[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/financial-investment/who-is-crowdstrike-stock-price-analysis-microsoft-impact-future-prediction

Who is CrowdStrike? Stock Price Analysis, Microsoft Impact & Future Prediction

CrowdStrike's software update last Thursday caused a big crash in Microsoft Window around the world.The market reacted swiftly, sending CrowdStrike shares tumbling. On Friday, July 19th, the stock fell a staggering $38.09, or 11.10%, closing at $304.96 per share, marking a three-month low. This marked the third consecutive day of losses, adding to a 3.4% decline from the previous day.

So, how big of an impact will this incident have on CrowdStrike? What's the future for CrowdStrike stock price?

CrowdStrike IT Outage – Solutions

On the evening of July 18, Eastern time, Microsoft suddenly broke out and crashed, affecting about 8.5 million Windows devices around the world, and it turned out that the culprit was the network information security giant CrowdStrike updating software, which caused global flight delays, more than 5,000 flight cancellations, and disruptions to transportation, medical institutions, administrative agencies and banking operations.

The repercussions of the CrowdStrike IT outage were felt across a wide range of companies, many still struggling to recover from the disruption. Microsoft, in a statement released on Saturday, assessed the impact and estimated that 8.5 million Windows devices were affected by the outage. This represents less than one percent of all Windows machines globally, yet the economic and societal impacts were significant due to the crucial services run by enterprises utilizing CrowdStrike's solutions.
The CrowdStrike IT outage serves as a stark reminder of the importance of rigorous testing and quality assurance in software updates. While software updates are crucial for maintaining system security and functionality, defects or errors in these updates can have far-reaching consequences. Enterprises rely on cybersecurity providers like CrowdStrike to protect their critical systems and data, and any disruptions in these services can have significant implications for their operations. CrowdStrike has taken swift action to address the issue and minimize the impact on its customers. The company has deployed a fix for the defective update and is working closely with its customers to ensure a smooth recovery. While the outage has caused some short-term disruption, CrowdStrike's prompt response and commitment to resolving the issue demonstrate its commitment to providing reliable and secure cybersecurity solutions.

CrowdStrike Stock Financial Impact & Consequences

Raj Joshi, a senior VP at Moody's Ratings, has issued a statement highlighting the risk of significant liability claims stemming from affected customers. "The outages have not only raised questions about CrowdStrike's software engineering practices, but they have also underscored the growing vulnerabilities in global cloud infrastructure, with an increasing number of potential failure points," he said.
This situation could have significant ramifications for CrowdStrike's stock price, as investors assess the potential impact of customer dissatisfaction and legal action. Endpoint security is a crucial aspect of any organization's cybersecurity posture, and any perceived weaknesses in CrowdStrike's offerings could erode investor confidence.
Moreover, with the company's second quarter ending on July 31, investors are likely to scrutinize the financial results for any signs of the outages' impact. Any negative financial indicators or comments from the company's leadership could further exacerbate the stock's downward trajectory.
Amidst the latest developments surrounding CrowdStrike, financial analysts are warning of potential consequences for the company's stock. BMO Capital Markets analyst Keith Bachman recently stated in a report, "We believe there will be financial consequences from this issue." Bachman cited the likelihood of customers seeking relief and compensation for damages, potentially including discounts or credits for new contracts and renewals, suggesting a potential impact on growth rates and cash flow.

The situation escalated on Friday when Tesla, SpaceX, and X Chief Executive Elon Musk took to social media to announce, “We just deleted CrowdStrike from all our systems.” Musk did not specify if this action was taken by one or all of his companies, further fueling speculation about the severity of the issue.

Jefferies analyst Joseph Gallo echoed these concerns with a dire view of the situation. Gallo’s assessment underscores the potential for significant financial repercussions for CrowdStrike, especially given the high-profile nature of Musk’s announcement and the potential ripple effects it could have on the company’s reputation and customer base.

In the wake of recent outages and potential customer losses, the financial implications for CrowdStrike stock are becoming increasingly evident. Analyst Gallo has raised concerns about the expense burden CrowdStrike faces as it works to address the issues and potentially dispense credits to affected customers, which could significantly impact its margins. While the exact extent of the credits, discounts, or additional free products remains unclear, Gallo predicts that CrowdStrike will need to take significant steps to appease its customers and mitigate the damage.

The reputational damage resulting from these outages is particularly concerning for CrowdStrike, particularly among mission-critical infrastructure and government customers. This damage is likely to elongate deal cycles and further constrain CrowdStrike’s potential upside as new customers await assurances that the situation has been adequately handled. The timing of these outages, occurring in the last two weeks of the quarter, could not have been worse for CrowdStrike, as this is typically the most crucial period for financial results.

Today, CrowdStrike stock fell sharply, down 11.1% to close at 304.96. This decline follows a strong run-up in 2024, with CrowdStrike stock gaining 34% through Thursday’s market close. However, the recent outages and customer losses have cast a shadow over the company’s prospects, and investors are starting to question whether the stock’s valuation can be sustained.

In contrast, SentinelOne stock popped 7.9% to 21.72, while Palo Alto Networks stock rose 2.2% to 330.89. These gains suggest that investors may be shifting their focus to other cybersecurity stocks, at least in the short term. However, it remains to be seen whether these gains will be sustained, given the overall volatility in the cybersecurity industry.

CrowdStrike’s XDR platform, which stands for extended detection and response, has been a key part of the company’s strategy. This platform provides a broad, threat-detection cybersecurity solution that monitors endpoints, web/email gateways, web application firewalls, and cloud business workloads. However, the recent outages have called into question the reliability and effectiveness of this platform, which could further erode investor confidence.

CrowdStrike: Definition & Overview

CrowdStrike stands as the pioneering and unparalleled force in the cybersecurity landscape, pioneering the integration of next-generation antivirus (AV), endpoint detection and response (EDR), and offering round-the-clock threat detection services. Founded in 2011, this California-based company has established itself as the global leader in endpoint security, leveraging cutting-edge technology to safeguard enterprises and government agencies against the ever-evolving cyber threats.

At the heart of CrowdStrike’s offerings lies the Falcon platform, a comprehensive cybersecurity solution that detects, prevents, and defends against cyber threats for customer computer systems, including Microsoft. Through remote operations, Falcon provides a robust defense mechanism that helps computer systems resist hacker intrusions, ensuring the integrity and security of critical data and systems.

However, a recent incident involving CrowdStrike’s Falcon Sensor software highlights the complexities and challenges in the cybersecurity domain. According to reports from computer system experts, the incident stemmed from the deployment of the latest version of the Falcon Sensor

software, which aimed to enhance customers' computer systems' ability to withstand hacker intrusions. Unfortunately, it was suspected that a defective program code interacted with Microsoft systems, leading to instability and eventual crashes.

CrowdStrike responded promptly, releasing a remote fix to address the issue. However, bringing the affected systems back online requires a manual cleanup of the defective code, which can be a time-consuming process. While some computer systems with lower protection levels can be restored within a day, those with higher levels of security may take several days to recover fully.

Despite this setback, CrowdStrike's position as a leading cybersecurity provider remains unwavering. The company's software is trusted by over half of the Fortune 500 companies and numerous government agencies, including the top U.S. cybersecurity agency and the Infrastructure Security Agency. This widespread adoption reflects CrowdStrike's ability to provide reliable and effective cybersecurity solutions that meet the stringent requirements of enterprises and governments worldwide.

Moreover, CrowdStrike's commitment to innovation and excellence is evident in its continuous investment in research and development. The company's team of experts is constantly working to stay ahead of the curve, identifying and mitigating emerging threats to ensure customers' systems remain secure.