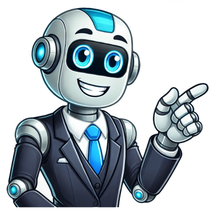
Continue



The cybersecurity platform for the AI era Stop the breach Cybersecurity is mission-critical. Stop sophisticated attacks with CrowdStrike. Reduce complexity Eliminate point products and multiple agents. Unify security and IT. Lower total cost Save time. Save money. Avoid potential business disruption and financial loss. The most anticipatedcybersecurity report of the year Download $6 of return for every $1 invested with a five-month payback period. 96% more potential threats identified in half the time. 2x as effective security teams with 66% faster investigations. Download report CBC unifies cybersecurity with CrowdStrike "The Falcon platform has allowed us to unify our security toolbox. It yields big savings for us, but more importantly, it allows us to focus. When an alert hits from the Falcon platform, we're able to address it without being distracted by other tools. Weve been more than delighted with CrowdStrike." Kevin Tsuei, SVP Information Security Officer Wyoming ends complexity and improves protection "Weve been able to add in Identity, weve been able to add in Vulnerability Scanning and bring all of those into that single pane of glass, which makes it accessible to our SOC as well as our leadership." Jason Strohbehn, Deputy CISO Montage Health threat response drops to seconds "One big consideration during the proof of concept (POC) was agent performance. We run a lot of virtual desktop infrastructure (VDI), so we didnt want our endpoint agent slowing down login or boot-up times. CrowdStrike was the superstar of the POC, so we bought it." Tahir Ali, CTO and CISO Our revolutionary, cloud-native architecture isnt bound by hardware-defined network perimeters. The Falcon platform converges security and IT to protect all key areas of risk. Easily deploy through a single, lightweight agent, then manage your security from a unified console. Add more platform modules using the same lightweight sensor from the original deployment. Integrate data from any source, try partner applications, and build with low-code tools. The Falcon platform drives the unification of data, security, and IT with generative AI and workflow automation built natively within. Threat Intel 1st and 3rd Party Data Using our native agent and expansive XDR integrations, the platform unifies threat intelligence with first- and third-party data for a platform database equipped to stop breaches. Security & ITAutomation Generative,Cloud and Sensor AI Designed with intention around an intelligent, AI-native platform that spans security and IT to predict and automate actions. Our x-factor: incident responders, threat hunters, intelligence analysts, and data scientists annotating our data to fuel the best AI models to stop breaches. IncidentResponders ThreatHunters food & beverage companies CrowdStrike named a Leader in the IDC MarketScape: Worldwide Managed Detection and Response 2024 Vendor Assessment. Get the report CrowdStrike receives the highest position of all vendors in the Strategy category and receives the highest scores possible in the Vision and Innovation criteria. Get the report CrowdStrike named a Leader in the IDC MarketScape: Worldwide Risk-Based Vulnerability Management Platforms 2023 Vendor Assessment. Learn more What you want Access to the entire CrowdStrike product portfolio, current and future. When you want Ability to swap modules annually, creating peace of mind when trying new products. At the best price Deploy and pay for what you need. No forced bundling. No costly suites. No shelfware. American cybersecurity technology companyThis article is about the company. For the widespread IT system outage in July 2024, see 2024 CrowdStrike-related IT outages.CrowdStrike Holdings, Inc.Company typePublicTraded asNasdaq:CRWD (Class A)Nasdaq-100 componentS&P 500 componentIndustryInformation securityFounded2011; 14years ago(2011)FoundersGeorge KurtzDmitri AlperovitchGregg MarstonHeadquartersAustin, Texas, United StatesKey peopleGeorge Kurtz (CEO)Michael Sentonas (President)[1]Revenue US$3.95 billion(FY25)Operating income US$120.4 million(FY25)Net income US$-19.27 million(FY25)Total assets US$8.7 billion(FY25)Total equity US$3.28 billion(FY25)Number of employees10,118(FY25)Websitewww.crowdstrike.com Footnotes/ referencesFinancials as of fiscal year ended January31, 2025[update].References:[2]Branch office in Sunnyvale, California which was formerly home to CrowdStrike headquartersCrowdStrike Holdings, Inc. is an American cybersecurity technology company based in Austin, Texas. It provides endpoint security, threat intelligence, and cyberattack response services.[3]The company has been involved in investigations of several high-profile cyberattacks, including the 2014 Sony Pictures hack, the 201516 cyberattacks on the Democratic National Committee (DNC), and the 2016 email leak involving the DNC.[4][5] On July 19, 2024, it issued a faulty update to its security software that caused global computer outages that disrupted air travel, banking, broadcasting, and other services.[6][7][8]CrowdStrike was co-founded in 2011 by George Kurtz (CEO), Dmitri Alperovitch (former CTO), and Gregg Marston (CFO, retired).[9][10][11][12] The following year, they hired Shawn Henry, a former Federal Bureau of Investigation (FBI) official, to lead the subsidiary CrowdStrike Services, Inc., which offered security and response services.[13][14] The company launched CrowdStrike Falcon, an antivirus package, as its first product in June 2013.[15][16]In May 2014, CrowdStrike's reports helped the United States Department of Justice to charge five Chinese military hackers with economic cyber espionage against U.S. corporations.[17] CrowdStrike also uncovered the activities of Energetic Bear, a group connected to Russia's Federal Security Service that conducted intelligence operations against global targets, primarily in the energy sector.[18]After the Sony Pictures hack, CrowdStrike uncovered evidence implicating the government of North Korea and demonstrated how the attack was carried out.[19] In 2014, CrowdStrike helped identify members of Putter Panda, the state-sponsored Chinese group of hackers also known as PLA Unit 61486.[20][21]In May 2015, the company released information about VENOM, a critical flaw in an open-source hypervisor called Quick Emulator (QEMU) that allowed attackers to access sensitive personal information.[22][23] In October 2015, CrowdStrike announced that it had identified Chinese hackers attacking technology and pharmaceutical companies around the time that U.S. President Barack Obama and China's leader Xi Jinping publicly agreed not to conduct economic espionage against each other. The alleged hacking would have been in violation of that agreement.[24]In July 2015, Google invested in the company's Series C funding round, which was followed by Series D and Series E, raising a total of $480 million as of May 2019.[25][26][27]In 2017, the company reached a valuation of more than $1 billion with an estimated annual revenue of $100 million.[28] In June 2018, the company said it was valued at more than $3 billion.[26] Investors include Telstra, March Capital Partners, Rackspace, Accel Partners and Warburg Pincus.[29][30]In June 2019, the company made an initial public offering on the Nasdaq.[31][32]CrowdStrike expanded its identity security offerings with Falcon Identity Threat Protection, initially available in 2020, which later evolved into a managed service integrating with Falcon Complete in 2022, and a Cloud Threat Hunting Service in July 2022.[33][34]In December 2021, the company moved its headquarters location from Sunnyvale, California, to Austin, Texas.[35]In 2023, CrowdStrike introduced CrowdStream service in collaboration with Cribl.io.[36] Charlotte AI, CrowdStrike's generative AI security analyst, was launched in May 2023 as part of Falcon's AI-driven security updates, enhancing automated threat triaging and response.[37]In September 2023, CrowdStrike launched Falcon Foundry, a no-code application development platform directed at a wider audience,[38] and in September 2024, the company launched CrowdStrike Financial Services, which offers payment solutions and financing to improve access to the Falcon platform.[39]CrowdStrike joined the S&P 500 index in June 2024.[40]As of 2024, CrowdStrike spent more than $360,000 on federal lobbying in the first half of 2024, according to OpenSecrets, and $620,000 during 2023.[41] The company has also focused on working with the U.S. government and selling its services to government agencies.[42]In November 2017, CrowdStrike acquired Payload Security, a firm that developed automated malware analysis sandbox technology.[43] In September 2020, the company acquired zero trust and conditional access technology provider Preempt Security for $96 million.[44] In February 2021, CrowdStrike acquired Danish log management platform Humio for $400million with plans to integrate Humio's log aggregation into CrowdStrike's XDR offering.[45] Later that November, CrowdStrike acquired SecureCircle, a SaaS-based cybersecurity service that extends zero trust endpoint security to include data.[46] In October 2022, CrowdStrike acquired Reposify, an external attack surface management vendor for risk management.[47] In 2023, CrowdStrike acquired Israeli cybersecurity startup Bionic.ai.[48] In 2024, CrowdStrike acquired Israeli cloud security startups Flow Security for $200 million[49] and Adaptive Shield for $300 million.[50]Recent Financial InformationYearRevenueNet Cash Flow (from operations)FY 2020$481.4 MM$99.9 MM[51]FY 2021$874.4 MM$356.6 MM[52]FY 2022$1.45 B$574.8 MM[53]FY 2023$2.24 B$941 MM[54]FY 2024$3.06 B$1.17 B[55]FY 2025$3.95 B$1.38 B[2]In 2024, total revenue was $3.06 billion, a 36% increase.[41]CrowdStrike helped investigate the Democratic National Committee cyberattacks and a connection to Russian intelligence services.[56] On 20 March 2017, James Comey testified before congress stating:[57]CrowdStrike, Mandiant, and ThreatConnect review[ed] the evidence of the hack and conclude[d] with high certainty that it was the work of APT 28 and APT 29 who are known to be Russian intelligence services.Comey previously testified in January 2017 that a request for FBI forensics investigators to access the DNC servers was denied, saying "Ultimately what was agreed to is the private company [CrowdStrike] would share with us what they saw."[58]In December 2016, CrowdStrike released a report stating that Russian government-affiliated group Fancy Bear had hacked a Ukrainian artillery app.[59] They concluded that Russia had used the hack to cause large losses to Ukrainian artillery units. The app (called ArtOS) is installed on tablet PCs and used for fire-control.[60] CrowdStrike also found a hacked variation of POPR-D30 being distributed on Ukrainian military forums that utilized an X-Agent implant.[61]The International Institute for Strategic Studies rejected CrowdStrike's assessment that claimed hacking caused losses to Ukrainian artillery units, saying that their data on Ukrainian D30 howitzer losses was misused in CrowdStrike's report. The Ukrainian Ministry of Defense also rejected the CrowdStrike report, stating that actual artillery losses were much smaller than what was reported by CrowdStrike and were not associated with Russian hacking.[62] Prior to this, CrowdStrike had published a report claiming that malware used in Ukraine and against the Democratic National Committee (DNC) appeared to be unique and identical, further evidence for a Russian origin of the DNC attack.[63]Cybersecurity firm SecureWorks discovered a list of email addresses targeted by Fancy Bear in phishing attacks. The list included the email address of Yaroslav Sherstyuk, the developer of ArtOS.[64] Additional Associated Press research supports CrowdStrike's conclusions about Fancy Bear.[65] Radio Free Europe notes that the AP report "lends some credence to the original CrowdStrike report, showing that the app had, in fact, been targeted."[66]In the TrumpUkraine scandal, Donald Trump, then the president of the United States, held a phone call with Volodymyr Zelensky, the president of Ukraine, on 25 July 2019, in which Trump asked Zelensky to look into a conspiracy theory that was being promoted on far-right websites such as Breitbart News and Russian state media outlets such as Russia Today and Sputnik.[67] The theory held that namely, that the Ukrainian government used CrowdStrike to hack into the Democratic National Committee's servers in 2016 and frame Russia for the crime to undermine Trump in the 2016 presidential election.[68][69] The conspiracy theory has been repeatedly debunked.[70][71][72]Main article: 2024 CrowdStrike-related IT outagesMultiple blue screens of death, caused by an update pushed by CrowdStrike, on airport luggage conveyor belts at LaGuardia Airport, New York CityOn 19 July 2024, CrowdStrike released a software configuration file update to the Falcon endpoint detection and response agent. Flaws in the update caused blue screens of death on Microsoft Windows machines, disrupting millions of Windows computers worldwide.[73][74] Affected machines were forced into a bootloop, making them unusable. This was caused by an update to a configuration file, Channel File 291, which CrowdStrike says triggered a logic error and caused the operating system to crash.[75] The downtime caused a widespread global impact, grounding commercial airline flights, temporarily taking Sky News and other broadcasters offline, and disrupting banking and healthcare services as well as 911 emergency call centers.[8][76]By the end of the day, CrowdStrike shares closed trading at a price of $304.96, down $38.09 or 11.10%.[77]Although CrowdStrike issued a patch to fix the error, computers stuck in a bootloop were unable to connect to the Internet to download the patch before Falcon would be loaded and crash the device again. The recommended solution from CrowdStrike was to boot into safe mode or Windows Recovery Mode and manually delete Channel File 291.[78] This requires local administrator access and if the device was encrypted by BitLocker, also required a recovery key.[79] Microsoft reported that some customers were able to remediate the issue solely by rebooting impacted devices up to 15 times.[80] On 22 July 2024, CrowdStrike shares closed the trading day at a price of $263.91, with a loss of $41.05 or 13.46%.[81] On 24 July 2024, five days after the incident, CrowdStrike published a Post-Incident Review.[82] That same day, CrowdStrike reportedly contacted affected channel partners with apology emails containing Uber Eats gift cards worth $10.[83][84][85] On 6 August 2024, Crowdstrike published a Root Cause Analysis to explain the causes of the Channel File 291 Incident, and the mitigation steps the company took to eliminate future incidents.[86] CrowdStrike made several process improvements in response to the 19 July incident. These include: adding new content configuration test procedures; implementing additional deployment layers and acceptance checks for its content configuration system; engaging two third-party vendors to review Falcon sensor code, and the company's quality control and release processes; and staggering update rollout in which users can select their preferred timing for updates.[87][41] The CrowdStrike incident cost Fortune 500 companies $5.4 billion.[41]Operating systemsChinese intelligence activity abroadChinese intelligence operations in the United StatesTimeline of Russian interference in the 2016 United States electionsTimeline of investigations into Donald Trump and Russia (JanuaryJune 2017)^ Richardson, Tom (31 March 2024). "CrowdStrike's Australian boss snares $225m cybersecurity fortune". Australian Financial Review. Archived from the original on 20 July 2024. Retrieved 21 July 2024.^ a b "US SEC: Form 10-K Crowdstrike Holdings, Inc., FY2025". U.S. Securities and Exchange Commission. 10 March 2025. Retrieved 19 March 2025.{{cite web}}: CS1 maint: url-status (link)^ "CrowdStrike's security software targets bad guys, not their malware". TechRepublic. 9 October 2015. Archived from the original on 2 June 2016. Retrieved 10 June 2016.^ "CrowdStrike demonstrates how attackers wiped the data from the machines at Sony". International Data Group. 2015. Archived from the original on 20 August 2016. Retrieved 9 June 2016.^ Hamburger, Tom; Nakashima, Ellen (24 July 2016). "Clinton campaign and some cyber experts say Russia is behind email release". The Washington Post.^ Banfield-Nwachi, Mabel (19 July 2024). "Windows global IT outage: what we know so far". The Guardian. London, United Kingdom. ISSN0261-3077. Archived from the original on 22 July 2024. Retrieved 19 July 2024.^ Plummer, Robert (19 July 2024). "Crowdstrike and Microsoft: What we know about global IT outage". BBC News. Archived from the original on 22 July 2024. Retrieved 19 July 2024.^ a b Godfrey, Paul; Druker, Simon; Wynder, Ehren (19 July 2024). "911 call centers back online after IT outage causes global chaos". United Press International. Retrieved 19 July 2024.^ "In conversation with George Kurtz, CEO of CrowdStrike". Fortune. Archived from the original on 1 July 2019. Retrieved 1 July 2019.^ "Bloomberg Dmitri Alperovitch". www.bloomberg.com. Archived from the original on 14 July 2020. Retrieved 14 February 2020.^ "Standing up at the gates of hell: CrowdStrike CEO George Kurtz". Fortune. 29 July 2015. Archived from the original on 29 May 2016. Retrieved 10 June 2016.^ Albert-Deitch, Cameron (15 May 2019). "CrowdStrike, the $3.4 Billion Startup That Fought Russian Spies in 2016, Just Filed for an IPO". Inc.com. Archived from the original on 3 June 2019. Retrieved 1 July 2019.^ Ragan, Steve (23 April 2012). "Former FBI Exec to Head CrowdStrike Services". SecurityWeek. Archived from the original on 20 January 2021. Retrieved 13 December 2020.^ Messmer, Ellen (18 April 2012). "Top FBI cyber cop joins startup CrowdStrike to fight enterprise intrusions". Network World. Archived from the original on 8 March 2024. Retrieved 10 June 2016.^ Messmer, Ellen (18 June 2013). "Start-up tackles advanced persistent threats on Microsoft, Apple computers". Network World. Archived from the original on 17 May 2019. Retrieved 1 July 2019.^ "U.S. firm CrowdStrike claims success in deterring Chinese hackers". Reuters. 13 April 2015. Archived from the original on 12 November 2017. Retrieved 14 June 2016.^ Gorman, Devlin Barrett and Siobhan (20 May 2014). "U.S. Charges Five in Chinese Army With Hacking". Wall Street Journal. ISSN0099-9660. Archived from the original on 15 February 2020. Retrieved 14 February 2020.^ "The old foe, new attack and unsolved mystery in the recent U.S. energy sector hacking campaign". CyberScoop. 12 July 2017. Archived from the original on 24 September 2019. Retrieved 14 February 2020.^ "What's in a typo? More evidence tying North Korea to the Sony hack". PCWorld. Archived from the original on 19 August 2016. Retrieved 14 June 2016.^ Perlroth, Nicole (9 June 2014). "2nd China Army Unit Implicated in Online Spying". The New York Times. ISSN0362-4331. Archived from the original on 12 November 2017. Retrieved 14 June 2016.^ "Second China unit accused of cyber crime". Financial Times. 10 June 2014. Retrieved 10 June 2014.^ "'Venom' vulnerability: Serious computer bug shatters cloud security". Fortune. 13 May 2015. Archived from the original on 25 April 2016. Retrieved 14 June 2016.^ Goodin, Dan (13 May 2015). "Extremely serious virtual machine bug threatens cloud providers everywhere". Ars Technica. Archived from the original on 22 June 2019. Retrieved 1 July 2019.^ Yadron, Danny (19 October 2015). "Report Warns of Chinese Hacking". Wall Street Journal. Archived from the original on 17 May 2019. Retrieved 1 July 2019.^ Kuranda, Sarah (17 May 2017). "Crowdstrike Lands $100M Funding Round, Looks To Expand Globally And Invest In Partners". CRN. Archived from the original on 3 June 2019. Retrieved 1 July 2019.^ a b "Cybersecurity startup CrowdStrike raises $200 million at $3 billion valuation". VentureBeat. 19 June 2018. Archived from the original on 3 June 2019. Retrieved 1 July 2019.^ "CrowdStrike may top these 6 biggest-ever U.S. security IPOs next month". www.bizjournals.com. Archived from the original on 28 April 2020. Retrieved 24 February 2020.^ Hackett, Robert (17 May 2017). "Hack Investigator CrowdStrike Reaches $1 Billion Valuation". FORTUNE. Archived from the original on 1 July 2019. Retrieved 9 June 2017.^ "Security Company CrowdStrike Scores $100M Led By Google Capital". TechCrunch. 13 July 2015. Archived from the original on 4 April 2019. Retrieved 1 July 2019.^ "CrowdStrike raises $100 million for cybersecurity". www.bizjournals.com. Archived from the original on 28 April 2020. Retrieved 24 February 2020.^ Murphy, Hannah (13 June 2019). "Cyber security group CrowdStrike's shares jump more than 70% after IPO". Financial Times. ISSN0307-1766. Archived from the original on 30 July 2024. Retrieved 13 June 2019.^ Feiner, Lauren (12 June 2019). "CrowdStrike pops more than 70% in debut, now worth over $11 billion". CNBC. Archived from the original on 12 June 2019. Retrieved 12 June 2019.^ "CrowdStrike launches Falcon Identity Threat Protection Complete," Techzine, March 2, 2022, retrieved March 3, 2025.^ "CrowdStrike introduces a new cloud threat hunting service," VentureBeat, July 26, 2022, retrieved March 3, 2025.^ "CrowdStrike Changes Principal Office to Austin, Texas". CrowdStrike. 28 December 2021. Archived from the original on 28 January 2022. Retrieved 2 February 2022.^ Alspach, Kyle. "RSAC 2023 Sees Big Moves From SentinelOne, CrowdStrike, Google Cloud, Accenture | CRN". www.crn.com. Archived from the original on 22 July 2024. Retrieved 29 February 2024.^ "CrowdStrike adds generative AI assistant to security tools," Axios, May 30, 2023, retrieved March 6, 2025.^ "CrowdStrike announces major build-out of its Falcon product suite," CSO, September 19, 2023, retrieved March 3, 2025.^ "CrowdStrike Unveils Financial Services, AI Tools at Fal.Con 2024," Channel Insider, September 23, 2024, retrieved March 6, 2025.^ Carson, Ed (9 June 2024). "CrowdStrike, KKR, GoDaddy To Join S&P 500 In Quarterly Rebalance; Stocks Jump". Investor's Business Daily. Archived from the original on 9 June 2024.^ a b c d Charlotte Ehrlich (9 October 2024). "Facing scrutiny over global outage, cybersecurity firm CrowdStrike on track for record year of federal lobbying spending".^ "CrowdStrike CEO George Kurtz on China, Microsoft and the SEC". CNBC. 14 December 2023. Archived from the original on 22 July 2024. Retrieved 19 July 2024.^ Kovacs, Eduard (21 August 2018). "CrowdStrike Adds Malware Search Engine to 'Hybrid Analysis'". Security Week.^ Gagliordi, Natalie. "CrowdStrike to acquire Preempt Security for $96 million". ZDNet. Archived from the original on 26 September 2020. Retrieved 28 September 2020.^ Cimpanu, Catalin (18 February 2021). "CrowdStrike acquires Humio for $400 million". ZDNet. Archived from the original on 11 July 2024. Retrieved 10 July 2024.^ Novinson, Michael (1 November 2021). "CrowdStrike To Buy Data Protection Startup SecureCircle". CRN. Archived from the original on 22 July 2024. Retrieved 10 June 2024.^ Dor, Ofir (20 September 2022). "CrowdStrike buying Israeli cybersecurity co Reposify". Globes.^ "CrowdStrike acquiring cyber startup Bionic for $350 million". CTech. 19 September 2023.^ "CrowdStrike acquiring cyber startup Flow Security in $200 million deal". CTech. 6 March 2024. Archived from the original on 20 July 2024. Retrieved 19 July 2024.^ Kovacs, Eduard (6 November 2024). "CrowdStrike to Acquire Adaptive Shield in Reported $300 Million Deal". SecurityWeek. Retrieved 6 November 2024.^ "US SEC: Form 10-K Crowdstrike Holdings, Inc., FY2020". U.S. Securities and Exchange Commission. 23 March 2020. Retrieved 19 March 2025.{{cite web}}: CS1 maint: url-status (link)^ "US SEC: Form 10-K Crowdstrike Holdings, Inc., FY2021". U.S. Securities and Exchange Commission. 18 March 2025. Retrieved 19 March 2025.{{cite web}}: CS1 maint: url-status (link)^ "US SEC: Form 10-K Crowdstrike Holdings, Inc., FY2022". U.S. Securities and Exchange Commission. 16 March 2025. Retrieved 19 March 2025.{{cite web}}: CS1 maint: url-status (link)^ "US SEC: Form 10-K Crowdstrike Holdings, Inc., FY2023". U.S. Securities and Exchange Commission. 8 March 2025. Retrieved 19 March 2025.{{cite web}}: CS1 maint: url-status (link)^ "US SEC: Form 10-K Crowdstrike Holdings, Inc., FY2024". U.S. Securities and Exchange Commission. 7 March 2024.^ - (Angel-Au Jung) (20 March 2020). " : , " [Hacker hunter and Trump's enemy: how a millionaire from the United States catches cybercriminals from Russia, China and Iran]. Forbes (forbes.ru) (in Russian). Archived from the original on 28 September 2020. Retrieved 20 September 2024.^ "Full transcript: FBI Director James Comey testifies on Russian interference in 2016 election". Archived from the original on 23 May 2017. Retrieved 22 May 2017.^ "FBI Director Comey: Agency requested access to DNC server". CBS News. 10 January 2017. Archived from the original on 21 September 2019. Retrieved 19 July 2024.^ "Russian hackers linked to DNC attack also targeted Ukrainian military, says report". theverge.com. 23 December 2016. Archived from the original on 17 November 2019. Retrieved 26 June 2019.^ Noosphere engineering school (31 October 2015). "New brainchild of engineering school was tested by the armed forces". noosphereengineering.com. Archived from the original on 29 December 2017. Retrieved 28 December 2017.^ Boldi (3 January 2017). "Technical details on the Fancy Bear Android malware (poprd30.apk)". Laboratory of Cryptography and System Security, Budapest University of Technology and Economics. Archived from the original on 9 February 2018. Retrieved 8 February 2018.^ Kuzmenko, Oleksiy (23 March 2017). "Think Tank: Cyber Firm at Center of Russian Hacking Charges Misread Data". Voice of America. Archived from the original on 20 January 2018. Retrieved 20 December 2017.^ "Group allegedly behind DNC hack targeted Ukraine, report finds". The Guardian. 22 December 2016. Archived from the original on 16 May 2017. Retrieved 19 July 2024.^ Miller, Christopher (2 November 2017). "Fancy Bear Tried To Hack E-Mail Of Ukrainian Making Artillery-Guidance App". RadioFreeEurope. Archived from the original on 6 February 2018. Retrieved 8 February 2018.^ Satter, Raphael (2 November 2017). "Russia hackers pursued Putin foes, not just US Democrats". Associated Press. Archived from the original on 2 April 2019. Retrieved 2 April 2019.^ Miller, Christopher (2 November 2017). "'Fancy Bear' Tried To Hack E-Mail Of Ukrainian Making Artillery-Guidance App". Radio Free Europe/Radio Liberty. Archived from the original on 2 April 2019. Retrieved 2 April 2019.^ Broderick, Ryan (26 September 2019). "Here's How Donald Trump Ended Up Referencing A Russian-Promoted 4chan Conspiracy Theory In His Call To The Ukrainian President". Buzzfeed News. Archived from the original on 8 October 2019. Retrieved 11 February 2024.^ Sullivan, Eileen (25 September 2019). "How CrowdStrike Became Part of Trump's Ukraine Call". The New York Times. Archived from the original on 26 September 2019. Retrieved 11 February 2024.^ Marks, Joseph (26 September 2019). "The Cybersecurity 202: Trump's CrowdStrike conspiracy theory shows he still doubts Russian election interference". The Washington Post. Retrieved 11 February 2024.^ Bajak, Frank (13 November 2019). "Debunked Ukraine conspiracy theory is knocked down again". Associated Press News. Archived from the original on 22 July 2024. Retrieved 11 February 2024.^ Cillizza, Chris (30 September 2019). "Don't miss the totally debunked conspiracy theory Donald Trump pushed in the Ukraine call". CNN. Archived from the original on 26 February 2024. Retrieved 11 February 2024.^ Collins, Ben (3 October 2019). "Trump seized on a conspiracy theory called the 'insurance policy.' Now, it's at the center of an impeachment investigation". NBC News. Archived from the original on 26 February 2024. Retrieved 11 February 2024.^ Baran, Guru (19 July 2024). "CrowdStrike Update Pushing Windows Machines Into a BSOD Loop". Cyber Security News. Archived from the original on 19 July 2024. Retrieved 19 July 2024.^ Sharwood, Simon. "CrowdStrike code update bricking Windows machines around the world". The Register. Archived from the original on 19 July 2024. Retrieved 19 July 2024.^ CrowdStrike (20 July 2024). "Technical Details: Falcon Update for Windows Hosts | CrowdStrike". crowdstrike.com. Retrieved 20 July 2024.^ Warren, Tom (19 July 2024). "Major Windows BSOD issue takes banks, airlines, and broadcasters offline". The Verge. Archived from the original on 19 July 2024. Retrieved 19 July 2024.^ "CrowdStrike Holdings Inc CRWD:NASDAQ". cnbc.com. 29 January 2012. Archived from the original on 16 June 2024. Retrieved 19 July 2024.^ "KB5042421: CrowdStrike issue impacting Windows endpoints causing an 0x50 or 0x7E error message on a blue screen - Microsoft Support". support.microsoft.com. Retrieved 20 July 2024.^ Warren, Tom (19 July 2024). "Here's how IT admins are fixing the Windows Blue Screen of Death chaos". The Verge. Archived from the original on 20 July 2024. Retrieved 20 July 2024.^ Warren, Tom (19 July 2024). "Microsoft on CrowdStrike outage: have you tried turning it off and on? (15 times)". The Verge. Archived from the original on 20 July 2024. Retrieved 20 July 2024.^ "CrowdStrike Holdings, Inc. Class A Common Stock (CRWD)". nasdaq.com. Retrieved 22 July 2024.^ "Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)". CrowdStrike. 24 July 2024. Retrieved 26 February 2025.{{cite web}}: CS1 maint: url-status (link)^ Franceschi-Bicchierai, Lorenzo (24 July 2024). "CrowdStrike offers a $10 apology gift card to say sorry for outage". TechCrunch. Retrieved 24 July 2024.^ Sato, Mia (19 July 2024). "CrowdStrike and Microsoft: all the latest news on the global IT outage". The Verge. Retrieved 14 August 2024.^ Milmo, Dan (25 July 2024). "CrowdStrike faces backlash as 'thank you' gift cards are blocked". The Guardian. ISSN0261-3077. Retrieved 14 August 2024.^ "External Technical Root Cause Analysis Channel File 29" (PDF). CrowdStrike. 6 August 2024. Retrieved 22 February 2025.{{cite web}}: CS1 maint: url-status (link)^ Vijayan, Jai (7 August 2024). "CrowdStrike Will Give Customers Control Over Falcon Sensor Updates". Dark Reading. Retrieved 22 February 2025.{{cite web}}: CS1 maint: url-status (link)Official website Business data for CrowdStrike Holdings, Inc.: GoogleReutersSEC filingsYahoo!Retrieved from " the CrowdStrike Falcon Sensor for LinuxNOTE: This software is NOT intended for use on computers that are NOT owned by Duke University or Duke Health. Please do NOT install this software on personally-owned devices. Installing this software on a personally-owned will place the device under Duke policies and under Duke control.Full Documentation and Further AssistanceA recent copy of the full CrowdStrike Falcon Sensor for Linux documentation (from which most of this information is taken) can be found at Duke NetID required).If you have questions or issues that this documentdoesn't address, please submit a ServiceNow case to "Device Engineering - OIT" or send an email tooitderequest@duke.edu.Troubleshooting Sensor Installation Issue: Your sensor installation fails.Solution: Verify that the SHA-256 checksum of the installer file you downloaded matches the SHA-256 checksum available from . Issue: Your Ubuntu installation fails with an error that "dependent packages are not installed."Solution: Use this command to install the dependent packages:$ apt-get -f install Issue: Your SLES installation fails with an error that nothing provides openssl1 >= 1.0.1. This is most commonly caused by a SLES version that doesn't include a modern OpenSSL implementation.Solution: Enable the SLES 11 security module: $ sudo zypper mr --enable SLE11-Security-ModuleRun the sensor installer again. Issue: Your installation fails with an error message about missing dependencies of libssl, libc, or libcrypto.–> Missing Dependency: libssl.so.10()(64bit) is needed by package falcon-sensor-1.0.3-1.e16x86_64 (/falcon-sensor-1.0.3-1.e16.x86_64)Error Missing Dependency: libc.so.6(GLIBC_2.7)(64bit) is needed by package falcon-sensor-1.0.3-1.e16x86_64 (/falcon-sensor-1.0.3-1.e16.x86_64)Error Missing Dependency: libcrypto.so.10()(64bit) is needed by package falcon-sensor-1.0.3-1.e16x86_64 (/falcon-sensor-1.0.3-1.e16.x86_64)Solution: Install a supported version of OpenSSL.Troubleshooting general sensor issues For hosts with the sensor already installed, verify kernel compatibility by checking RFM status. Run this command on the host:sudo /opt/CrowdStrike/falconctl -g --rfm-stateFor more info about RFM status, see "Appendix: Reduced Functionality Mode (RFM)" below. Check running processes to verify the Falcon sensor is running:ps -e | grep -e falcon-sensorCheck kernel modules to verify the Falcon sensor's kernel modules are running:lsmod | grep falconCheck the Falcon sensor's configurable options: sudo /opt/CrowdStrike/falconctl -g GET_OPTIONSGET_OPTIONS parameters:--cid for CustomerId--aid for AgentId--apd for App Proxy Disable--aph for App Proxy Host--app for App Proxy Port--rfm-state for indicating whether the sensor is in Reduced Functionality Mode--rfm-reason to determine reason for sensor running in Reduced Functionality Mode--trace for determining the configured trace level--feature to determine the configured sensor feature flags--metadata-query to determine the configured sensor cloud provider metadata query flags--version for version of sensor currently running--message-log for logging messages to disk--billing to configure the sensor billing type--tags for sensor grouping tags--provisioning-token for Provisioning Token--systags for system tags currently applied to a running sensorThe sensor requires these runtime services:networksystemdlocal-fssysinitmulti-usershutdown If the sensor is not running, verify that the sensor's application files exist on your host:$ sudo ls -al /opt/CrowdStrike /opt/CrowdStrike/falcon-sensorThis should be a symlink to either:the original sensor installation at /opt/CrowdStrike/falcon-sensora sensor update package with a release build number, such as /opt/CrowdStrike/falcon-sensor3000 You can verify that the host is connected to the cloud using Planisphere or a command line on the host.Planisphere:If a device is communicating with the CrowdStrike Cloud, Planisphere will collect information about that device on its regular polling of the CrowdStrike service. You can see the timing of the last and next polling on thePlanisphere Data Sources tab. You can see the specific information for your device on the device's Details tab.Host: Enter the following command in a terminal:$ sudo netstat -tapn | grep falconIf the Falcon sensor is communicating with the cloud, you'll see output like this:tcp 0 0 192.0.2.176:35382 ec2-54-148-96-12:443 ESTABLISHED 3228/falcon-sensor If OIT needs to forward a sensor issue to CrowdStrike Support, you will need to collect data using the falcon-diagnostic script.LogsLogs are stored within your host's syslog. The syslog locations vary but are specified in /etc/syslog.conf or rsyslog.conf, with these being the most common:/var/log/messages/var/log/syslog/var/log/rsyslog/var/log/daemongrep for the string falcon for sensor logs, similar to this example:sudo grep falcon /var/log/messages | tail -n 100Logs are kept according to your host's log rotation settings.Appendix: Reduced functionality mode (RFM)Reduced functionality mode (RFM) is a safe mode for the sensor that prevents compatibility issues if the hosts kernel is unsupported by the sensor. Both Windows and Linux sensors can enter RFM, but RFM behaves differently on each platform. RFM is a protective state to prevent damage to incompatible hosts.Hosts in RFM are unprotected by Falcon. When installing the sensor and upgrading hosts, ensure that kernels are compatible. Check regularly to verify your hosts arent in RFM.A sensor enters RFM when its installed on a host that has an incompatible kernel on a supported Linux distro. Sensors can enter RFM if their kernels are updated to an unsupported kernel version. Linux sensors in RFM do very little, due to their strong dependency on the host's kernel. They dont have detections or process execution events, but continue sending SensorHeartBeat events to indicate that a sensor is installed on the host. You can run the following command in terminal to verify RFM status:/opt/CrowdStrike/falconctl -g --rfm-state Upgrade the sensor to a version that supports your installed kernel, or change the hosts kernel to one supported by the sensor. While newly released long-term support (LTS) kernels for supported distros arent immediately compatible with the sensor, we add support as quickly as possible.To prevent existing sensors from entering RFM, CrowdStrike recommends disabling automatic kernel updates and upgrading your kernel when it is supported by the Falcon sensor. Consult your distros support documentation for pinning the existing kernel or configuring regular updates to leave the existing kernel in place.Appendix: Falcon-Kernel-Check toolThe falcon-kernel-check tool ensures the Falcon sensor will be fully operational on a host by verifying host kernels are compatible with Falcon. Its intended to be run before the sensor is installed. If a kernel is incompatible, the sensor might still install on a host but will be in Reduced Functionality Mode (RFM). While in RFM, the sensor is in a safety mode that protects it from severe compatibility errors. The sensor generates a heartbeat event, but does not perform any monitoring or prevention actions.Falcon sensor for Linux version 5.38 and later includes a feature to add support for new kernels without requiring a sensor update. Support for new kernels is added through Zero Touch Linux (ZTL) channel files that are deployed to hosts. The falcon-kernel-check tool currently only verifies kernel support for the initial release of the sensor version. As a result, kernel support that has been added through channel files for a sensor version are not reflected in the results of the falcon-kernel-check tool. For an up-to-date list of kernel support, including kernel support added through channel files, see Supported kernels.For hosts with the sensor already installed, verify kernel compatibility by checking RFM status. Run this command on the host:sudo /opt/CrowdStrike/falconctl -g --rfm-stateFor more info about RFM status, see "Appendix: Reduced Functionality Mode (RFM)" above. Download the appropriate sensor package for your host from falcon-dl.oit.duke.edu.New kernel support is added regularly, so it is important to ensure that you have the latest sensor installer before running falcon-kernel-check.System requirements:Supported Linux distro,Rpm2cpio (RPM-based distros only) Follow the appropriate extraction instructions for your distro:RPM-based distros:$ mkdir -p /tmp/crowdstrike$ rpm2cpio .rpm | (cd /tmp/crowdstrike; cpio -idv)DEB-based distros:$ mkdir -p /tmp/crowdstrike$ dpkg -x .deb /tmp/crowdstrike If extracted with one of the commands above, the falcon-kernel-check tool will be located in the /tmp/crowdstrike/opt/CrowdStrike/ directory and can be used two ways.To check the host's active kernel, run falcon-kernel-check with no parameters$ falcon-kernel-checkHost OS Linux 5.13.0-27-generic #29~20.04.1-Ubuntu SMP Fri Jan 14 00:32:30 UTC 2022 is not supported by Sensor version 12606.To check any other kernel, run falcon-kernel-check with the -k parameter. For example:$ sudo /opt/CrowdStrike/falcon-kernel-check -k 5.11.0-46-generic5.11.0-46-generic matches:5.11.0-46-generic #51~20.04.1-Ubuntu SMP Fri Jan 7 06:51:40 UTC 2022If a kernel version is available in multiple distributions, falcon-kernel-check displays the list of all kernels that match the specified parameter. For example:$ sudo /opt/CrowdStrike/falcon-kernel-check -k 5.11.0-10095.11.0-1009 matches:5.11.0-1009-aws #9~20.04.2-Ubuntu SMP Tue Jun 22 11:32:51 UTC 20215.11.0-1009-gcp #10~20.04.1-Ubuntu SMP Tue Jun 22 15:57:39 UTC