# CrowdStrike

February 24, 2026

# Disclaimer

The analyses and conclusions contained in this presentation are based on publicly available information. There may be confidential or otherwise nonpublic information in the possession of the companies discussed in this presentation that could lead these companies and others to disagree with these analyses, conclusions and opinions.

This presentation may include forward-looking statements, estimates, and projections which reflect various assumptions that may not be accurate.

The content expresses the views of the author as of the time of writing and such views are subject to change. This presentation and the information contained herein is not investment advice or a recommendation or solicitation to buy or sell any securities. Past performance is not indicative of future results. All investments involve risk, including loss of principal.

# Overview

CROWDSTRIKE

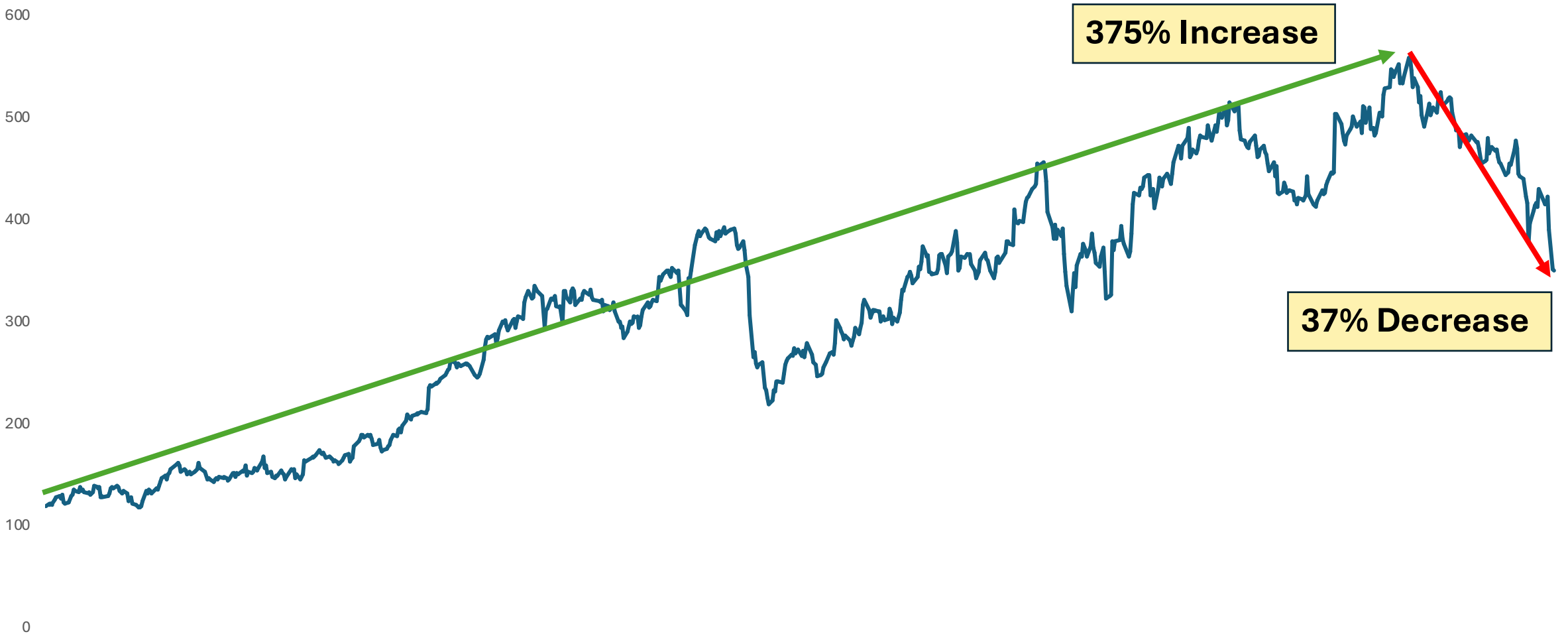
**Ticker: CRWD**

**Stock Price:**

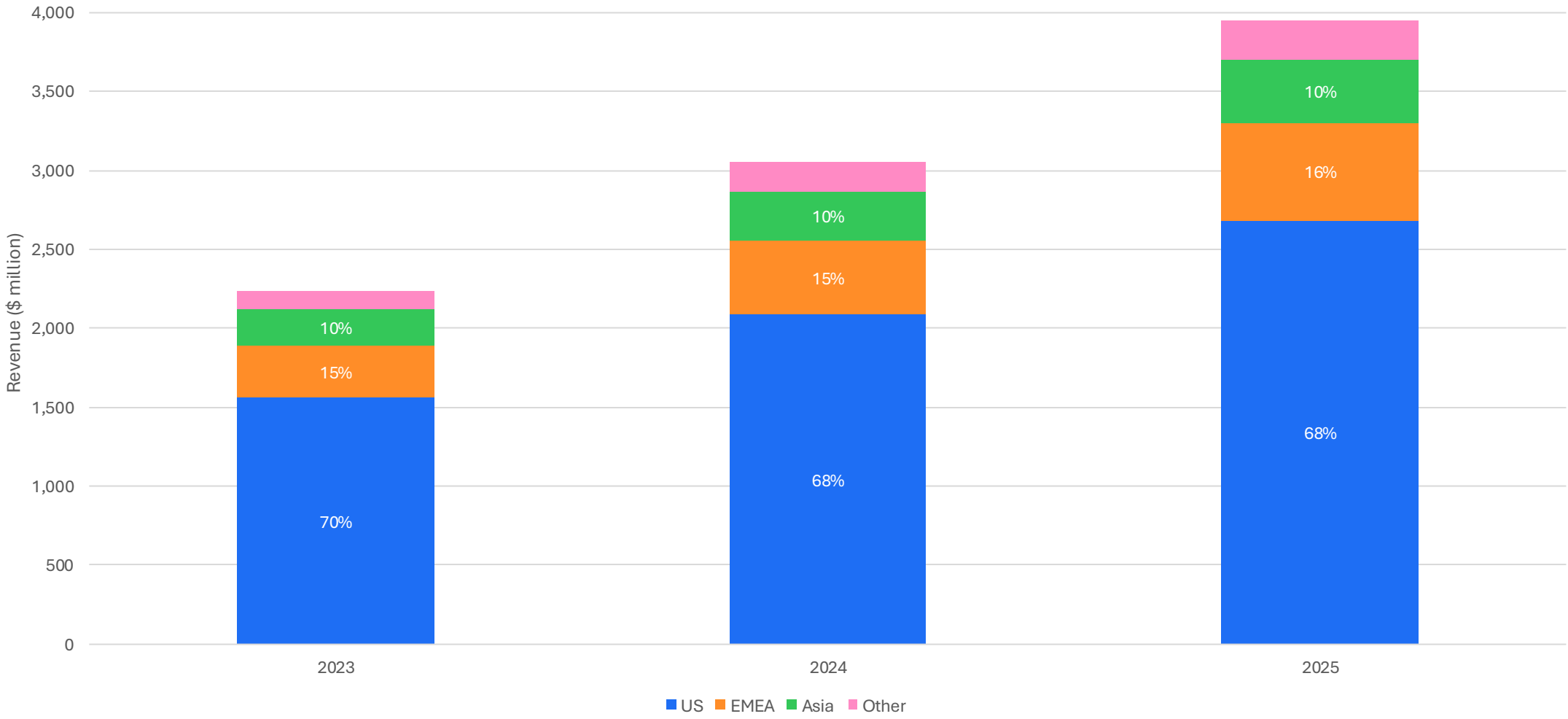
**$350.25**

- The leading cloud-native endpoint security platform
  - Founded in 2011; IPO in June 2019
- ~$4.24 billion in annual revenue (FY2026 guidance)
  - ~96% subscription revenue, ~4% professional services
- Market capitalization of ~$88 billion
- CEO George Kurtz has led CrowdStrike since founding

# 3 Year Stock Performance (since Feb. 2023)



# Revenue by Region



# Industry Overview

- Cybersecurity Market
  - ~$225 billion TAM by 2027, growing at ~12% CAGR
  - Fragmented market with no single dominant player above ~10% share
  - Platform consolidation is the key secular trend
- Endpoint Security
  - CrowdStrike, Microsoft, Palo Alto Networks, SentinelOne
  - Cloud-native architecture is the new standard
- Adjacent Markets
  - SIEM/log management, identity protection, cloud security
  - CrowdStrike expanding aggressively into all three

# Cybersecurity Market Dynamics

- Enterprises face an expanding attack surface
  - Cloud migration, remote work, and IoT proliferate endpoints
  - AI-powered attacks increasing in sophistication
- Regulatory pressure drives spending
  - GDPR, CCPA, SEC disclosure rules, NIS2 in Europe
  - Board-level priority: cybersecurity is no longer optional
- Platform consolidation replaces point solutions
  - Average enterprise uses 40-70 security tools
  - Consolidation onto fewer platforms reduces TCO and improves outcomes
  - CrowdStrike Falcon platform addresses this directly

# The Falcon Platform

- Single-agent, cloud-native architecture
  - Lightweight sensor deployed on endpoints
  - All processing in the cloud (no on-premise infrastructure)
- 28+ modules across multiple security domains
  - Endpoint Detection and Response (EDR/XDR)
  - Cloud Security (CNAPP/CSPM)
  - Identity Protection
  - Next-Gen SIEM (LogScale)
  - IT Operations (Falcon for IT)
  - Data Protection
- Falcon Flex: flexible licensing enabling platform consolidation
  - Customers adopt modules incrementally, deepening lock-in

# Competitive Standing

- Market leader in endpoint security with largest independent market share
  - Named a leader in Gartner Magic Quadrant for Endpoint Protection
  - #1 in IDC market share for modern endpoint security
- Strongest net retention and module adoption metrics in the industry
  - Net retention rate consistently above 120%
  - Customers with 5+ modules: 65%+; 7+ modules: 33%+
- Cloud-native architecture provides structural advantage vs legacy vendors
  - Microsoft bundling is the primary competitive threat
  - CrowdStrike positions as best-of-breed vs bundled solutions

# Competitive Advantage

- Massive data moat: trillions of security events processed weekly
  - AI/ML models improve with scale; more data = better detection
  - Threat graph correlates signals across entire customer base
- High switching costs once embedded in enterprise infrastructure
  - Deep integration with IT workflows, compliance, and incident response
  - Multi-module adoption compounds stickiness
- Network effects: each customer makes the platform better for all
- Platform breadth creates cross-sell engine
  - Land with endpoint, expand into cloud, identity, SIEM, and IT ops

# Why now?

- Post-incident recovery validates management and platform durability
  - July 2024 outage was a severe stress test
  - FY2026 Q2-Q3: reacceleration arrived earlier than expected
  - Record net new ARR in FY2026 Q3
- AI-driven security demand is accelerating
  - Enterprises need AI-powered defenses against AI-powered attacks
  - Cybersecurity spending is non-discretionary and growing
- Massive TAM expansion through platform consolidation
  - Falcon Flex driving larger, longer-term platform deals
  - Next-gen SIEM and identity markets represent major new growth vectors
- Stock has fallen ~37% from its highs

# AI “disruption”

- Claude Security scans a codebase to find vulnerabilities
  - Can export findings into existing security workflows (positioned as complementary to existing tools)
- Falcon platform provides endpoint security (AV/EDR/XDR) plus broader modules such as cloud security, exposure management, identity protection, and SIEM/log management
- CrowdStrike’s focus is detect/respond using telemetry from endpoints/workloads/identities
  - Claude Code Security is pre-deploy code review + patch suggestion
- Falcon Enterprise is $184.99 / year
  - The cost for 500 devices is less than just a single security engineer

# AI “disruption”

- Near-term revenue displacement is likely limited
- Longer-term displacement is also unlikely
  - Large-scale vendors have a positive feedback loop: more customers → more data → better detections → more customers
  - They correlate activity across industries, geographies, and cloud providers
  - Easier for security focused firms to hire the best talent
- Replicating these capabilities internally would require global sensor coverage, dedicated ML teams, 24/7 threat research, and continuous red-teaming and validation
  - That cost structure only works when amortized across thousands of customers

# The July 2024 Incident

- On July 19, 2024, a Falcon sensor update caused widespread system crashes
  - Issue identified at 04:09 UTC, remediated by 05:27 UTC
  - Affected millions of Windows endpoints globally
  - CISA issued a formal alert about the incident
- Near-term impact on sales cycles and customer sentiment
  - Management launched Customer Commitment Packages (CCP)
  - CCP designed as adoption accelerator, not permanent concession
  - Guided for approximately year-long headwind profile

# Post-Incident Recovery

- Reacceleration arrived earlier than management guided
  - FY2026 Q2: net new ARR inflected positively a quarter early
  - FY2026 Q3: record quarterly net new ARR, accelerating ARR growth
- CCP program ended on schedule as incident became historical
  - Temporary measure sunset, not perpetuated (key management quality signal)
  - Falcon Flex adoption accelerated as a direct result of CCP
- Record free cash flow and operating income in FY2026 Q3
- Demonstrates platform durability through the most severe stress test

# Strong Financial Position

- Minimal debt for a high-growth software company
  - Net cash position: the company is net cash positive
  - $1 billion share repurchase authorized in FY2026 Q1
- Strong and improving free cash flow generation
  - Free cash flow margins consistently expanding toward 35%+
  - Capital-light SaaS model requires minimal reinvestment

# Management

- Platform consolidation + module adoption as central strategy
- Maintained discipline: grew revenue while expanding margins
- Transparent about challenges
  - Upfront about July 2024 incident impacts on sales cycles and KPIs
  - Quantified CCP costs and timeline for investors
  - Guided conservatively, then delivered reacceleration ahead of schedule

# Management

- Consistently at the forefront of product innovation
  - Expanded from endpoint into cloud, identity, SIEM, and IT ops
  - Multiple successful acquisitions integrated (Humio/LogScale, Bionic, etc.)
- Strategic realignment plan (5% workforce reduction) to improve margins
- Actions taken quickly within a year of the incident

Management has shown that they operate as owners and understand what drives business value.

# Earnings Growth

- CrowdStrike guided toward the top end of their Q2 range in their Q3 call

| | Old | New |
|---|---|---|
| Revenue | $4.78 ± $0.03 billion | $4.80 ± $0.01 billion |
| Margins | 19.6% ± 0.5% | 19.8% ± 0.05% |
| non-GAAP EPS | $3.66 ± $0.06 | $3.71 ± $0.01 |

- Two quarters of EPS acceleration
- Strong revenue and ARR growth should continue
- Cloud Security will continue to be the fastest growing segments within security at ~25% CAGR (Gartner)
- Endpoint has one of the largest TAMs within security and is one of the fastest growing

# Risks

- Lingering fallout from the July 2024 incident
  - Delta litigation and DOJ/SEC information requests remain unresolved
- Microsoft bundling intensifies
  - Microsoft Defender gaining share, especially in SMB/mid-market
- Macro spending slowdown reduces security budgets
  - Cybersecurity is non-discretionary but enterprise budgets can stretch timelines
- Execution risk in adjacent markets (SIEM, identity, cloud)
  - Entering crowded markets against entrenched competitors
- Valuation compression if growth decelerates
  - Premium multiple requires sustained high growth

# CrowdStrike: Summary Investment Thesis

- ✓ Dominant platform in the large and growing cybersecurity market
- ✓ Cloud-native architecture provides structural competitive advantage
- ✓ 28+ modules create deep customer lock-in and cross-sell engine
- ✓ Proven management that navigated a major crisis with discipline
- ✓ Post-incident recovery validates platform durability and customer loyalty
- ✓ AI-driven threats ensure cybersecurity spending remains non-discretionary
- ✓ Attractive entry point after post-AI panic

CrowdStrike is a good business, in a good industry, with good management, at a good price.