BlackBerry
Intelligent Security. Everywhere.

Solution Brief

Ransomware Prevention and Remediation

Reduce Risks and Impacts of Ransomware Incidents

Introduction

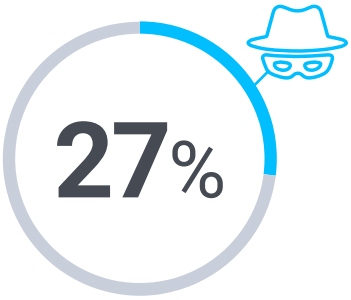
Ransomware is a form of extortionware that encrypts files to prevent victims from accessing their systems and data. In many cases, encrypted files can only be recovered by purchasing a decryption key from the ransomware threat actor. If the victim doesn't respond promptly enough to the ransom demand, the attacker may increase the ransom amount or delete the decryption key, rendering the files impossible to retrieve.

While phishing remains the most common attack vector, threat actors have introduced tactics, techniques, and procedures that don't require a victim to click on a malicious link or open a weaponized document to become infected. Instead, they are utilizing exploits, such as Eternal Blue, and uncommon programming languages and obscure data formats[1] to deposit ransomware directly on to victims' systems, thereby acquiring the persistent access they need to exchange encryption keys and process payments. Attacks like these are designed to evade network security controls capable of detecting and interdicting suspect traffic that would otherwise flow between infected systems and external command and control (C2) servers.

Increasingly, threat actors are also exfiltrating and threatening to expose victims' data, or to notify regulatory authorities, if their ransom demands are not met. In December 2019, for example, the Maze ransomware group began posting excerpts of data stolen from purported victims on a dedicated website.[2]

Although law enforcement advises victims not to pay, many firms will do so anyway based on the degree to which their operations are impaired, the potential impact on customers and shareholders, the relative costs of recovery and cleanup, and the extent to which exposure of data could subject the organization to regulatory penalties or damage its brand or reputation.

there will be a ransomware attack on businesses by the end of 2021.

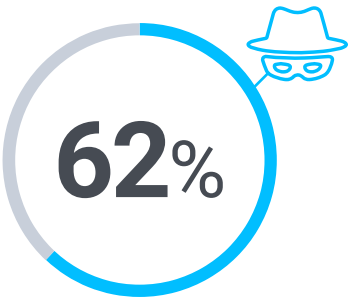


of all malware-related security incidents are ransomware

Business Challenge

Today, ransomware is big business for nation-state actors and cyber-criminal organizations alike, accounting for 27%[3] of all malware-related security incidents. Consider these troubling statistics:

- There will be a ransomware attack on businesses every 11 seconds by the end of 2021[4]. Every 40 seconds, one of those attacks will prove successful.[5]
- 62% of the organizations responding to a 2020 Cyberthreat Defense Report[6] said they had been victimized by ransomware. 58% of those firms opted to pay the ransom, an increase of 13% over the year before.



of the organizations responding to a 2020 Cyberthreat Defense Report said they had been victimized by ransomware.

1 Threat Spotlight: Tycoon Ransomware Targets Education and Software Sectors
2 Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up
3 Verizon 2020 Data Breach Investigations Report
4 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
5 What It Means to Have A Culture of Cybersecurity
6 2020 Cyberthreat Defense Report

- The global damage costs of ransomware are projected to reach $20 billion in 2021[7], a 300% increase since the $5 billion forecast for 2017. This includes not only ransom payouts, but also costs for recovery and remediation, lost productivity, reputational harm, and more.

Despite the known risks, many firms remain poorly prepared for a ransomware attack or its aftermath. According to an NTT Security survey[8]:

- One-third of respondents would rather pay a ransom than make upfront security investments to prevent breaches from occurring.
- Only 58% of respondents have a formal security policy in place.
- 48% lack an incident response (IR) plan. Of those that do, only 57% know all the details.

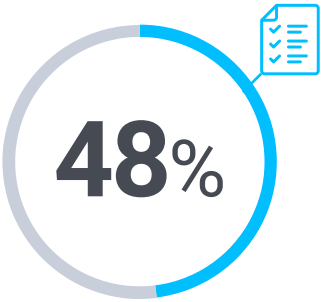
of respondents would rather pay a ransom than make upfront security investments to prevent breaches from occurring

BlackBerry Approach

BlackBerry Spark® Unified Endpoint Security Suite applications and BlackBerry Security Services solutions enable organizations to minimize risks from ransomware by transitioning from a reactive to a prevention-first security posture.

BlackBerry® Protect is an endpoint protection platform that utilizes advanced artificial intelligence (AI) technology combined with application and script control, memory protection, and device policy enforcement to stop malware, ransomware, fileless malware, and malicious scripts from compromising client systems and data. BlackBerry Protect prevents variants of WannaCry, Goldeneye, and Satan from executing with predictive mathematical models dating back to September 2015, long before the ransomware was detected in the wild. This third-party verified Predictive Advantage also extends to Emotet (816 days), GandCrab (795 days), Glassrat (548 days), PolyRansom (862 days), Sauron/Strider/Remsec (548 days), Zcryptor (182 days), and many more.

BlackBerry® Optics is an endpoint detection and response (EDR) solution that extends the threat prevention delivered by BlackBerry Protect with automated detection and response workflows ranging from collecting and forwarding endpoint telemetry data to taking systems offline. Workflows can be triggered by AI-based Context Analysis Engine (CAE) models, by custom rules, and by rules that leverage MITRE ATT&CK® tactics, techniques, and procedures of advanced persistent threats[9]. BlackBerry Optics also provides advanced capabilities for root cause analysis, smart threat hunting, and more.



of respondents lack an incident response (IR) plan.

7 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
8 NTT Report - Risk:Value 2019 Destination standstill. Are you asleep at the wheel?
9 BlackBerry Outperforms on the MITRE ATT&CK Framework Testing

Incident Response and Forensics Consulting Engagements conducted by BlackBerry Security Services IR teams provide the expert support and direction organizations need to investigate, contain, and remediate ransomware and other security breaches, and prevent them from recurring. By integrating AI into their proprietary tools and processes, BlackBerry teams produce preliminary results quickly. Detection, forensic analysis, and containment of ransomware and advanced persistent threats can begin within hours of completing initial data collection.

Attack Simulation Consulting Engagements conducted by BlackBerry Security Services Attack Simulation teams enable organizations to identify critical gaps in their prevention, detection, and response capabilities by testing and exercising their defenses under realistic conditions. Breach Simulations are a good fit for organizations that want to exercise their defensive capabilities, validate their security assumptions, and identify gaps in their security posture. Adversary Simulations are a good fit for organizations that want to acquire experience in detecting and responding to attacks by real-world threat actor groups that are actively targeting their industry.

BlackBerry® Guard is a subscription-based managed detection and response offering that leverages BlackBerry Protect, BlackBerry Optics, and the 24x7 support of a world-class team of BlackBerry incident response and prevention experts. BlackBerry Guard enables security teams to focus on key security initiatives instead of recovering from breaches.

To Learn More

Click here to learn more about BlackBerry's portfolio of ransomware prevention and remediation solutions or call **+1-888-808-3119** for immediate assistance.

Expected Benefits

BlackBerry's portfolio of ransomware software and service solutions enable organizations to:

- **Minimize incidents** by preventing ransomware from executing and spreading via automated detection, response, and remediation routines that aid in proactive threat hunting and root cause analysis.
- **Minimize risk exposure** by obtaining the expert guidance and support that CISOs and security teams need to identify and close gaps in their security fabric, harden their cyber defenses, implement robust processes for incident response, and transition efficiently from a reactive to a prevention-first security posture.
- **Respond rapidly to ransomware incidents**. The wait time for a mid-tier provider or large consulting firm to respond to a breach can stretch into weeks, allowing damage to spread and driving up the costs of recovery and cleanup. BlackBerry ransomware experts are available at a moment's notice to deliver consistent, best-in-class services.
- **Recover rapidly.** BlackBerry was one of only six companies identified that can help organizations recover from ransomware attacks in *Forrester's Guide To Paying Ransomware*.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

MKTG20-0504 | 200923