SECURITY SERVICES

TECH SPOTLIGHT SERIES

INNOVATION IN GOVERNMENT®

ABOUT VENDOR

BlackBerry 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. 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.

RESOURCES

Solution Brief
Incident Response Use Case
carah.io/BlackBerry-Security-Response

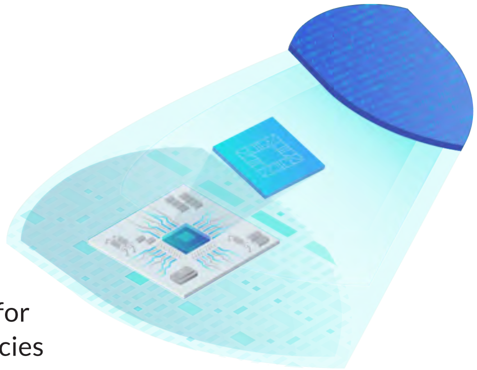
Data Sheet
Compromise Assessment
carah.io/BlackBerry-Security-Compromise

Solution Brief
BlackBerry Guard
carah.io/BlackBerry-Security-Guard

Data Sheet
Incident Response and Forensics
carah.io/BlackBerry-Security-Forensics

White Paper
Artificial Intelligence: The Platform of Choice
carah.io/BlackBerry-Security-Platform

BlackBerry Security Services



TECHNICAL SUMMARY

Government agencies are always tempting targets for bad actors, including nation states. Therefore, agencies must consider security as a top priority. However, limited resources and a widening cyber-skills gap leave critical public sector data and assets vulnerable to attack. Even with the best prevention, agencies may have compromises that should be identified, contained, and remediated.

When employing BlackBerry® Security Services, networks are assessed for the full spectrum of cybersecurity challenges to identify vulnerabilities introduced by missing patches, poor setups, remote access issues, and other problems. Clients are provided with a detailed list of recommendations along with risk rankings, most being product agnostic and independent, to fix identified problems. BlackBerry experts can then assist with the implementation of changes to construct a strong and effective security posture with prevention-first methodologies.

THE SOLUTION

Penetration Testing: BlackBerry has spent decades protecting the most critical systems, networks, and applications in the world. The BlackBerry Penetration Testing team can do everything from regulatory penetration testing to custom-tailored adversary simulation. BlackBerry Security Services are scalable, working with organizations ranging in size from 50 to over 400,000 endpoints, and take a manual approach, focusing on identifying true risks.

Compromise Assessment: The BlackBerry team can rapidly determine if an organization is currently compromised or shows signs of past compromise or security incidents. This assists organizations in identifying environmental risks, current or previous security incidents, and potential threat actor activity. It's a system-by-system analysis that combs through environments and x-rays each system for any evidence of compromise. Clients are provided with a detailed report of any threats found and suggestions to prevent future attacks.

Incident Response: BlackBerry experts can enhance an organization's incident handling and response capabilities while supporting the development of robust processes to minimize the impact of breaches. The BlackBerry team is particularly fast at identifying a problem and developing a containment plan. The data collection process just takes a few minutes on each host, allowing analysts to examine the entire environment and identify impacted systems. Having a BlackBerry Incident Response Retainer — a contractual agreement for help in the face of an incident — can help by greatly speeding your time to resolution. BlackBerry Security Services offers four levels of Incident Response Retainer with varying levels of prepaid hours to suit your needs and budget.

BlackBerry. carahsoft.

CERTIFICATIONS

- FedRAMP
- Certificate of Networthiness (CoN) and Authority to Operate (ATO)
- FIPS 140-2
- Common Criteria EAL 4 +
- NATO Restricted
- Department of Defense Information Network (DoDIN) Approval - UEM

CONTRACTS

- GSA
- ITES-2

THE BLACKBERRY DIFFERENCE

Antivirus Protection: Traditional antivirus are reactive, relying on signature files and requiring daily updates. This approach makes organizations especially vulnerable to zero-day attacks and threats that alter themselves too quickly for signature updates. BlackBerry® Protect, driven by Cylance ® AI, provides a different approach to endpoint security; prevention. Cylance AI has been trained to identify common attributes of malicious files, accurately identifying malware that has never been seen before, on average 25 months in advance of being seen in the wild[1]. BlackBerry Protect shields clients from attacks like DarkSide, HAFNIUM, REvil, and ChaChi that effectively halted the operations of millions of organizations worldwide.

Dedicated Team: Having worked with government clients at the highest levels, BlackBerry experts understand additional needs based on regulations or tight deadlines. The BlackBerry Security Services team will dedicate both an engagement manager and a technical lead to each project, building in multiple levels of oversight and providing multiple escalation paths so employees can get clarification. This dedication earned BlackBerry first place in the 2021 SOC X World Championship, a competition during which 50 global Security Operations Center (SOC) and Incident Response (IR) teams compete to show their best capabilities against real attacks. The team also won first and third place in the 2021 OpenSOC Network Defense Range (NDR) at DEF CON 29.

Customized Approach: Many vendors rely on automated tools that typically detect 20% to 40% of threats. Experienced BlackBerry experts follow a detailed methodology, using a manual process to uncover issues difficult to detect. For example, during a red team attack simulation, BlackBerry experts accurately mimic a sophisticated human-based attack centered on intelligence that identifies an organization's defenses and formulates a custom attack, simulating a sophisticated attacker who spends time and resources planning a specific attack.

BLACKBERRY GOVERNMENT CUSTOMER SUCCESS

BlackBerry Security Services works with a wide variety of civilian and military government organizations, as well as state and local agencies. For example, Cylance AI technology was used to track and identify breaches in the U.S. Office of Personnel Management (OPM)[2]. OPM handles sensitive data for thousands of federal employees. In 2015, OPM saw large unauthorized data transfers occurring, but the initial incident team OPM deployed had difficulty identifying the attack vector. Finally, when the Cylance AI technology was implemented, the malware was identified and shutdown within 24 hours and the damage to OPM's systems was then mitigated through a joint effort with the OPM team.

FOOTNOTES:

[1] SE Labs Intelligent Testing, Predictive Malware Response Test, March 2018

[2] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

© 2021 Carahsoft Technology Corp.