BlackBerry. Cybersecurity

Gartner Peer Insights.

Combating Ransomware

Ransomware is unfortunately the new normal for security leaders everywhere. It can lock out workstations, mobile devices, and networks with an unbreakable encryption key. Everyone is at risk, and impacts can be devastating for businesses of all sizes.

Gartner Peer Insights and BlackBerry surveyed 300 IT, engineering, and security leaders involved with cybersecurity purchasing decisions to understand how they view their current security posture, and their progress towards a prevention-first approach.

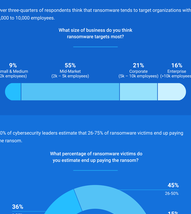
Key Insights

- Organizations of all shapes and sizes are at risk of ransomware attacks.
- Cybersecurity leaders lack confidence in their current security posture.
- The majority of cybersecurity teams lack full visibility, monitoring, and comprehensive incident response plans—leaving them vulnerable to attack.
- Artificial intelligence (AI) is a key security component for security leaders seeking endpoint protection.

Data collection: July 19 to September 1, 2022
Respondents: 300 IT, engineering, and security leaders

Organizations of all shapes and sizes are at risk of ransomware attacks.

Over one-third of respondents expect that the financial industry will be the most targeted by ransomware attacks in 2022.

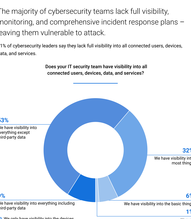


Stay up to date on ransomware attack protection and prevention.

LEARN MORE →

Over three-quarters of respondents think that ransomware tends to target organizations with 2,000 to 10,000 employees.

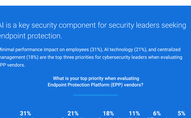
60% of cybersecurity leaders estimate that 26-75% of ransomware victims end up paying the ransom.



Cybersecurity leaders lack confidence in their current security postures.

Only 9% of cybersecurity leaders are very confident with their current security defense against cyberattacks.

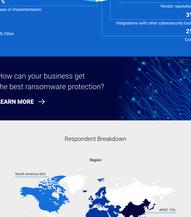
Only 11% of respondents say they feel very prepared for a ransomware attack.



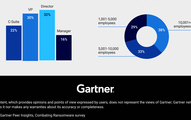
Additionally, nearly one-third of respondents have not implemented a prevention-first security posture.

The majority of cybersecurity teams lack full visibility, monitoring, and comprehensive incident response plans—leaving them vulnerable to attack.

91% of cybersecurity leaders say they lack full visibility into all connected users, devices, data, and services.



Less than one-third of respondents (29%) say they have a comprehensive incident response plan in place currently.



Additionally, 43% of respondents say their organization lacks 24x7 monitoring.

AI is a key security component for security leaders seeking endpoint protection.

Minimal performance impact on employees (31%), AI technology (21%), and centralized management (18%) are the top three priorities for cybersecurity leaders when evaluating EPP vendors.

Meanwhile, continuous threat and incident prevention (51%), AI/ML technologies (21%), and root cause analysis (11%) are the top three priorities when evaluating EDR vendors.

How can your business get the best ransomware protection?

LEARN MORE →

Respondent Breakdown

Gartner.