



MERIDIAN CAPITAL

Cybersecurity Market Update

Q3 2026

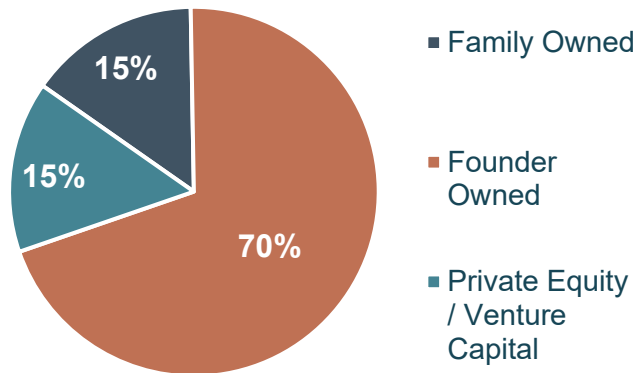


MERIDIAN CAPITAL

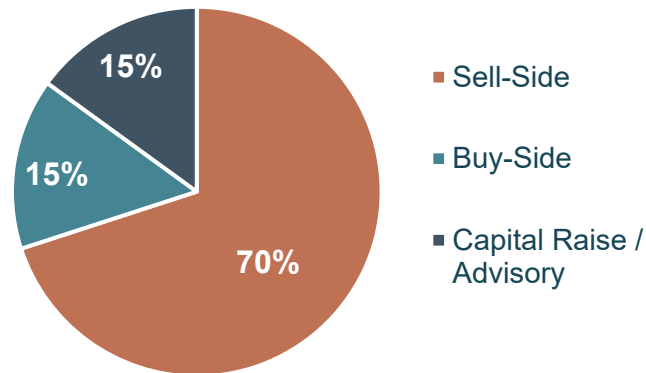
Firm Overview

CLA Meridian Capital has served as a trusted advisor to founders and entrepreneurs in achieving their M&A and corporate finance goals since 1995

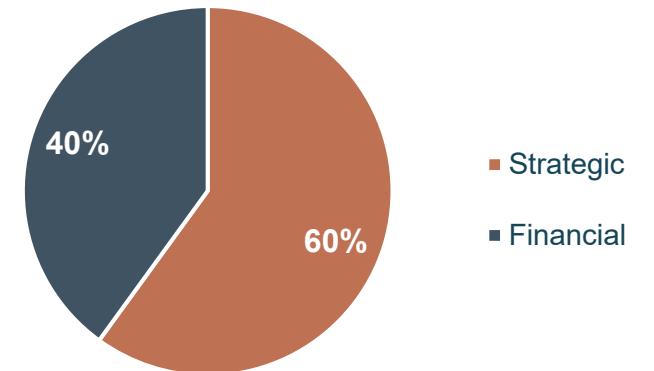
Client Type



Transaction Type



Buyer Type



85%+
Success Rate on Engaged Transactions

92%+
Deals Closed Above or Within Initial Valuation Range

CLA Meridian Capital Technology Investment Banking

CLA Meridian Capital leverages deep industry knowledge to execute complex and important transactions for middle market founder-focused clients

CLA Meridian Capital by the Numbers

400+ transactions completed	\$20M - \$500M transaction size range
50+ finance professionals	30+ countries via REACH M&A Partners

CLA Meridian Technology Practice Areas

				
Cybersecurity	Tech-Enabled Services	Hardware / Systems	Vertical Software	IT Services

Representative Transactions

Project Bastion Cybersecurity Consulting Firm - In Market / Sell-Side Engagement -	Project Obsidian Multimodal AI Fraud Detection Firm - In Market / Sell-Side Engagement -	Crosslake Technologies CROSSLAKE - Acquired by - FALFURRIAS CAPITAL	Ascent Solutions ASCENT SOLUTIONS - Acquired by - RUNTIDE CAPITAL
ASERVO Software ASERVO Software - Acquired by - knowmad mood	Avant Systems Group AVANT SYSTEMS GROUP - Acquired by - PRAECIPIO REACH	Blended Perspectives blended perspectives - Acquired by - CONTEGIX REACH	Accelalpha accelalpha - Recapitalized by - CENTURY PARK CAPITAL PARTNERS

Meet the Technology Team

Cybersecurity Leads		Patrick Ringland <i>President & Managing Director</i> 15+ years experience		Kendell Jensen <i>Vice President</i>
		Teague Collins <i>Managing Director</i> 15+ years experience		Tim Johnson <i>Vice President</i>
		Matt Rehtin <i>Managing Director</i> 15+ years experience		David Leber, CFA <i>Sr. Analyst</i>
				Luca Andonian <i>Analyst</i>

*Includes transactions completed by current employees while at previous firms

Select Business Services & Technology Transactions

CLA Meridian's bankers have significant experience across many years and technology transactions

Project Bastion Cybersecurity Consulting Firm - In Market / Sell-Side Engagement -	Project Obsidian Multimodal AI Fraud Detection Firm - In Market / Sell-Side Engagement -	Ascent Solutions  ASCENT SOLUTIONS - Acquired by -  RUNTIDE CAPITAL	ASERVO Software  ASERVO Software - Acquired by -  knowmad mood	Avant Systems Group  AVANT SYSTEMS GROUP - Acquired by -  PRAECIPIO REACH	Blended Perspectives  blended perspectives - Acquired by -  CONTEGIX REACH
Health Perspectives Group  HPG LLC Health Perspectives Group - Acquired by -  424 CAPITAL	Crosslake Technologies  CROSSLAKE - Acquired by -  FALFURRIAS CAPITAL	Xtreme Consulting  XTREME CONSULTING GROUP, INC. - Acquired by -  DISYS	QC Data  QC DATA - Acquired by -  ENENGINEERING	Cyient  CYIENT - Buy-side Advisory -  MERIDIAN CAPITAL	Accelalpha  accelalpha - Recapitalized by -  CENTURY PARK CAPITAL PARTNERS
Subsplash  SUBSPASH® - Growth equity financing by -  Enterprise Software Investors	Incluit  INCLUIT powered by avenga - Acquired by -  Avenga REACH	Apax Partners  apax - Has Acquired -  vitaprotech REACH	ENEA  ENEA - Acquired by -  AROBS Transilvania Software REACH	Smartfront  SMARTFRONT - Venture Funding by -  HIVENTURES REACH	Nirvana Soft  nirvanasoft People Development • Facilitation - Acquired by -  HANSEN TECHNOLOGIES

Cybersecurity Market Update

Cybersecurity Industry Overview & Trends



Spend Pivots to AI, Identity & Cloud - Security spend is forecast at \$248.9B in 2026 (+12.7%), with securing AI, cloud, and zero trust capturing incremental dollars and rewarding integrated platforms over subscale point products



The New Economics of Ransomware - Attackers are shifting from encrypting systems to stealing data, and with fewer victims paying ransoms, the exposure is now leaked data and extortion



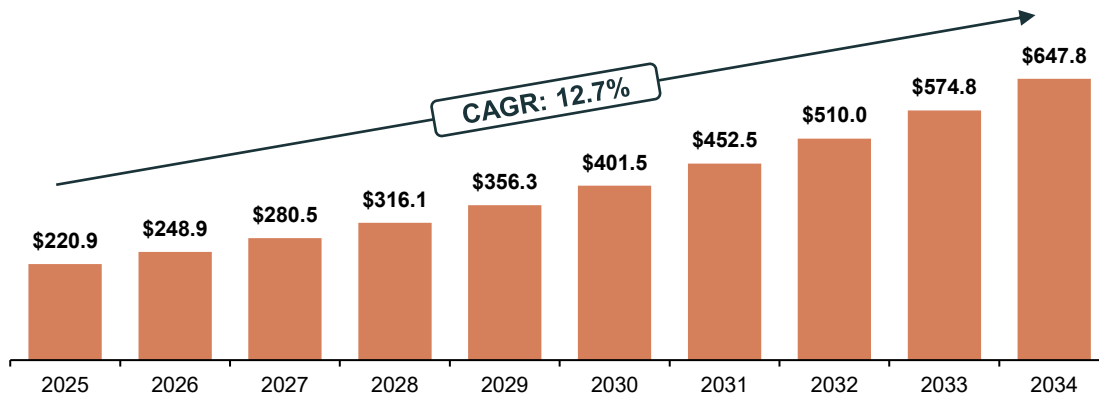
The Quantum Countdown Begins - Post-quantum standards are final and today's encryption is being phased out, yet most enterprises lack a migration plan, making cryptographic inventory an urgent priority



Regulation Diverges Across the Atlantic - The U.S. is easing mandates while the EU and UK extend reporting duties to vendors and service providers, driving durable demand for compliance services

Global Cybersecurity Market Size¹

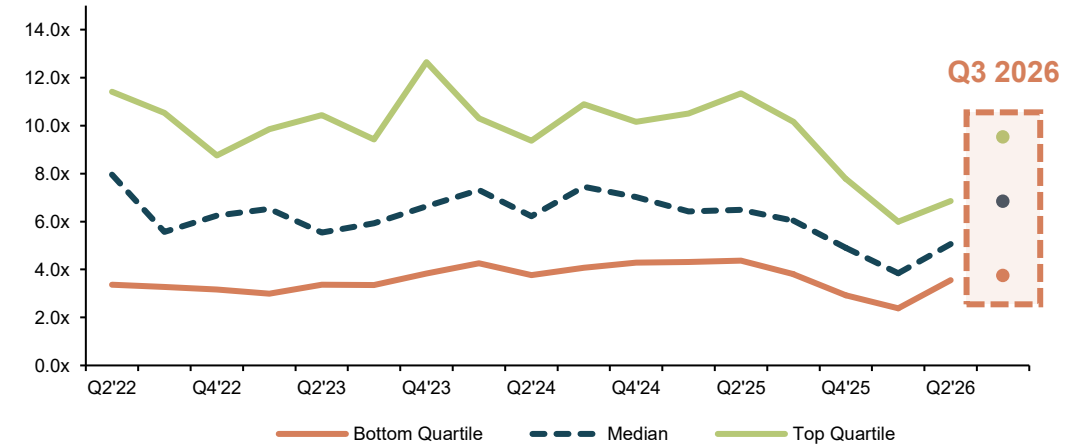
\$ in billions



Source: (1) Gartner, (2) PitchBook as of 09/30/2026

Cybersecurity – Public Company Valuation Multiples²

EV / LTM Revenue Multiple



- Multiples are rebounding off their Q1'26 trough as the AI-substitution sell-off of early 2026 has faded and premium strategic exits, a record pace of deal activity, and increased forecast spend growth have re-anchored valuations for scaled platforms
- As growth expectations normalize, investors have become increasingly selective, favoring platforms with durable growth, profitability, and clear strategic differentiation, while valuations for slower-growth or non-platform assets have faced greater pressure.
- Valuations in 2026 are expected to bifurcate further as the market shifts from broad sector tailwinds to a performance-driven environment. While median multiples for legacy tools remain compressed, premium assets that anchor on identity-first security and autonomous remediation are positioned for valuation expansion. This trend will likely carry through the year as enterprise buyers consolidate spend toward integrated platforms that meet the "Rule of 40" and demonstrate clear ROI against increasingly automated threats



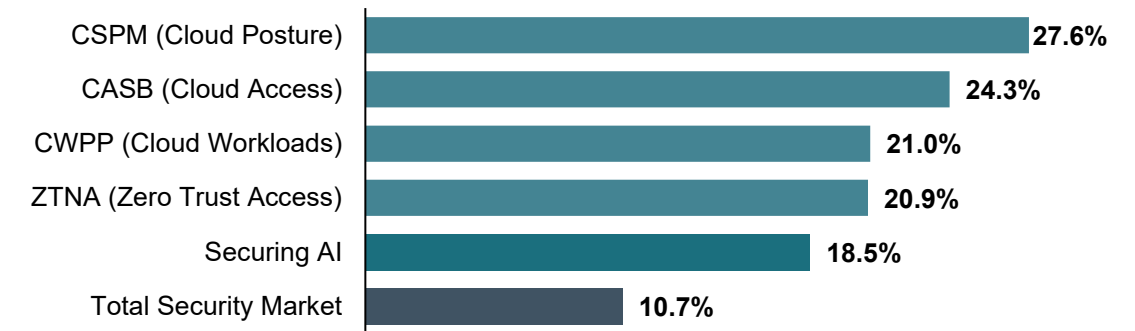
Security Spend Pivots to AI, Identity & Cloud

Security budgets continue to outgrow overall IT, but incremental dollars are concentrating in securing AI, cloud, and zero trust, rewarding integrated platforms while subscale point products lose share

Where the New Dollars Are Going¹

Gartner forecasts \$248.9B of worldwide security spend in 2026, up 12.7% and well ahead of overall IT, reaching \$372.6B by 2030 (10.7% CAGR). The fastest growth sits in cloud and zero-trust tools, while securing AI now stands as its own category and the largest single source of new spend

Fastest-Growing Categories, 2025–2030 CAGR¹



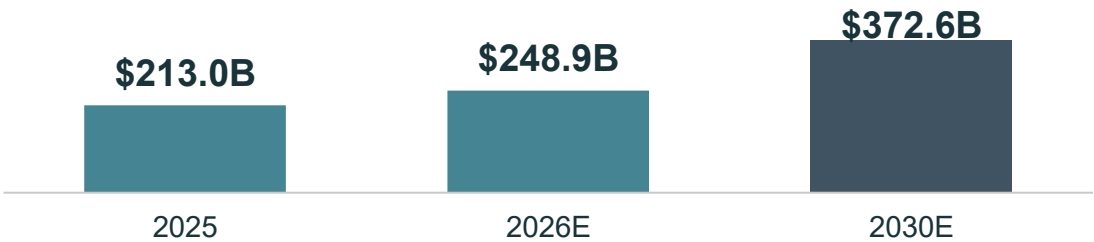
Securing AI is now tracked as its own category: \$15.6B in 2025 rising to \$37.6B by 2030 (18.5% CAGR), the only segment with accelerating growth and the largest source of new spend (\$21.9B). Strategics are buying agent-security capabilities (e.g., Palo Alto / Koi, Cyera / Oasis) rather than building them

Platforms Win as AI Reshapes the Stack^{1,2,3}

Momentum Cyber describes a “sharp bifurcation”: platform-aligned vendors command premiums while subscale point products struggle. AI is also emerging as a substitute for some tools; when Anthropic launched Claude Code Security in February 2026, CrowdStrike, Okta, and SailPoint shares fell 8–9%. Defensively, security AI is delivering measurable ROI in the SOC



Worldwide Security Spend (\$B)¹:



Investors are rewarding exposure to securing AI, identity, and cloud / zero trust, while undifferentiated point products face pressure from both platform consolidation and AI substitution

Source: (1) Gartner – Info. Security Forecast 2Q26 (Jun 2026); (2) Momentum Cyber – Mid-Year 2026 Review; Bloomberg (Feb 2026); (3) IBM – Cost of a Data Breach 2026; Palo Alto Networks (Feb 2026)

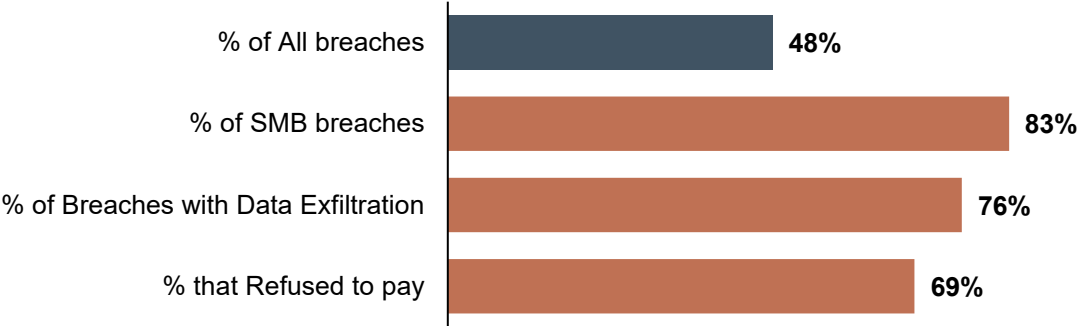
The New Economics of Ransomware

Ransomware has shifted from encryption to data-theft extortion: claimed attacks are hitting record highs even as victims increasingly refuse to pay, turning it into a data-breach and extortion problem more than a business-continuity one

From Encryption to Data Extortion^{1,2}

Ransomware remained the most common threat in 2025 breaches: a record 48% of all breaches (up from 44%) and 83% of breaches at small and mid-sized businesses. Attackers now steal data rather than lock systems, with exfiltration in 76% of cases

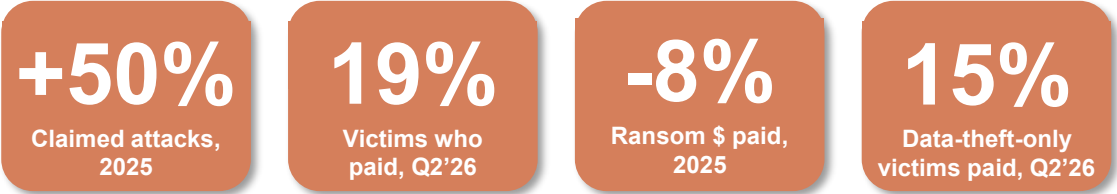
Ransomware by the Numbers



Ransomware was the single most common threat in 2025 breaches, reached a record 48% of all breaches, and appeared in 83% of breaches at small and mid-sized businesses. Because attackers now steal data rather than just lock it, clean backups no longer contain the damage: the real exposure is leaked data, extortion demands, and breach disclosure

Payments Fall as Attacks Hit Records^{2,3}

Total ransom dollars paid fell 8% to ~\$820M in 2025, 35% below the 2023 peak, even as claimed attacks rose 50%. A few large data-theft payments lifted the Q2 2026 average to \$1.88M while the median halved, and the share of victims paying has dropped to record lows amid stronger defenses, law-enforcement disruption, and a growing refusal to fund criminal enterprises



Average vs. Median Ransom Payment, Q2 2026 (\$)²:



As payment rates fall and attackers monetize stolen data over encryption, ransomware is becoming an extortion-and-breach exposure: shifting priority toward data governance, exfiltration detection, and disclosure readiness

Source: (1) Verizon – 2026 Data Breach Investigations Report (May 2026); (2) Coveware by Veeam – Q2 2026 Ransomware Report (Aug. 2026); (3) Chainalysis – 2026 Crypto Crime Report, ransomware chapter (Feb. 2026)

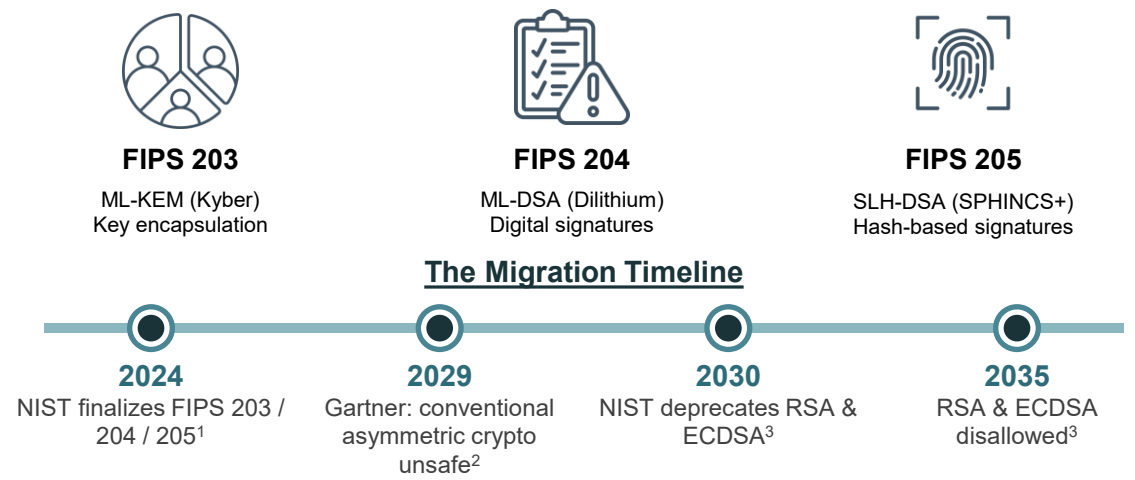


The Quantum Countdown Begins

With NIST’s post-quantum standards finalized and a deprecation clock now running, “harvest now, decrypt later” makes long-lived data an immediate risk; yet the vast majority of enterprises still have no migration roadmap

Harvest Now, Decrypt Later - The New Standards^{1,2,3}

- Adversaries are already stealing encrypted data to decrypt once quantum computers mature, a threat to any information with a multi-year shelf life. In August 2024, NIST finalized the first three post-quantum cryptography standards,¹ and its transition roadmap starts deprecating RSA and ECDSA in 2030 and disallows them after 2035.

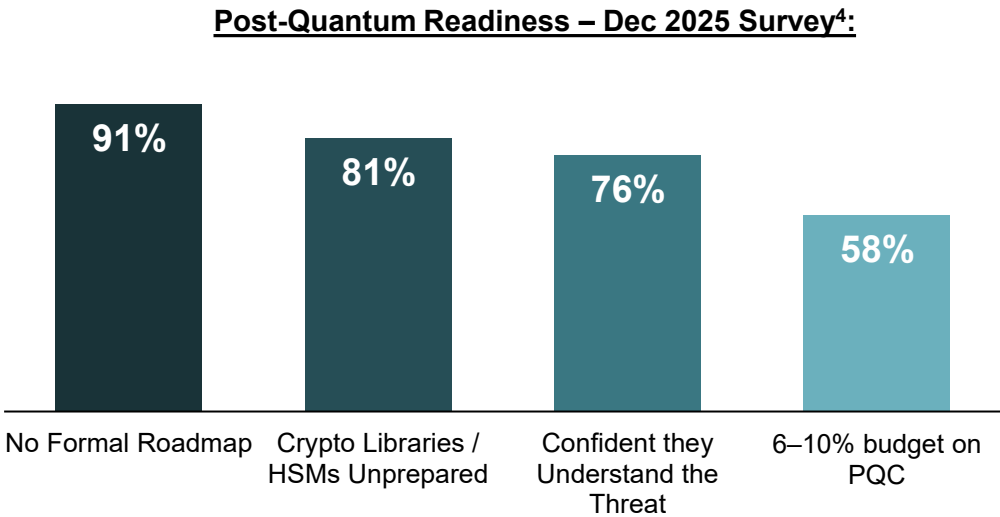


What this means for business owners

- Encryption is expiring:** the digital locks protecting your data will likely be unsafe by 2029, and U.S. rules phase them out between 2030 and 2035
- The risk is already here:** hackers can copy your data today and unlock it once quantum computers arrive, so anything that must stay private for years is exposed now
- Start now:** treat this as a multi-year project, and plan and budget for the move to quantum-safe encryption well before 2030

The Enterprise Readiness Gap⁴

- The standards exist, but migration is a multi-year, organization-wide effort spanning every system, vendor, and protocol that uses public-key cryptography. A December 2025 survey of 1,500 security professionals across the U.S. and Europe found most understand the threat but have not begun the work



The cryptographic standards are set and the deprecation clock has started, but crypto-agility takes years. Because “harvest now, decrypt later” puts long-lived data at risk today, building a cryptographic inventory is an urgent priority now, not a later problem

Source: (1) NIST – FIPS 203/204/205 (Aug 2024); (2) Gartner – Top Strategic Technology Trends 2025; (3) NIST – IR 8547; (4) Trusted Computing Group / Censuswide – PQC Readiness Survey (Dec 2025, n=1,500)

Cyber Regulation Diverges Across the Atlantic

The U.S. is streamlining and pausing compliance mandates while the EU and UK extend reporting duties to product vendors and managed service providers, shifting where compliance-driven demand shows up

U.S.: Lighter, More Targeted Rules^{1,2,3}

- The March 2026 Cyber Strategy for America favors offensive disruption and “common sense regulation” to cut compliance burden; in July, CMMC Phase 2 third-party certification (due Nov 2026) was suspended pending review
- CIRCIA's final rule, targeted for fall 2026, would require critical-infrastructure incident reports within 72 hours and ransom-payment reports within 24 hours

\$11.7B

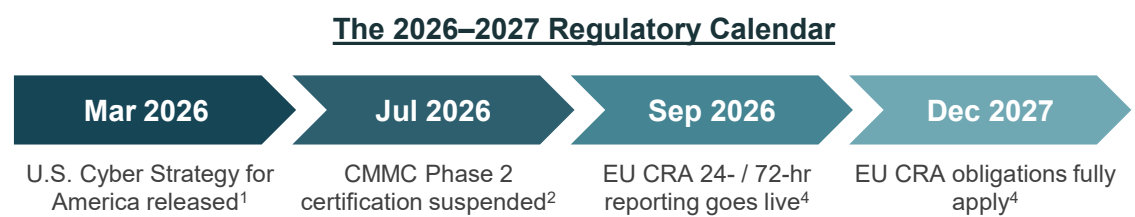
FY26 federal civilian cyber budget (down \$900M)³

+11.9%

FY26 DoD cyber spending growth³

Dec-26

Expiry of CISA 2015 info-sharing law³



What it means for companies

- **Defense-industrial-base demand is on hold:** it now hinges on the CMMC review, so underwrite on today's Phase 1 status quo with upside if certification returns
- **Steady EU / UK demand:** new rules drive recurring need for incident reporting, SBOM, vulnerability-management, and MSP-assurance services
- **MSPs become regulated entities:** providers selling into the UK or EU should expect obligations in their own right

EU & UK: Wider Scope, Faster Reporting^{4,5,6}

- Europe is moving the other way: obligations now reach software and device manufacturers and managed service providers, with 24-hour early warnings and penalties tied to global turnover. EU and UK rules also pull mid-sized companies into scope for the first time

Regime	Status	Key Requirements
EU Cyber Resilience Act	Reporting live Sep 2026; full application Dec 2027	Manufacturers must report actively exploited vulnerabilities and severe incidents in 24 hrs (early warning) / 72 hrs
EU NIS2 Amendments & Cybersecurity Act 2	Proposed Jan 2026; in negotiation	New “small mid-cap” tier (<750 employees, <€150M turnover); tighter ransomware reporting
UK Cyber Security & Resilience Bill	In Lords Committee; Royal Assent expected late 2026	Brings MSPs and data centres into scope; fines up to £17M or 4% of global turnover

Regulation is no longer a uniform tailwind: U.S. compliance demand is now timing-dependent, while EU and UK mandates create durable, recurring demand for reporting and assurance services, along with new liability for MSPs

Source: (1) Mayer Brown – Cyber Strategy for America (Mar 2026); (2) WilmerHale – CMMC Phase 2 suspension (Jul 2026); (3) Federal News Network (Jul & Sep 2026); Capstone Partners – Cybersecurity Market Update (May 2026); (4) Freshfields – CRA reporting obligations (2026); (5) Covington – NIS2 amendments & Cybersecurity Act 2 (Jan 2026); (6) ComplianceHub – UK Cyber Security and Resilience Bill (Sep 2026)

Top Cybersecurity Deals of the Last 12 Months

\$81B of value across 15 top deals since October 2025 shows buyers paying up to own identity, cloud, and OT control points, while new classes of acquirers bring cyber into payments, insurance, and IT workflows

Top Deals Over the Last 12 Months¹

Date	Target	Acquirer	Value	EV/ARR	Theme
Mar-26	Wiz	Google (Alphabet)	\$32.0B	32.0x	■ Cloud Security
Feb-26	CyberArk	Palo Alto Networks	\$25.0B	17.4x	■ Identity & AI Agents
Apr-26	Armis	ServiceNow	\$7.8B	22.9x	■ OT & Exposure Mgmt
Sep-26	Dragos, runZero, & NetRise	Accenture	\$4.2B	20.2x	■ OT & Exposure Mgmt
Aug-26	BioCatch	Visa	\$2.4B	13.0x	■ Fraud, Risk & Insurance
Jan-26	Jamf	Francisco Partners	\$2.2B	3.1x	■ Data & Device Security
Dec-25	Securiti AI	Veeam Software	\$1.7B	n/a	■ Data & Device Security
Sep-26	Oasis Security	Cyera	\$1.0B	n/a	■ Identity & AI Agents
Dec-25	Veza	ServiceNow	\$1.0B	n/a	■ Identity & AI Agents
Jul-26	Lansweeper	Bridgepoint	\$920M	8.0x	■ OT & Exposure Mgmt
Feb-26	SGNL	CrowdStrike	\$740M	n/a	■ Identity & AI Agents
Aug-26	At-Bay	Munich Re	\$575M	n/a	■ Fraud, Risk & Insurance
Sep-26	Console	Palo Alto Networks	\$500M	n/a	■ SecOps Automation
Apr-26	Koi	Palo Alto Networks	\$400M	n/a	■ Identity & AI Agents
Jun-26	Apono	1Password	\$250M	n/a	■ Identity & AI Agents

\$81B

Combined value of the top 15 deals

71%

of that value in two mega-deals (Wiz, CyberArk)

6 of 15

Top deals targeting identity & AI-agent security

7 of 15

Top deals won by buyers outside core cyber

What It Means for the Industry

- 1

Identity is the consolidation battleground

Six of the top 15 deals buy identity or AI-agent security. Platforms are paying to own the operating system for human, machine, and autonomous-agent identities, and agent security is now a bolt-on priority for every major vendor
- 2

Scale commands the premium

Strategics will pay for category leaders that anchor a platform, widening the valuation gap versus subscale point products. Growth remains the biggest driver of an outsized premium
- 3

The buyer universe is broadening

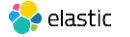
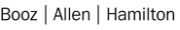
Visa, Munich, Accenture, ServiceNow, and Veeam show security being embedded into adjacent markets, adding new strategic bidders for sellers
- 4

Platforms are absorbing point products

Palo Alto Networks, ServiceNow, and CrowdStrike each bought specialist startups to fill gaps in their platforms. Standalone point products increasingly end up inside larger security platforms

Source: (1) Company press releases and news releases

Cybersecurity – Representative Competitive Landscape

Application Security Vulnerability scanning, application security testing, web application firewall and intrusion prevention systems	               
Data Security Data encryption, data loss prevention solutions and data access control	            
Managed Services Threat intelligence, firewall management, vulnerability management and SIEM	             
Identity/Access Management Identity governance, privileged access management, authentication and access control	        
Cloud Security Cloud intelligence & threat prevention solutions, cloud access security broker and workload protection solutions	              
Network Security Network firewalls, intrusion detection, prevention systems and virtual private networks protection	               
Endpoint Security Integrated firewall security, advanced antivirus programs, zero-day threat detection and response & encryption	           
Professional Services Cybersecurity assessment, incident detection & response, penetration testing, security architecture, and strategy	                 

Select Active Financial Investors: Cybersecurity

Investor	# of Investments Since 2020	Select Investments & Descriptions			
 THOMABRAVO	50+	 VARONIS Cybersecurity vendor focused on data privacy and security Jun-26	 KEYLESS Developer of a passwordless authentication platform designed for privacy-preserving biometrics Dec-25	 HORNETSECURITY Developer of AI-enabled threat detection, e-mail security and cloud backup solutions Dec-25	
 TA ASSOCIATES	40+	 ZERO POINT SECURITY Provider of cybersecurity training courses and hands-on labs Sep-25	 VALIMAIL Developer of an e-mail authentication and anti-fraud defense platform Sep-25	 EGNYTE Developer of a cloud-enabled content governance platform Feb-25	
 Charlesbank	30+	 Intangic Developer of a technology risk platform designed make informed decisions on cyber insurance risk Oct-25	 RANGEFORCE Operator of a learning platform intended to provide cybersecurity training and exercises Sep-25	 Lookout Developer of cloud-based security and secure access solutions May-25	
 ALPINE	25+	 ALL I.T. Provider of managed infrastructure, security, and cloud integration services Jun-26	 DATAGROUP TECHNOLOGIES, INC. Provider of cybersecurity, monitoring, data protection, and networking services Sep-25	 pch technologies Provider of cybersecurity and backup recovery services Jun-25	
 VISTA EQUITY PARTNERS	25+	 dryvIQ Developer of a unified platform intended to continuously automate security controls Aug-26	 kentic Developer of a network intelligence platform for complex network operations Aug-26	 AXUR Developer of an anti-fraud and digital risk protection platform May-26	
 KKR	25+	 evo Developer of an identity and access management software Jul-26	 Memética Provider of threat intelligence and online risk monitoring services Jan-26	 Saviynt Developer of cloud security and identity governance software Dec-25	
 TPG	20+	 strongdm Developer of an access control platform designed to secure access to every database Jan-26	 TROMZO Developer of an application security management platform Dec-25	 securiti Developer of a privacy management, governance, and compliance software Dec-25	

Source: PitchBook as of 09/30/2026

Disclosures

CLA Meridian Capital is the investment banking division of CliftonLarsonAllen Wealth Advisors, LLC. Securities and investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor, member FINRA/SIPC. For more information about CLA Wealth Advisors' business practices, fees, and services, please refer to our Form ADV Part 2A (the "Disclosure Brochure"). Your investment professional must provide you with a copy of the Disclosure Brochure before or at the time when you enter into a legal agreement with us.

Performance can not be guaranteed and any references to past specific performance should not be interpreted as a promise to achieve results. Investing involves various degrees of risk. You may lose money, including the principal of your investment.

Before deciding whether to engage CLA Wealth Advisors to manage any investment assets, you should review CLA Wealth Advisors' Form ADV Part 2A (the "Disclosure Brochure"). Our Disclosure Brochure provides detailed description of CLA Wealth Advisors, its services, fees, and other important information including explanation of conflicts of interest. CliftonLarsonAllen Wealth Advisors, LLC is a wholly owned company of CliftonLarsonAllen LLP.

Different types of investments involve varying degrees of risk, including the loss of principal. There can be no assurance that the future performance of any specific investment or investment strategy (including those undertaken or recommended by CLA Wealth Advisors), will be profitable or equal any historical performance level(s).



Thank you

CONTACT INFORMATION

Patrick Ringland
President & Managing Director
(206) 224-6155
patrick.ringland@claconnect.com

Kendell Jensen
Vice President
(425) 420-7270
kendell.jensen@claconnect.com



MERIDIAN CAPITAL



@CLA Meridian Capital



<https://meridianib.com>

