

# Q2 2024 Cyber Security Update

## Cyber Security News/Insight

- Revenue in the global cybersecurity market is expected to reach \$185.7 billion in 2024, with an annual growth rate of 11.0%<sup>1</sup>. The security services segment is expected to contribute \$97.3 billion and cyber solutions is expected to contribute the rest.<sup>2</sup> During the period 2024-2029, revenue is expected to show an annual growth rate of 7.9%, resulting in a total market of \$271.9 billion by 2029<sup>3</sup>. This growth is expected to be led by the cyber solutions segment with an estimated CAGR of 10.9% and a resultant market size of \$148.3 billion<sup>4</sup> by 2029, followed by the security services segment at a lower rate of 4.9% and a resultant market size of \$123.6 billion by 2029<sup>5</sup>. The largest market for cybersecurity is the U.S. with a market size of \$81.4 billion in 2024. It is expected to grow at a CAGR of 9.4% during the period 2024-2029 to a market size of \$116.2 billion by 2029.<sup>6</sup>
- According to Statista, cybercrimes are expected to cost about \$9.2 trillion in 2024 with the cost expected to grow to \$13.8 trillion in 2028.<sup>7</sup> Based on a new report from the International Monetary Fund (IMF), global financial stability is threatened by the increasing frequency and sophistication of cyberattacks.<sup>8</sup>
- In April, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) publicly issued Emergency Directive 24-02 in response to a recent campaign by Russian state-sponsored cyber actor Midnight Blizzard targeting Microsoft corporate email accounts and potentially accessing correspondence with Federal Civilian Executive Branch (FCEB) agencies.<sup>9</sup>
- In May 2024, Germany announced that cybercrime by foreign actors rose 28% y/y in 2023. Furthermore, it has accused Russia of launching cyberattacks on German aerospace & defense firms, and the ruling party.<sup>10</sup>
- The 2024 Paris Olympic Games are facing an "unprecedented level" of cyber threats, according to the authorities. During the previous Olympic Games in Tokyo, it endured an estimated 450 million cyberattacks, according to technology giant Cisco. The company, which is an official partner for Paris 2024, says it expects eight times more attacks than the previous games in Tokyo.<sup>11</sup>

## Cybersecurity – Notable Ransomware Attacks and Breaches in Q2 2024

- On June 19, there were back-back cybersecurity attacks on a software company, CDK Global, that provides software for auto dealerships across the U.S. Nearly 15,000 car sellers that depend on CDK's dealer management software were affected. The company was forced to stop access to its core product, known as the dealer management system. Hackers demanded tens of millions of dollars in ransom. CDK issued a notice to customers that outside parties were reaching out to customers, while not naming the entity behind the intrusion.
- On June 4, Australian rare-earth metals producer Northern Minerals (ASX: NTU) announced that it was a victim of a cyberattack in March 2024 by the ransomware gang. The cybergang claimed to have exfiltrated project and mining research data, R&D and financial data, shareholder and investor information, the personal information of employees, and corporate email archives.<sup>12</sup>

- On May 9, Dell Technologies started informing millions of customers that data including full names and physical addresses – in addition to order service tags, item description, dates of orders and customer warranty information – was stolen during a security incident.<sup>13</sup>
- On May 8, Ascension, a non-profit that runs one of the largest healthcare systems in the U.S., was struggling to contain a cyberattack that caused disruption at hospitals throughout the country. Affected systems include electronic health records, the MyChart patient communication portal, certain phone systems, and systems used for ordering tests, procedures, and medications.<sup>14</sup>
- On May 5, the City of Wichita, Kansas shut down its computer network after becoming a victim of cyberattack by the Lockbit gang. The systems were encrypted with malware and it's unclear if any data was compromised, but the attack impacted water utility, municipal court, cultural, and public transportation payments.<sup>15,16</sup>
- On April 16, the United Nations Development Programme (UNDP) announced it is investigating a ransomware attack that occurred on March 27 with hackers stealing sensitive data. While UNDP has not shared any additional information on the incident, it appears to be the handiwork of a group named 8base as they listed UNDP on their Tor-based website.<sup>17</sup>
- On April 16, hospitality chain Omni Hotels & Resorts confirmed that a cyberattack on March 29 resulted in customer information being stolen and disruptions across all properties. The attack by the Daixin Team ransomware group claimed to have stolen records from 2017 belonging to 3.5 million visitors. The gang demanded \$2 million in ransom money.<sup>18</sup> On March 30, Japan-based optics giant Hoya, one of the largest global manufacturers of optical products, suffered a cyberattack that caused some of its production plants and business divisions to go offline. The company received a \$10 million ransomware demand from the Hunters International ransomware gang who claimed to have stolen 2TB of data.<sup>19,20</sup>
- On March 30, AT&T (NYSE: T) disclosed that the data including social security numbers and other personal information of approximately 73 million current and former customers were exposed on the dark web. The company revealed the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders. AT&T is yet to determine if the source of data was AT&T or one of its vendors.<sup>21</sup>

## New Products

- In June 2024, Darktrace (NASDAQ: DARK) launched its new service offering, Darktrace Managed Detection & Response (MDR), which combines its detection and response capabilities with expertise of its global analyst team.<sup>22</sup>
- In May 2024, CrowdStrike Holdings (NASDAQ: CRWD) announced new CrowdStrike Falcon Next-Gen SIEM innovations, which modernize SOC operations with a single, unified platform to deliver full visibility and protection across all workloads.<sup>23</sup>
- In May 2024, Palo Alto Networks (NASDAQ: PANW) introduced new security solutions infused with Precision AI to help enterprises tackle AI-generated attacks and effectively secure AI-by-design.<sup>24</sup>

## Cybersecurity – M&A and IPO Activity in Q2 2024

### Inside HUR Index Activity:

- On June 10, Fortinet (NASDAQ: FTNT) announced plans to acquire Lacework, a late-stage cloud security startup. Fortinet said the plan is to integrate Lacework's CNAPP product into the Fortinet Unified SASE offering.<sup>25</sup>
- On May 7, cloud and security giant Akamai (NASDAQ: AKAM) announced plans to acquire U.S.-based application programming interface (API) protection company Noname Security for \$450 million. The deal is expected to close in the second quarter of 2024 and Akamai expects the transaction to deliver roughly \$20 million in revenue for the fiscal year 2024.<sup>26</sup>
- On April 26, PE firm Thoma Bravo agreed to acquire UK-based cybersecurity firm Darktrace (NASDAQ: DARK) for ~\$5.32 billion in cash, representing a 44% premium to the volume-weighted average price per share for the three-month period ended April 25, 2024. The acquisition represents an EV / Revenue multiple of 8.1 times, and EV / Adjusted EBITDA multiple of 34.2 times.<sup>27</sup>

## Top 3 Contributors to HUR Index Performance in Q2 2024

### Broadcom<sup>28, 29, 30</sup>

- Stock price was up 36.0% from March 28, 2024 - June 18, 2024.
- Broadcom's performance was driven by strong results across its growing AI product portfolio and legacy VMware businesses with strong cybersecurity exposure. Q2 2024 revenue increased by 43% y/y to \$12.5 bn. Excluding VMware, revenue was up 12% y/y. Adjusted EBITDA increased by 31% y/y to \$7.4 bn. However, GAAP net profit was down to \$2.1 bn from \$3.5 bn in Q2 2023. Non-GAAP net profit increased to \$5.4 bn from \$4.5 bn in Q2 2023. Q2 Free Cash Flow (FCF) increased by 1.6% y/y to \$4.4 bn. Excluding restructuring and integration costs, FCF was up 18% y/y to \$5.3 bn.
- Raised FY 2024 guidance for consolidated revenue to \$51 bn and adjusted EBITDA to 61% of revenue.

### Darktrace<sup>31</sup>

- Stock price was up 32.3% from March 28, 2024 - June 18, 2024.
- On April 26, PE firm Thoma Bravo agreed to acquire UK-based cybersecurity firm Darktrace (NASDAQ: DARK) for ~\$5.32 billion in cash, representing a 44% premium to the volume-weighted average price per share for the three-month period ended April 25th 2024.

### CrowdStrike<sup>32, 33</sup>

- Stock price was up 21.5% from March 28, 2024 - June 18, 2024.
- CrowdStrike's stock rose due to a strong start to their fiscal year 2025 and strong guidance. Additionally, it is largely viewed as a GenAI beneficiary. Fiscal Q1 2025 ended with an ARR of \$3.65 bn and new net ARR of \$212 mn (+22% y/y growth). Operating income was \$199 mn and operating margin of 22% was 5% above the corresponding period last year. FCF was \$322 mn and up 42% y/y.

- Subscription revenue was \$872 mn and was up 34% y/y while total revenue grew 33% to \$921 mn. Non-GAAP subscription gross margin was >80%.
- Guided FCF margin of 31%-33% of revenue for FY 2025 and non-GAAP operating margin of 28%-32%.

## Bottom 3 Contributors in Q2 2024

### Fastly<sup>34,35</sup>

- Stock price was down 46.1% from March 28, 2024 - June 18, 2024.
- Stock came under pressure due to disappointing Q2 revenue guidance of 6%-9% and annual guidance of 12% driven by challenges in the short-term environment.
- Revenue came in at \$133.5 mn for Q1 2024, at the mid-point of guidance range. Operating loss narrowed to \$9.7 mn from a loss of \$14.1 mn in Q1 2023. Adjusted EBITDA was +\$3.7 mn and cash flow from operations was +\$11.1 mn. The company added two very large new customers in Q1, one of whom will move into the top 10 over the course of the year.
- Decline in revenue from a few of its largest customers resulted in guidance coming below expectations. Revenue from top 10 customers dropped from 40% to 38%. There was significant volatility within the top 10 customers, many of whom were on a multi-vendor strategy. The company won lower traffic share and the timing of rate and volume changes resulted in increased volatility this quarter.
- Enterprise customers stood at 3,290 at the end of Q1, down by one compared with an increase of 31 in Q4. Enterprise customer average spend was \$846,000, down 4% from \$880,000 in the previous quarter, and up 6% from \$795,000 in Q1 of last year.
- Q2 gross margin is expected to decrease approximately 130 basis points compared to Q1, plus or minus 50 basis points. Non-GAAP operating loss is expected to increase to \$12-\$16 mn in Q2, and FY 2024 gross margin is expected to improve by 200 basis points relative to FY 2023. FY 2024 free cash flow is expected to be close to breakeven compared to negative \$59 million in FY 2023.

### Qualys<sup>36,37,38</sup>

- Stock price was down 20.4% from March 28, 2024 - June 18, 2024.
- Qualys' stock came under pressure due to underwhelming revenue growth and guidance, at least partly attributed to macroeconomic headwinds. While the company has made investments to expand its channel partnerships and sales capacity, they have not yet translated to meaningful revenue growth.
- FY 2024 revenue is expected to be in the range of \$601.5-\$608.5 mn, representing a growth rate of 8%-10% y/y. Deals are being scrutinized with the upsell environment remaining challenging.

### SentinelOne<sup>39</sup>

- Stock price was down 22.1% from March 28, 2024 - June 18, 2024.
- The stock came under pressure due to a decline in net new ARR (annualized recurring revenue) and changes to its GTM (go-to-market) strategy that are yet to materialize. In fiscal Q1 2025, revenue grew

40% year-over-year (y/y) to \$186 million, and Annualized Recurring Revenue (ARR) grew 35% y/y to \$762 million. Growth was fueled by a combination of new customer growth and existing customer expansion. GAAP gross margin was 73%, compared to 68% in the year-ago quarter. GAAP operating margin was (43)%, compared to (86)%.

Disclaimer:

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. **ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.**

© 2024. Nasdaq, Inc. All Rights Reserved.

---

<sup>1</sup> <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

<sup>2</sup> <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

<sup>3</sup> <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

<sup>4</sup> <https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/worldwide>

<sup>5</sup> <https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide>

<sup>6</sup> <https://www.statista.com/outlook/tmo/cybersecurity/united-states>

<sup>7</sup> <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>

<sup>8</sup> <https://es.weforum.org/agenda/2024/06/la-estabilidad-financiera-mundial-en-peligro-debido-a-las-ciberamenazas-advierte-el-fmi-lo-que-hay-que-saber/>

<sup>9</sup> <https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-immediately-mitigate-significant-risk-russian-state-sponsored-cyber>

<sup>10</sup> <https://www.usnews.com/news/world/articles/2024-05-13/germany-says-cybercrime-by-foreign-actors-rose-by-28-in-2023>

<sup>11</sup> <https://www.weforum.org/agenda/2024/06/paris-olympics-2024-cybersecurity-experts-cyber-threats/>

<sup>12</sup> <https://www.securityweek.com/ransomware-gang-leaks-data-from-australian-mining-company/>

<sup>13</sup> <https://www.securityweek.com/dell-says-customer-names-addresses-stolen-in-database-breach/>

<sup>14</sup> <https://www.securityweek.com/healthcare-giant-ascension-hacked-hospitals-diverting-emergency-service/>

<sup>15</sup> <https://www.securityweek.com/city-of-wichita-shuts-down-network-following-ransomware-attack/>

<sup>16</sup> <https://www.securityweek.com/lockbit-takes-credit-for-city-of-wichita-ransomware-attack/>

<sup>17</sup> <https://www.securityweek.com/united-nations-agency-investigating-ransomware-attack-involving-data-theft/>

<sup>18</sup> <https://www.securityweek.com/omni-hotels-says-personal-information-stolen-in-ransomware-attack/>

<sup>19</sup> <https://www.bleepingcomputer.com/news/security/hoyas-optics-production-and-orders-disrupted-by-cyberattack/>

<sup>20</sup> <https://www.bleepingcomputer.com/news/security/optics-giant-hoya-hit-with-10-million-ransomware-demand/>

<sup>21</sup> <https://www.securityweek.com/att-says-data-on-73-million-customers-leaked-on-dark-web/>

<sup>22</sup> <https://darktrace.com/news/darktrace-launches-managed-detection-response-service-to-bolster-security-operations>

<sup>23</sup> <https://www.crowdstrike.com/press-releases/crowdstrike-delivers-falcon-next-gen-siem-innovations/>

<sup>24</sup> <https://investors.paloaltonetworks.com/news-releases/news-release-details/palo-alto-networks-launches-new-security-solutions-infused>

- 
- <sup>25</sup> <https://www.securityweek.com/fortinet-expands-cloud-security-portfolio-with-lacework-acquisition/>
  - <sup>26</sup> <https://www.securityweek.com/akamai-to-acquire-api-protection-startup-noname-security-for-450-million/>
  - <sup>27</sup> <https://www.securityweek.com/darktrace-to-be-taken-private-in-5-3-billion-sale-to-thoma-bravo/>
  - <sup>28</sup> <https://investors.broadcom.com/financial-information/quarterly-results>
  - <sup>29</sup> <https://investors.broadcom.com/news-releases/news-release-details/broadcom-inc-announces-second-quarter-fiscal-year-2024-financial>
  - <sup>30</sup> <https://investors.broadcom.com/static-files/602c2fd3-89a0-436f-b638-4890f20feda7>
  - <sup>31</sup> <https://ir.darktrace.com/financial-results>
  - <sup>32</sup> <https://ir.crowdstrike.com/financial-information/quarterly-results>
  - <sup>33</sup> <https://ir.crowdstrike.com/static-files/8ae4af6f-8d70-4c59-822d-c78b2bd43327>
  - <sup>34</sup> <https://investors.fastly.com/financials/quarterly-and-annual-results/default.aspx>
  - <sup>35</sup> [https://investors.fastly.com/files/doc\\_earnings/2024/q1/transcript/Fastly-Inc-FSLY-US-Q1-2024-Earnings-Call-1-May-2024-4\\_30-PM-ET.pdf](https://investors.fastly.com/files/doc_earnings/2024/q1/transcript/Fastly-Inc-FSLY-US-Q1-2024-Earnings-Call-1-May-2024-4_30-PM-ET.pdf)
  - <sup>36</sup> <https://investor.qualys.com/financials-filings/quarterly-results>
  - <sup>37</sup> <https://investor.qualys.com/static-files/9f08dcee-372c-4807-8032-64802c5e951a>
  - <sup>38</sup> <https://investor.qualys.com/static-files/073bb0de-7699-49c1-b378-b525c470df60>
  - <sup>39</sup> <https://investors.sentinelone.com/financial-info/quarterly-results/default.aspx>