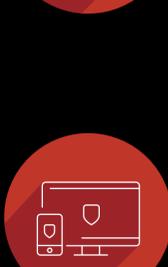


# CrowdStrike Global Security Attitude Survey

**Customers are losing trust in Microsoft and legacy IT, as software supply chain attacks present an increasing concern for organizations**



**63%**

of respondents admit that their organization is losing trust in suppliers, such as Microsoft, due to frequent security incidents



**84%**

believe that software supply chain attacks could become one of the biggest cyber threats to organizations like theirs within the next three years

**45% of respondents' organizations experienced at least one software supply chain attack** in the last 12 months, **compared to 32% in 2018**

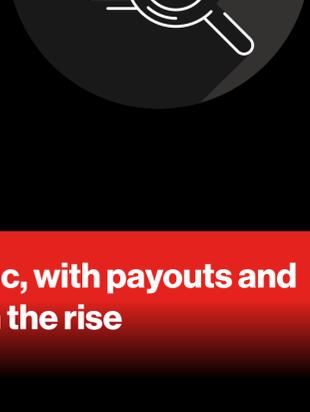


**77% of respondents** report that their organization has experienced a **supply chain attack** in the past, **increasing from 66% in 2018**



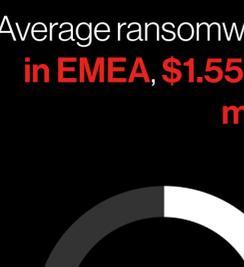
**Only 36%**

have vetted all new and existing suppliers for security purposes in the last 12 months



**Ransomware remains prolific, with payouts and extortion fees on the rise**

The average ransom payment for those who paid one was **\$1.79 million (USD)**, compared to **\$1.10 million (USD)** in 2020



of those who **paid the initial ransom** also had to pay **extortion fees**, on average totaling **\$792,493**

Average ransomware payment was **\$1.34 million in EMEA**, **\$1.55 million in the US**, and **\$2.35 million in APAC**



of respondents' organizations **suffered at least one ransomware attack** in the **past 12 months**



of those hit by ransomware **didn't have a comprehensive strategy** in place to coordinate their response

**Organizations are moving in the wrong direction when it comes to detection and response time, demonstrating that security transformation must be an urgent priority, particularly given the shift to remote and hybrid working models**



CrowdStrike encourages organizations to strive to meet the 1-10-60 rule: where security teams demonstrate the ability to detect threats within the first minute of an intrusion, investigate and understand the threat within 10 minutes, and contain and eradicate the threat within 60 minutes.



	CrowdStrike benchmark	2021 survey average
Time to <b>detect</b>	1 minute	146 hours
Time to <b>investigate</b>	10 minutes	11 hours
Time to <b>remediate</b>	60 minutes	16 hours

## Methodology

CrowdStrike commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 2,200 senior IT decision makers and IT security professionals were interviewed during September, October, and November 2021, with representation across the US, EMEA and APAC regions. All respondents had to be from organizations with 100 or more employees and are from a range of private and public sectors. Unless otherwise indicated, the results discussed are based on the total sample.

For more insights, [download the full report](#)

## About CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: <https://www.crowdstrike.com/>  
Follow us:

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

© 2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.