026 deal count is on track to exceed activity for the past three years.

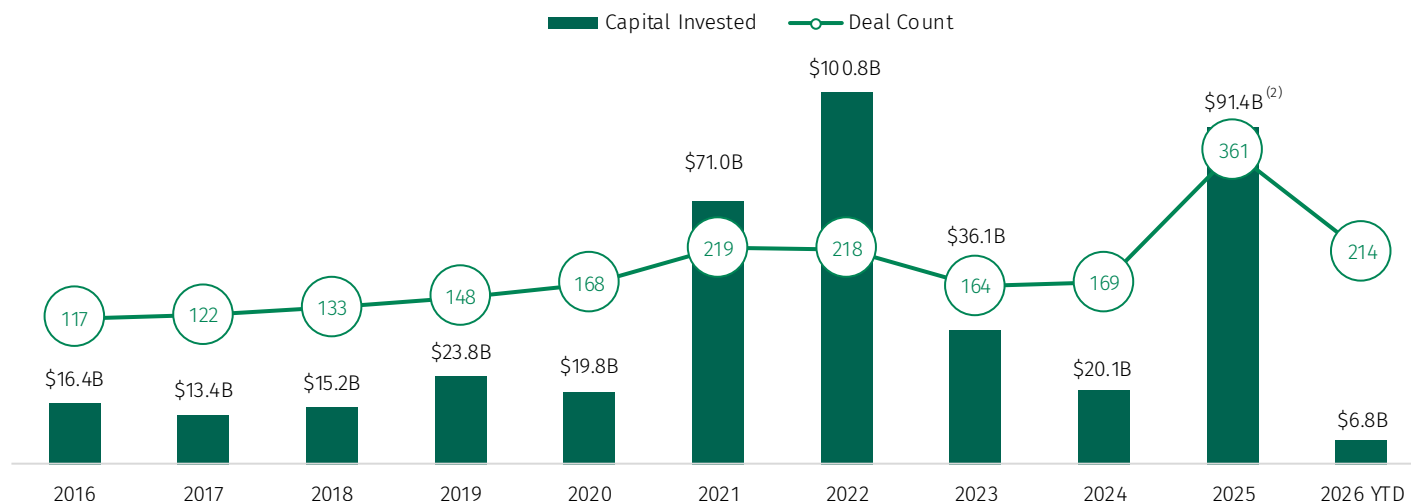
SELECT CYBERSECURITY FINANCINGS



Source(s): Pitchbook, Company press releases. Only displays financing rounds over \$30m. Bubble size represents funding size

(1) YTD as of 09/30/26 (2) Twenty Raise in Extension of Previous Round (3) Cyera Series G Extension from previous round

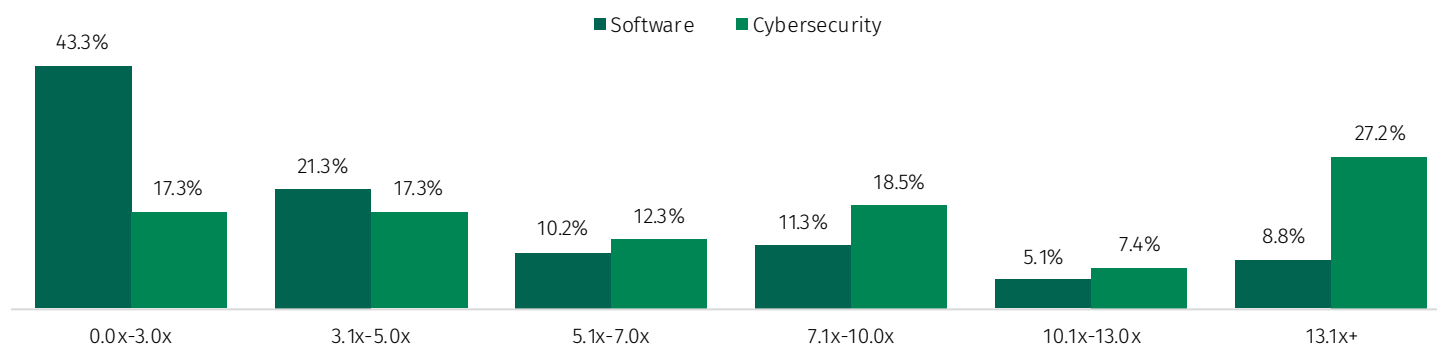
M&A ACTIVITY

CYBERSECURITY M&A SUMMARY⁽¹⁾

Cybersecurity M&A remains strong after a record 2025, with 214 deals YTD, putting 2026 on pace to be the second most active year since 2016.

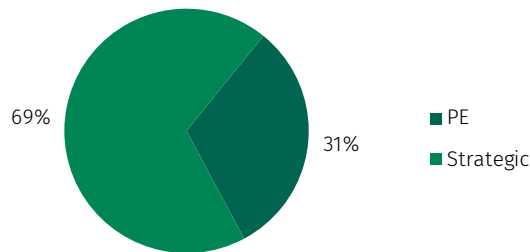
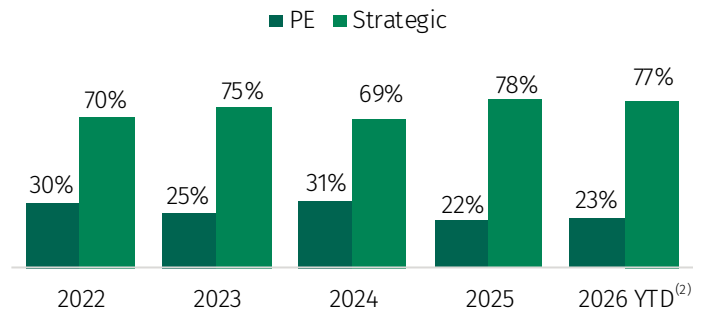
SOFTWARE & CYBERSECURITY M&A MULTIPLES⁽¹⁾

MEDIAN MULTIPLE (EV/LTM REV)		
YEAR	SOFTWARE	CYBERSECURITY
2026 YTD ⁽³⁾	3.0x	7.1x
2025	4.0x	10.0x
2024	2.9x	6.3x
2023	3.1x	5.9x
2022	4.8x	8.9x



OCTOBER 2026

DEAL ACTIVITY

Q3 CYBERSECURITY M&A ACTIVITY BY BUYER⁽¹⁾HISTORICAL CYBERSECURITY M&A ACTIVITY BY BUYER⁽¹⁾SELECT BUYERS OF CYBERSECURITY: STRATEGIC⁽³⁾

BUYER	SELECT ACQUISITIONS			
CHECK POINT	CYCLOPS Feb-26	LAKERA Nov-25	VERITI Jun-25	Cyberint Sep-24
CROWDSTRIKE	sgnl Feb-26	seraphic Jan-26	pangea Sep-25	unit4 Nov-24
FORTINET	VirtueAI Aug-26	suridata May-25	PERCEPTION POINT Dec-24	next Aug-24
okta	PERMISO Aug-26	AXIOM Sep-25	Spera Feb-24	veeva Oct-23

BUYER	SELECT ACQUISITIONS			
paloalto	KOI Feb-26	CYBERARK Feb-26	PROTECT AI Apr-25	TALON Dec-23
SailPoint	entro Jun-26	SAVVY Sep-25	Imprivata Dec-24	Q3 Double Zero Aug-24
servicenow	ARMIS Dec-25	veza Dec-25	MIBISU Capiv Nov-24	Atrinet Feb-24
zscaler	SYMMETRY May-26	SquareX Feb-26	splix Oct-25	red canary Aug-25

SELECT BUYERS OF CYBERSECURITY: PE⁽²⁾

BUYER	SELECT PORTFOLIO COMPANIES			
IEQT	Acronis Aug-24	SK shieldus Jul-23		
FP FRANCISCO PARTNERS	efficient IP Jun-26	jamf Jan-26	PROMO2 Dec-25	BLACKDUCK Sep-24
PERMIRA	EXCLUSIVE NETWORKS Jul-24	BioCatch May-24	mimecast May-22	
TA ASSOCIATES	EGNITE Feb-25	FORTRA Sep-23	VERACODE Mar-22	

BUYER	SELECT PORTFOLIO COMPANIES			
THOMABRAVO	DARKTRACE Oct-24	Pingidentity Aug-22	SailPoint Aug-22	proofpoint Aug-21
TPG	SAYARI Jan-24	Delinea Feb-21	Cerity Jan-21	
TURN // RIVER	solarwinds Apr-25	tufin Aug-22	Invicti Nov-21	
VISTA	KnowBe4 Feb-23	CRITICALSTART Mar-22	sonatype Nov-19	RadarFirst Nov-19

SELECT INVESTORS OF CYBERSECURITY: CYBER-FOCUSED VC⁽⁴⁾

INVESTOR	SELECT PORTFOLIO COMPANIES			
BALLISTIC VENTURES	oligo Aug-26	MANDIANT Jun-26	Above Mar-26	native Mar-26
CYBERSTARTS	Island Sep-26	upwind Sep-26	onyx Jul-26	glow Jul-26
evo/ution EQUITY PARTNERS	Island Sep-26	CYERA Sep-26	Outerlimit Sep-26	QIZ Jul-26
FORGEPOINT	hackuity Sep-26	DATABAHN Jul-26	DISCERN SECURITY Jul-26	RAPIDPORT Feb-26

INVESTOR	SELECT PORTFOLIO COMPANIES			
GLILOT CAPITAL PARTNERS	Bloom Jul-26	MAY Jul-26	JAZZ Mar-26	sweet. Nov-25
SYN VENTURES	BalanceTheory Sep-26	Bloom Jul-26	Arcade Jun-26	nullify Feb-26
TENEELEVEN	Rig Sep-26	HIDEHLAYER Sep-26	Bloom Jul-26	Geordie May-26
VL VENTURES	B2B2B Sep-26	HushSecurity Jul-26	native Mar-26	opti Nov-25

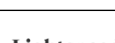
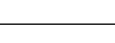
OCTOBER 2026

RECENT DEAL ACTIVITY⁽¹⁾

Q3 2026 – SELECT M&A TRANSACTIONS

DATE ANNOUNCED	TARGET	ACQUIROR	TARGET DESCRIPTION	EV (\$M)
9/24/2026	 empowerID	 Omada	Provides AI agent identity governance software for businesses globally	ND
9/16/2026	 Ontinue	 Quorum Cyber	Provides agentic managed extended detection and response (MXDR) software and managed cybersecurity services for businesses in the US	ND
9/16/2026	 AVERTIUM	 CyberMaxx	Provides Microsoft-partnered managed cybersecurity services for businesses in the US	ND
8/27/2026	 FRAVITY	 Socure	Provides agentic fraud, risk and compliance management software for businesses globally	ND
8/17/2026	 VirtueAI	 FORTINET	Provides AI security and governance software for businesses in the US	ND
8/3/2026	 BioCatch	 VISA	Provides AI-based behavioral biometrics fraud prevention software, related APIs and SDKs for financial institutions and telecommunication brands globally	\$2,400
7/30/2026	 PERMISO	 okta	Provides cloud-native identity security management software for businesses in the US	\$200
7/28/2026	 OASIS	 CYERA	Provides non-human and agentic AI identity and access management and data security software for businesses globally	\$1,000
7/1/2026	 sam seamless network	 Qualcomm	Developer of network-based security software designed to tackle cybersecurity threats at the source	\$150

Q3 2026 – SELECT CAPITAL RAISES

DATE ANNOUNCED	COMPANY	LEAD INVESTOR(S)	DEAL SIZE (\$M)	POST-VALUATION (\$M)	COMPANY DESCRIPTION
9/24/2026	 Island	 evo/ution EQUITY PARTNERS	\$400	\$6,400	Developer of an enterprise browser designed to allow work to flow freely while remaining fundamentally secure
9/22/2026 ⁽²⁾	 CYERA	 Goldman Sachs Growth Equity	\$400	\$12,400	Developer of an AI-powered data-security platform designed to discover, classify and protect sensitive enterprise data
9/15/2026	 exe1n	 Headline	\$270	\$1,700	Developer of a cybersecurity platform designed to protect any device locally, respecting the privacy and security of the device's data
9/8/2026	 CYLAKE	 Lightspeed	\$245	ND	Developer of an AI-native cybersecurity platform intended to provide data-sovereign security architecture for highly regulated organizations
9/2/2026	 Upwind	 Bessemer Venture Partners  TCV	\$300	\$3,800	Developer of a runtime-powered cloud and AI security platform designed to identify, prioritize and remediate risks across cloud infrastructure
9/2/2026	 HIDDENLAYER	 delta-v	\$100	ND	Developer of cybersecurity software designed to protect the machine learning algorithms, models and the data that power them
8/31/2026	 Saviynt	 CARRICK Investing in New Capital	\$255	ND	Developer of cloud security and identity governance software designed to help enterprises scale cloud initiatives and solve security and compliance challenges
8/27/2026	 Socure	 SUMMIT PARTNERS	\$156	\$5,200	Developer of a digital identity verification platform designed to support compliance and fraud prevention
8/27/2026	 ALICE	 Apax DIGITAL GROWTH	\$140	\$800	Developer of an internet security tool designed to collect, analyze and contextualize data to provide maximum protection
8/3/2026	 HORIZON3.ai AI-Driven Cyber	 NEA  NIGHTDRAGON	\$250	\$2,000	Developer of a security automation platform designed to perform autonomous penetration testing and operational security assessments
7/20/2026	 TWENTY	 khosla ventures	\$130	\$1,200	Developer of a cyber-warfighting platform designed to enable real-time offensive cyber operations for defense missions

Source(s): Company press releases; CapIQ, 451 Research, PitchBook, SecurityWeek, Telecom.com

(1) Deal amounts are based on publicly disclosed figures (2) Cyera Series G Extension

SECTION IV.

PUBLIC MARKET ACTIVITY



PUBLIC CYBER EARNINGS INSIGHTS

CYBERSECURITY EMERGES AS A KEY AI INVESTMENT THEME

AI-DRIVEN MARKET CATALYSTS:

Rapid adoption of generative and agentic AI is expanding the number of identities, applications, data flows and autonomous actions enterprises must secure, while also enabling faster vulnerability discovery, social engineering and attack execution.

This structural demand has become increasingly visible through high-profile developments, including the OpenAI-Hugging Face incident and calls from Anthropic leadership for stronger safeguards, independent evaluations and greater coordination around AI systems.

These events are examples of a broader shift in which AI security, governance and cyber resilience are becoming essential requirements for enterprise adoption.

MARKET RESPONSE:

The publicity around AI-related risk has focused investor attention on cybersecurity as a key derivative of the AI investment cycle. Strong earnings, raised guidance, recurring-revenue momentum and expanding adoption of security products have provided fundamental support, with the strongest gains accruing to scaled platforms demonstrating measurable execution and credible AI-security exposure.

EARNINGS HIGHLIGHTS

	 CLOUDFLARE	 CROWDSTRIKE	 FORTINET	 okta	 paloalto [®] NETWORKS	 rubrik
Share Price Growth YTD ⁽¹⁾	76%	126%	125%	142%	116%	114%
Reported Revenue Growth	36%	26%	26%	11%	34%	38%

Across the group, the recurring themes are platform adoption, AI-agent security, identity governance and machine-to-machine traffic. Although AI is expanding the overall cybersecurity opportunity, vendors with slower growth, narrower portfolios, acquisition-supported results or go-to-market disruption remain “show-me” stories despite credible long-term positioning.



Agentic Internet Infrastructure

Positioning its global network as the infrastructure and security layer for the “Agentic Internet,” supporting growing machine-to-machine traffic, AI agents and automated commerce.



Platform Expansion:

Using Falcon Flex to accelerate multi-product platform adoption while expanding beyond endpoint security into cloud, identity, data protection, agentic security and SecOps.



Networking-Security Convergence

Driving the convergence of networking and security through its integrated SASE Firewall strategy while broadening into AI-enabled SOC, endpoint and data-security capabilities.



Agentic Identity Security

Expanding identity from human authentication into a broader control layer that discovers, secures and governs human, machine and AI-agent identities.



Consolidating AI Security

Advancing its platformization strategy by integrating network, AI, identity, cloud and security-operations capabilities into a consolidated enterprise security platform.



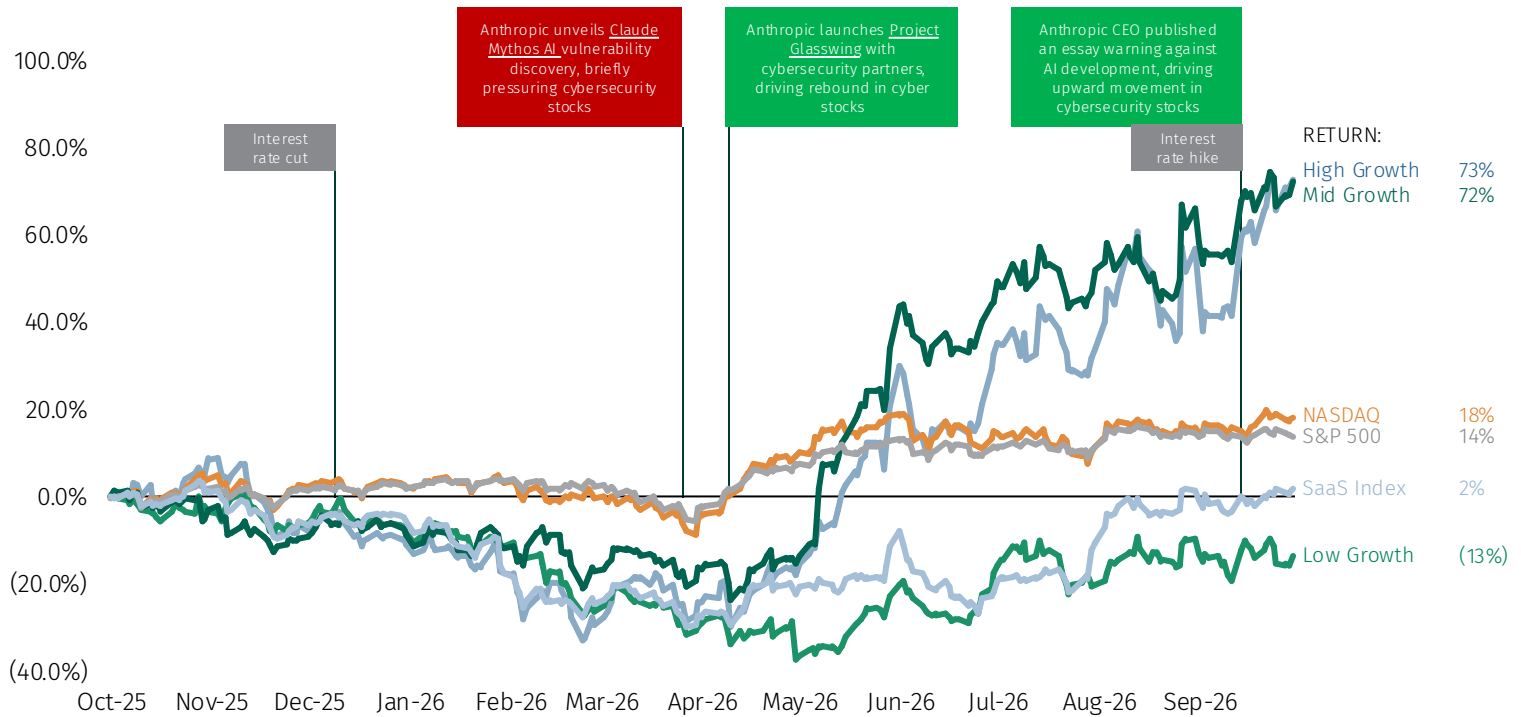
AI-Driven Resilience

Evolving from data protection and recovery toward Agentic Cyber Resilience, combining machine-speed cyber recovery with runtime protection for autonomous AI agents.

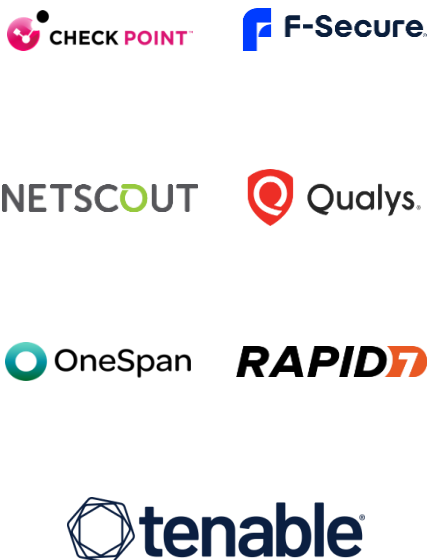
OCTOBER 2026

PUBLIC COMPANY ANALYSIS

High-growth cybersecurity companies materially outperformed broader market benchmarks, reflecting continued investor preference for scalable security platforms with strong growth and AI exposure.



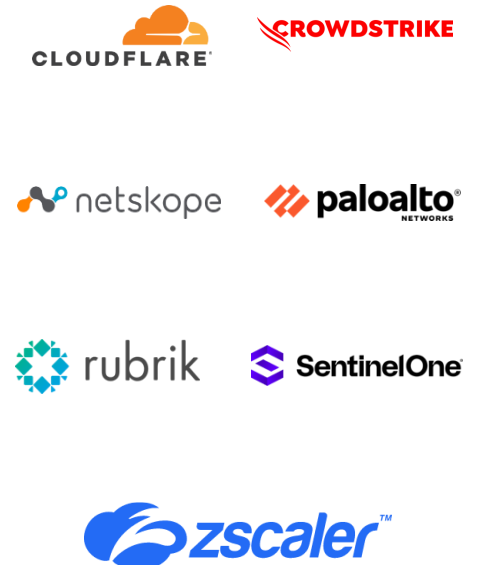
LOW GROWTH (<10%)



MID GROWTH (10-20%)



HIGH GROWTH (>20%)



OCTOBER 2026

PUBLIC COMPANY ANALYSIS

(\$ in millions; except share price)

COMPANY INFORMATION		CURRENT MARKET DATA			VALUATION METRICS				OPERATIONAL METRICS					
NAME	SYMBOL	SHARE PRICE 9/30/2026	MARKET VALUE	ENTERPRISE VALUE	EV / REVENUE		EV / EBITDA		REVENUE GROWTH		GROSS MARGIN %		EBITDA MARGIN %	
					CY26E	CY27E	CY26E	CY27E	'25-'26E	'26E-'27E	CY26E	CY27E	CY26E	CY27E
 CLOUDFLARE	NET	\$347.28	\$127,695	\$127,062	44.7x	34.4x	nm	nm	32%	29%	73%	73%	24%	26%
 CROWDSTRIKE	CRWD	\$264.75	\$272,569	\$268,413	44.2x	36.5x	nm	nm	25%	23%	79%	79%	31%	32%
 paloalto	PANW	\$397.31	\$326,603	\$326,099	24.8x	21.5x	74.5x	61.2x	33%	15%	76%	75%	33%	35%
 FORTINET	FTNT	\$178.76	\$131,909	\$128,401	15.8x	14.2x	41.7x	36.4x	19%	11%	80%	80%	38%	39%
 rubrik	RBRK	\$114.47	\$24,478	\$23,880	14.1x	11.6x	nm	nm	28%	21%	81%	81%	6%	7%
 SailPoint	SAIL	\$20.36	\$11,624	\$11,345	10.7x	7.5x	45.2x	35.7x	19%	19%	78%	78%	20%	21%
 Qualys	QLYS	\$187.20	\$6,560	\$6,187	8.9x	7.8x	18.5x	17.1x	10%	8%	85%	84%	46%	46%
 zscaler	ZS	\$199.42	\$32,516	\$30,910	8.5x	7.3x	30.3x	25.3x	21%	16%	80%	80%	28%	29%
 netskope	NTSK	\$17.44	\$7,685	\$7,350	8.4x	6.8x	nm	nm	26%	21%	77%	79%	(5%)	5%
 okta	OKTA	\$209.11	\$36,669	\$34,423	8.3x	9.7x	39.6x	34.9x	10%	10%	82%	82%	27%	28%
 VARONIS	VRNS	\$47.45	\$5,450	\$5,280	7.2x	6.0x	nm	63.6x	18%	19%	78%	78%	4%	9%
 SentinelOne	S	\$23.76	\$8,413	\$7,758	6.4x	5.5x	49.1x	33.5x	20%	18%	77%	78%	13%	16%
 CHECK POINT	CHKP	\$128.35	\$13,105	\$12,800	5.9x	5.5x	11.9x	12.1x	5%	8%	87%	88%	50%	46%
 A10	ATEN	\$27.11	\$2,011	\$1,880	5.7x	5.1x	18.6x	16.4x	13%	12%	80%	80%	31%	31%
 Gen	GEN	\$22.02	\$13,181	\$20,824	3.9x	3.6x	7.8x	7.3x	12%	8%	84%	82%	50%	50%
 tenable	TENB	\$36.39	\$4,033	\$4,157	3.9x	3.6x	14.9x	13.5x	8%	7%	82%	82%	26%	27%
 radware	RDWR	\$29.81	\$1,264	\$1,073	3.2x	3.0x	na	na	10%	8%	82%	82%	na	na
 F-Secure	FSECURE	\$1.75	\$306	\$469	2.6x	2.6x	8.5x	7.8x	4%	3%	83%	83%	31%	33%
 NETSCOUT	NTCT	\$40.18	\$2,921	\$2,332	2.6x	2.5x	9.4x	8.9x	3.5%	4%	81%	81%	28%	28%
 OneSpan	OSPN	\$17.91	\$660	\$629	2.5x	2.5x	9.1x	8.8x	2.9%	2%	73%	73%	28%	28%
 RAPID7	RPD	\$12.22	\$824	\$1,083	1.3x	1.3x	6.8x	6.4x	(2.4%)	(1%)	72%	72%	19%	20%
MEAN					11.1x	9.5x	25.7x	24.3x	\$2,615	\$2,994	15%	12%	80%	80%
MEDIAN					7.2x	6.0x	18.5x	16.7x	\$1,205	\$1,420	13%	11%	80%	80%

OCTOBER 2026

PUBLIC COMPANY ANALYSIS

EV/26E REVENUE TO RULE OF 40⁽¹⁾

BELOW "RULE OF 40"

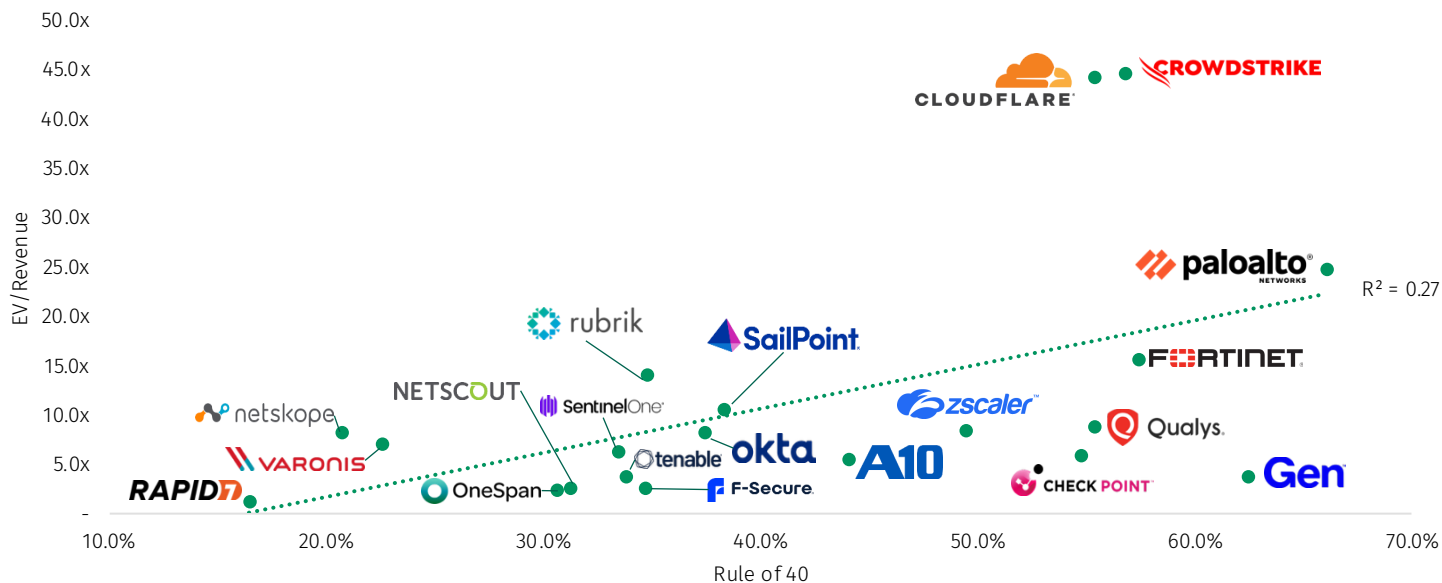
Mean: 30.4% | 6.2x

Median: 33.5% | 6.4x

ABOVE "RULE OF 40"

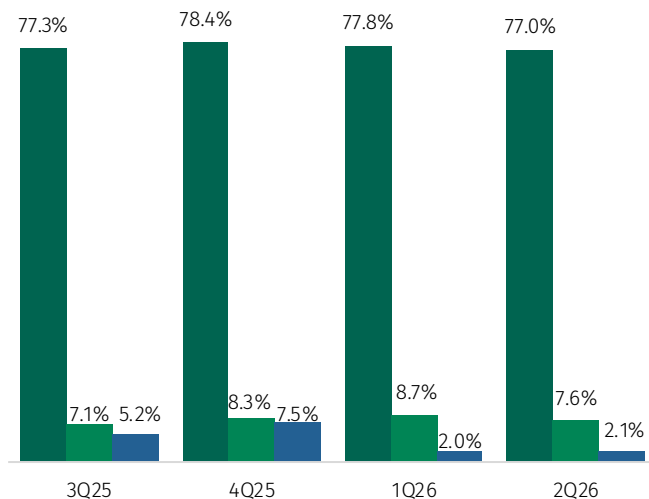
Mean: 55.8% | 18.1x

Median: 55.4% | 8.9x

OPERATING METRICS⁽²⁾

MEDIAN MARGIN PERFORMANCE – QUARTERLY

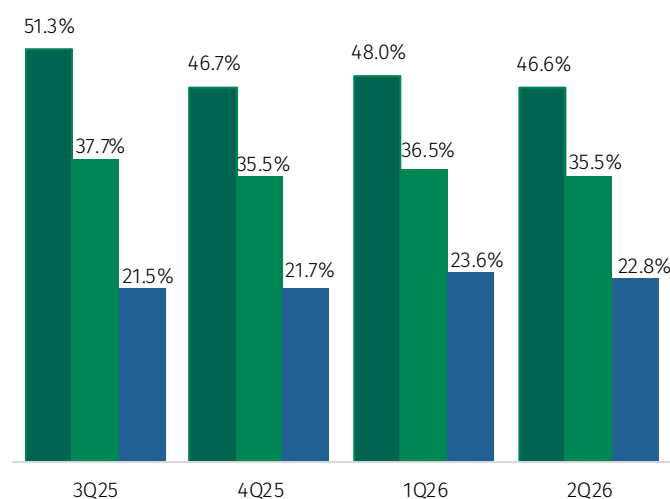
■ Gross Profit Margin ■ EBITDA Margin ■ Net Income Margin



MEDIAN OPERATING RATIOS – QUARTERLY

As % of Revenue

■ SG&A ■ S&M ■ R&D



SECTION V.

MARKET MAP



DL-JMP-CybersecurityTeam@citizensbank.com

Private Cybersecurity

For more information, contact:

DL-JMP-CybersecurityTeam@citizensbank.com

Private Cybersecurity

For more information, contact:

DL-JMP-CybersecurityTeam@citizensbank.com

SECTION VI.

CITIZENS OVERVIEW



CITIZENS CYBERSECURITY PRACTICE

COMPREHENSIVE RESEARCH AND BANKING COVERAGE ACROSS THE FIRM

INVESTMENT BANKING



DOUG BROCKWAY

Managing Director,
Head of Cybersecurity & Infrastructure Investment Banking
35+ Years of Experience



SALIL KAPOOR

Vice President,
Cybersecurity and Infrastructure Software Investment Banking
7+ Years of Experience

EQUITY RESEARCH



RUSTAM KANGA

Vice President,
Cybersecurity and IT Infrastructure Equity Research



TREVOR WALSH

Director,
Head of Aerospace & Defense

RELEVANT CITIZENS ADVISORY STATS

20+ years

Average Sector
Experience Across
Senior Bankers

\$40B+

Technology
Assignments since
Inception

600+

Technology
Strategic Advisory
Roles

RELEVANT COVERAGE UNIVERSE

ESTABLISHED TRACK RECORD OF M&A TRANSACTIONS⁽¹⁾

 Formal Verification Software Platform Pending Financial Advisor	 AI-Native MDR Platform Pending Financial Advisor	 A portfolio company of Has sold ALERT LOGIC to LevelBlue Sell-Side Advis or	 Has been acquired by SUNSTONE Sell-Side Advis or	 A portfolio company of Has been acquired by THRIVE Sell-Side Advis or	 Has sold certain commercial assets to DARKOWL A portfolio company of Five Elms Capital Sell-Side Advis or	 A portfolio company of Has been acquired by Kiteworks A portfolio company of BPEA Sell-Side Advis or	 Has been acquired by Dropbox Sell-Side Advis or	 Has been acquired by HUMAN Financial Advisor
 Has been acquired by POINTSHARP A portfolio company of MAIN Sell-Side Advis or	 Has been acquired by PERISCOPE Sell-Side Advis or	 Has been acquired by Pingidentity Sell-Side Advis or	 A portfolio company of Has been acquired by Deloitte Sell-Side Advis or	 Has been acquired by FORTRA Sell-Side Advis or	 Has been acquired by sumo logic Sell-Side Advis or	 Has been acquired by Avira NortonLifeLock Sell-Side Advis or	 Has been acquired by FORTINET Sell-Side Advis or	 Has been acquired by exterro Sell-Side Advis or
 Has been acquired by cisco Sell-Side Advis or	 Has been acquired by BROADCOM Sell-Side Advis or	 Has been acquired by hp Sell-Side Advis or	 Has been acquired by FORESCOUT Sell-Side Advis or	 A portfolio company of Has been acquired by import.io Sell-Side Advis or	 Has been acquired by eSENTIRE Sell-Side Advis or	 Has been acquired by ENTRUST Buy-Side Advis or	 Has been acquired by CYBERARK Sell-Side Advis or	 A portfolio company of Has been acquired by ORACLE Sell-Side Advis or

ESTABLISHED TRACK RECORD OF ECM & DCM TRANSACTIONS⁽²⁾

 \$908,200,000 Initial Public Offering Active Bookrunner	 \$1,293,750,000 Convertible Senior Notes Co-Manager	 \$517,499,970 Follow-On Offering Co-Manager	 \$650,000,000 Convertible Senior Notes Co-Manager	 \$575,000,000 Convertible Senior Notes Co-Manager	 \$745,200,000 Initial Public Offering Co-Manager	 \$603,750,000 Initial Public Offering Co-Manager	 \$703,800,000 Initial Public Offering Co-Manager	 \$375,000,000 Initial Public Offering Co-Manager
 \$192,000,000 Initial Public Offering Co-Manager	 \$215,050,000 Initial Public Offering Co-Manager	 \$86,000,000 Initial Public Offering Co-Manager	 \$2450,000,000 Senior Credit Facility Joint Lead Arranger, Joint Bookrunner and Co-Syndication Agent	 Has raised Equity & Debt Financing Morgan Stanley TRINITY CAPITAL Sell-Side Advis or	 \$800,000,000 Senior Credit Facility Joint Lead Arranger, Joint Bookrunner and Co-Syndication Agent	 \$425,000,000 Senior Credit Facility Joint Lead Arranger and Co-Syndication Agent	 \$1,500,000,000 Senior Unsecured Notes Co-Manager	 A portfolio company of \$1,085,000,000 Senior Credit Facilities Joint Lead Arranger and Joint Bookrunner

Source(s):

(1) Includes deals completed by current team members at prior firms (2)

ECM Deals

DCM Deals

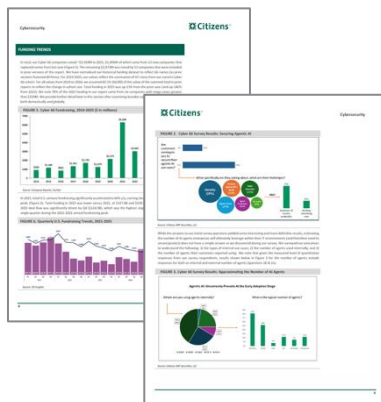
CITIZENS CYBERSECURITY PRACTICE

2026 CYBER 66 PUBLICATION

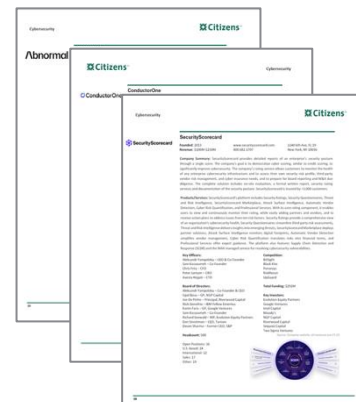
The Citizens Cyber 66 is an annual research report identifying the 66 most strategically important private cybersecurity companies shaping the future of the security market.

What's included

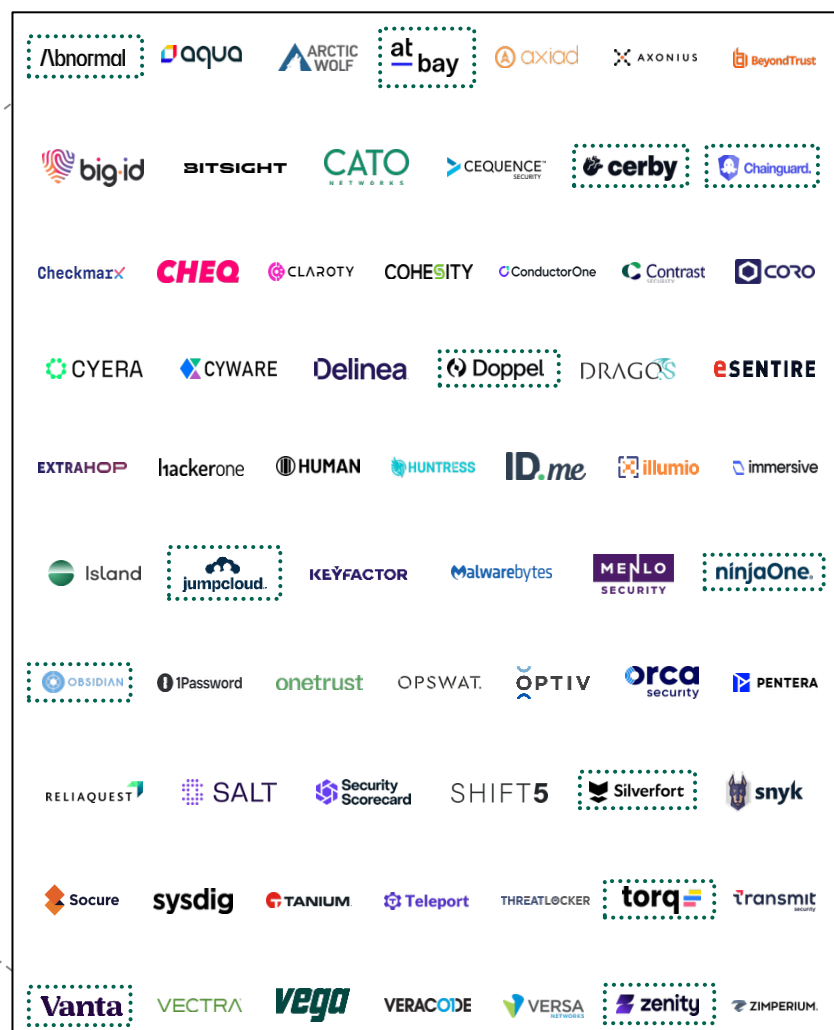
Market and Financial Trends from Surveyed Cyber Professionals



One-Page Profiles Covering Relevant Company and Investor Information



Citizens 2026 Cyber 66 Report link:
<https://app.box.com/s/eu1jv4skp1t55c31i0kv5fq9h4mxsdip>



Denotes Additions from the 2025 Edition

CITIZENS TECH CONFERENCE

CITIZENS 2027 TECHNOLOGY CONFERENCE



The Citizens Technology Conference returns to San Francisco, bringing together leading public and private technology companies with institutional investors through company presentations, executive discussions and one-on-one meetings.

DATES: MARCH 8-9, 2027

San Francisco, CA

CITIZENS 2026 TECHNOLOGY CONFERENCE RECAP

CONFERENCE OVERVIEW

66

Public Participating Companies

52

Private Participating Companies

1,153

Investor Meetings Held

NOTABLE ATTENDEES













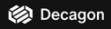






































































Denotes Cybersecurity Company

KEY CYBERSECURITY TAKEAWAYS

I. Identity Remains a Focal Point

"Identity is the perimeter, there's a lot of marketing around that, but it's really true. The form of the worker, whether human or non-human, is the atomic unit of where the badness begins." – Greg Keller, CTO of JumpCloud.

II. The Identity Stack is Consolidating

Recent M&A highlights consolidation across PAM, IGA and adjacent controls, while a clear divide is emerging between identity infrastructure providers and identity security platforms focused on monitoring and enforcement.

III. AI is an Accelerant, Not a Disruptor

Frontier AI labs are unlikely to displace incumbent cybersecurity vendors; instead, AI is viewed as a table-stakes capability that accelerates product velocity, supports margin expansion and increases demand for cybersecurity solutions.

IV. Enterprise AI Expands the Security Market

As with cloud security, enterprise AI is creating new security categories and spend, with monetization accruing disproportionately to a subset of scaled platform vendors rather than evenly across the market.

Source(s): Citizens Research

28

2026-2027 SELECT CYBER CONFERENCE SCHEDULE

ISC2 Security Congress



The ISC2 Security Congress brings together cybersecurity practitioners and leaders for technical sessions, strategic programming and hands-on workshops covering AI security, Zero Trust, identity-first security, governance, risk and emerging threats.

DATES: OCT 24–28, 2026

Aurora, CO

Forrester Security & Risk Forum



This forum aims to provide security, risk and privacy leaders with actionable insights, frameworks and peer collaboration to help protect the enterprise and translate strategy into execution.

DATES: NOV 9-10, 2026

Washington, DC

Aspen Cyber Summit



The Aspen Cyber Summit brings together leaders from government, industry and civil society to address evolving cyber threats and drive actionable, cross-sector solutions.

DATES: NOV 18, 2026

Washington, DC

AWS re:Invent



AWS re:Invent provides an inside look into the cutting edge of cloud technology. By hearing from experts at the forefront of the field, attendees can learn where the industry is going and what security challenges come with that direction.

DATES: NOV 30-DEC 4, 2026

Las Vegas, NV

Gartner IAM Summit



The Gartner Identity & Access Management Summit brings together IAM and cybersecurity leaders to address identity governance, privileged access, machine and AI-agent identities, continuous authorization and identity's expanding role as the control plane for enterprise security.

DATES: DEC 7-9, 2026

Las Vegas, NV

SANS Cyber Threat Intelligence Summit



The SANS Cyber Threat Intelligence Summit brings together threat-intelligence professionals for technical sessions, hands-on workshops and real-world case studies focused on adversary analysis, investigative tools and actionable intelligence.

DATES: FEB 1–2, 2027

Alexandria, VA

RSAC Conference



The RSAC Conference 2027 brings together cybersecurity practitioners, technology providers, investors, researchers and policymakers to explore developments across AI, digital trust, security strategy and emerging cyber technologies.

DATES: APR 5-8, 2027

San Francisco, CA

IEEE Symposium on Security and Privacy



The IEEE Symposium on Security and Privacy 2027 is a leading academic conference featuring peer-reviewed research across cybersecurity, privacy, cryptography, software security and emerging threats to AI and machine-learning systems.

DATES: MAY 17-20, 2027

Montreal, Canada

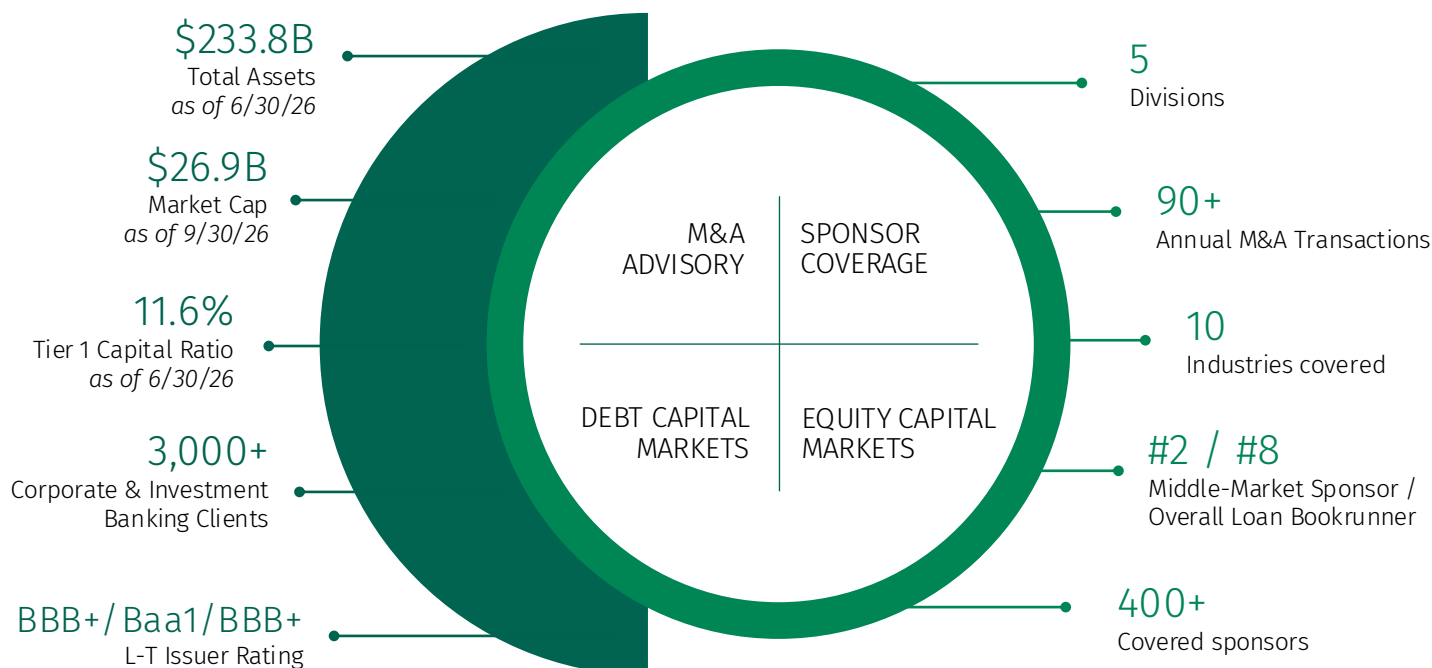
CITIZENS OVERVIEW

CITIZENS FINANCIAL GROUP⁽¹⁾

Citizens is one of the oldest and largest financial institutions in the U.S. and currently ranked the 16th largest bank.

CAPITAL MARKETS & ADVISORY⁽²⁾

Capital Markets & Advisory is a fast-growing, full-service investment banking platform that provides capital market access, M&A services and valuation advisory.



For more information, reach out to:
DL-JMP-CybersecurityTeam@CitizensBank.com

CITIZENS TECHNOLOGY TEAM AND PRODUCT PARTNERS

STRATEGIC ADVISORY

GAVIN SLADER

Head of Strategic Advisory
gavin.slader@citizensbank.com

INVESTMENT BANKING

KEVIN MCCLELLAND

Head of Technology Investment Banking
kevin.mcclelland@citizensbank.com

INVESTMENT BANKING

DOUG BROCKWAY

Head of Cybersecurity and Infrastructure
Software Investment Banking
douglas.brockway@citizensbank.com

INVESTMENT BANKING

SALIL KAPOOR

Cybersecurity and Infrastructure Software
Investment Banking
salil.kapoor@citizensbank.com

EQUITY CAPITAL MARKETS

ANDREW MERTZ

Head of Equity Capital Markets
andrew.mertz@citizensbank.com

EQUITY CAPITAL MARKETS

GIANPAOLO ARPAIA

Head of Equity-Linked Capital Markets
gianpaolo.arpaia@citizensbank.com

DEBT CAPITAL MARKETS

TAD BENDER

Managing Director
charles.bender@citizensbank.com

CORPORATE BANKING

ANDREW KIRBY

Managing Director, Technology Coverage
andrew.kirby@citizensbank.com

FINANCIAL SPONSORS

SAM SHAW

Head of Financial Sponsor Coverage
samuelg.shaw@citizensbank.com

©2026 Citizens Financial Group, Inc. "Citizens" is the marketing name for the business of Citizens Financial Group, Inc. ("CFG") and its subsidiaries. "Citizens Capital Markets & Advisory" is the marketing name for the investment banking research, sales and trading activities of our institutional broker-dealer, Citizens JMP Securities, LLC ("CJMPS"), Member [FINRA](#) and [SIPC](#) (See [FINRA BrokerCheck](#) and [SIPC.org](#)). Securities products and services are offered to institutional clients through CJMPS. ([CJMPS disclosures](#) and [CIMP Form CRS](#)). Banking products and services are offered through Citizens Bank, N.A., Member FDIC.

Securities and investment products are subject to risk, including principal amount invested and are: NOT FDIC INSURED · NOT BANK GUARANTEED · MAY LOSE VALUE