

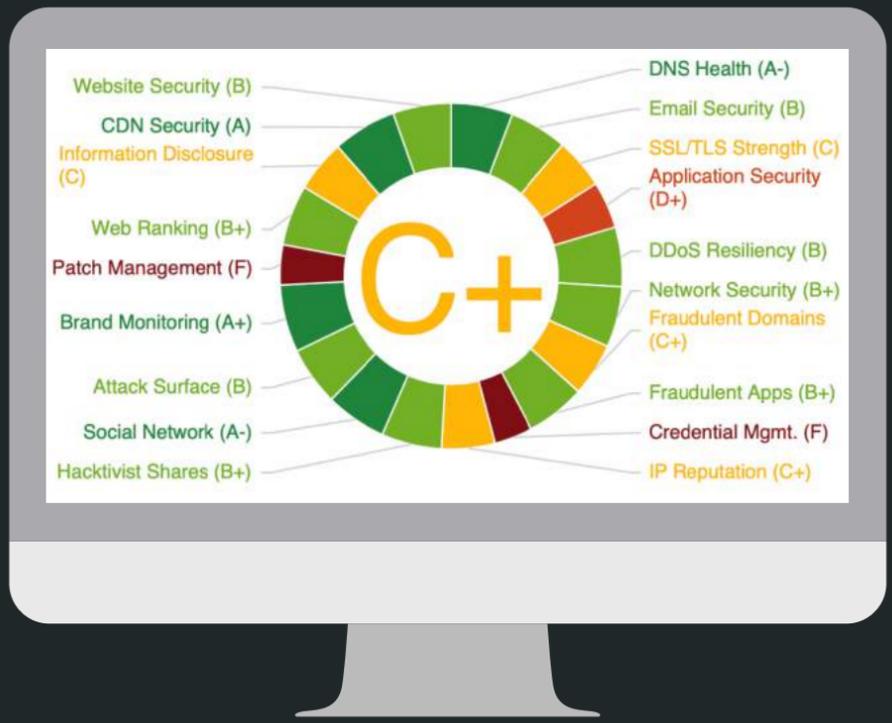


NASDAQ 100

The State of Cyber Risk and Ransomware Susceptibility

The second-largest stock and securities exchange in the world attracts high-growth companies eager to operate their trades in an entirely electronic fashion. Major stocks that trade on the Nasdaq include Apple, Amazon, Microsoft, Facebook, Gilead Sciences, Starbucks, Tesla, and Intel.

Black Kite's research team completed a thorough risk assessment on the top 100 NASDAQ businesses currently operating in the exchange in order to discover key security vulnerabilities that could lead to a supply chain breach.



INSIDE THE RATING: KEY RANSOMWARE FINDINGS

Dive deeper to better understand common ransomware indicators



92%

92% of companies have at least one high-severity vulnerability due to out-of-date systems

Exploiting vulnerabilities that allow remote code execution is trending in the ransomware community. Although it's not as easy as using RDP ports, it's not as arduous as (spear) phishing.



15%

15% of companies are above the critical Ransomware Susceptibility Index™ (RSI) threshold

Using data and machine learning, Black Kite's RSI™ discovers the likelihood that an organization will experience a ransomware attack. 15% of companies are highly susceptible to a ransomware incident.



82%

82% of companies have publicly visible ports

A publicly visible port is a critical resource ransomware groups exploit. Although the use of ports is declining each year, cybercriminals can still easily scan open ports with autonomous tools.

41.3M

AVERAGE ANNUAL FINANCIAL RISK

Black Kite leverages the OpenFAIR™ methodology to transform cyber risk into financial terms. The FAIR calculation depicts an annual risk quantification that allows a company to estimate the cost of a cyber breach to the organization itself, or from a breach caused by a third party.

- CISOs, CROs, and CFOs have an automated tool to communicate risk in quantitative, easy-to-understand business terms.
- The capacity to use an Open FAIR™ assessment at scale will elevate your vendor risk management program.
- A cyber rating alone lacks context related to business impact. FAIR helps fill the gaps by providing a proven standard risk-quantification methodology that can be leveraged with other frameworks.

HOW DO NASDAQ ORGANIZATIONS STACK UP AGAINST TODAY'S FORTUNE 100?

Free Download: Fortune 100 Ransomware Risk, Revealed