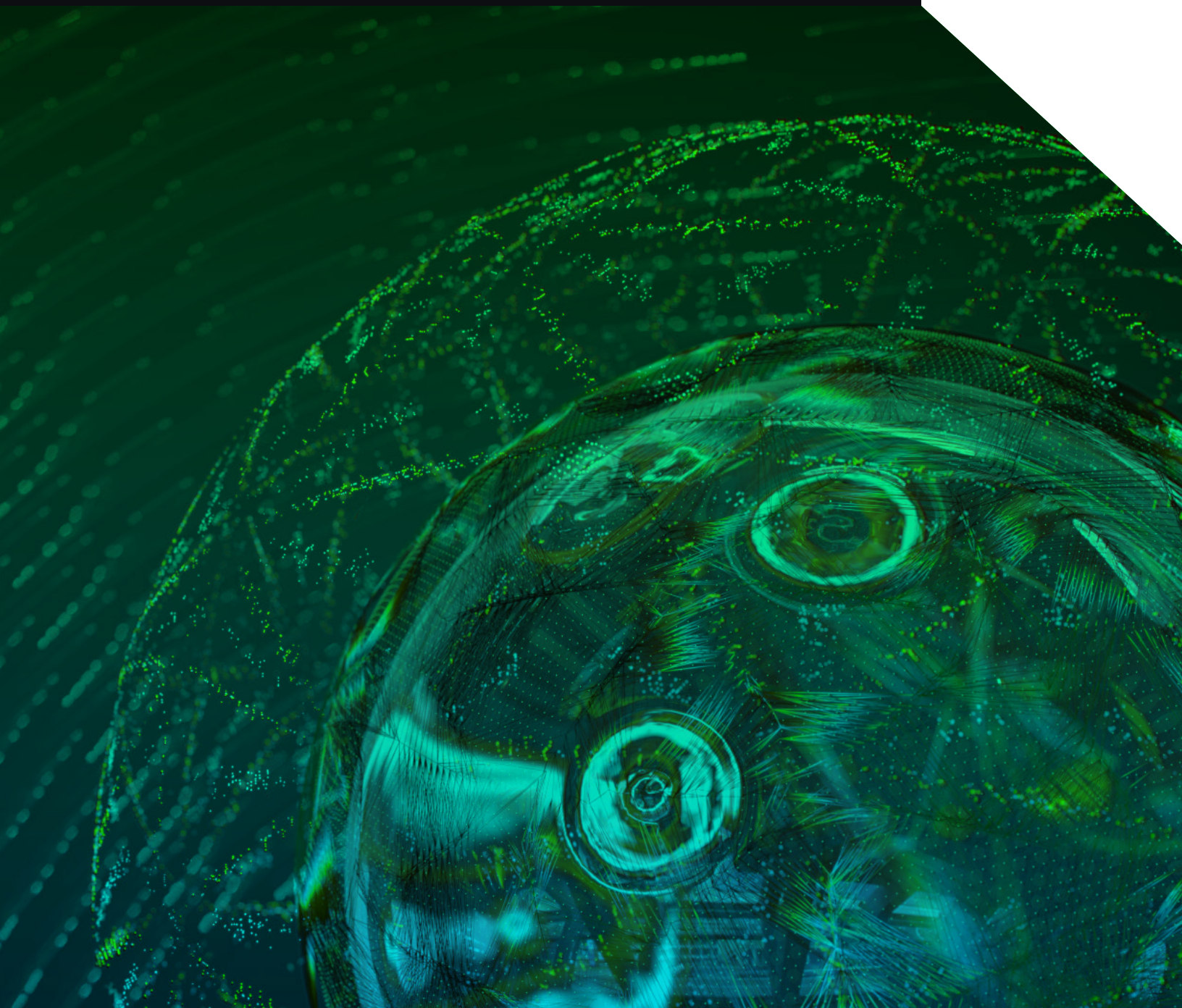
BlackBerry | CYLANCE®

SOLUTION BRIEF

Ransomware Remediation and Prevention



Ransomware is a form of extortionware that encrypts files in order 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 entirely, making the files virtually impossible to retrieve. Although law enforcement advises victims not to pay, many organizations will do so anyway based on business factors that include the degree to which operations are impaired, the potential impact on customers and shareholders, the relative costs of recovery and cleanup, and whether the threatened exposure of data could damage the organization's brand or reputation.

Business Challenge

Today, ransomware is big business for nation-state actors and cyber criminal organizations alike. Consider these troubling statistics:

- There will be a ransomware attack on businesses every 14 seconds by the end of 2019[1]. Every 40 seconds, one of those attacks will prove successful[2].
- Ransomware volume has increased by 350% since 2016[1]. Ransomware now accounts for nearly 24% of malware-related security incidents[3].

1 Global Ransomware Damage Costs Predicted to Hit $11.5 Billion By 2019. Cybersecurity Ventures.
2 What It Means to Have A Culture of Cybersecurity. Forbes Technology Council 09-21-17.
3 Verizon 2019 Data Breach Investigations Report.

- The global damage costs of ransomware are projected to reach $11.5 Billion in 2019[4]. 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.

- One third of the respondents to an NTT Security survey reported they would rather pay a ransom than make upfront security investments to prevent breaches from occurring. Another 15% were unsure[5].
- A quarter of the respondents to a 2018 Telstra study[6] either didn't have, or didn't know if they had, an incident response plan in place.

BlackBerry Cylance Approach

BlackBerry Cylance offers a native AI platform and portfolio of consulting services solutions that help organizations minimize their risks of a ransomware breach by transitioning from a reactive to a prevention-first security posture.

The BlackBerry Cylance Native AI Platform

CylancePROTECT® delivers industry-leading malware prevention powered by artificial intelligence, combined with application and script control, memory protection, and device policy enforcement to prevent successful cyber attacks. Without the use of signatures or need to stream data to the cloud, CylancePROTECT delivers protection against common threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and many other attack vectors, no matter where the endpoint resides.

CylanceOPTICS™ is an EDR solution that extends the threat prevention delivered by CylancePROTECT by using artificial intelligence to prevent security incidents. CylanceOPTICS provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities. Unlike many other EDR products, CylanceOPTICS and its true AI incident prevention are designed to run on endpoints. This lightweight architecture means organizations can adopt EDR capabilities quickly and affordably.

Cylance Consulting Services Solutions[7]

Through its Cylance Consulting division, BlackBerry Cylance offers two complementary consulting services engagements to help organizations minimize the risks and impacts of a ransomware incident.

- Proactive Prevention and Readiness services:
  - Leverage artificial intelligence to allow predictive, autonomous, pre-execution prevention

4 Global Ransomware Damage Costs Predicted to Hit $11.5 Billion By 2019. Cybersecurity Ventures.
5 NTT 2018 Risk: Value Report Executive Summary: Prevention Is Better Than Cure.
6 Telstra Security Report 2018.
7 The descriptive copy that follows is drawn from Cylance collateral entitled, "Ransomware Prevention & Remediation. Don't be the next victim."

- Provide world-renowned, highly sought after, knowledgeable consultants with the expertise to facilitate remediation of a ransomware attack
- Impart wisdom *before* the attack occurs to ensure the best preparation preventative technologies and workflows are in place

- Incident Response, Rapid Containment, and Risk Reduction services provide:
  - Access to experts who complete hundreds of IR engagements each year
  - Custom-developed tools to address today's advanced ransomware
  - Structured and proprietary response workflows to rapidly identify and contain campaigns

In fact, BlackBerry Cylance was recognized and recommended by Forrester as one of only six firms who specialize in ransomware in their recent report *Forrester's Guide To Paying Ransomware*.

Expected Benefits

BlackBerry Cylance's portfolio of ransomware solutions enable organizations to:

- Minimize incidents by preventing the execution of ransomware, including all variants of WannaCry, Goldeneye, and Satan, 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.
- Stop ransomware from spreading and inflicting damage via automated detection, response, and remediation routines that aid in proactive threat hunting and root cause analysis. These range from collecting and consolidating forensic data to terminating a compromised device's network connectivity.
- Obtain the expert guidance and support 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 containment, and transition efficiently from a reactive to a prevention-first security posture.

To learn more about how BlackBerry Cylance can help your organization to successfully prevent and mitigate ransomware, visit www.cylance.com/ransomware.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 0468-20190702