BlackBerry
Intelligent Security. Everywhere.

Solution Brief

Incident Response

Expert Support for Investigating, Containing, and Remediating Security Breaches

Business Challenge

According to an IBM study[1], the "vast majority" of organizations today are unprepared to respond effectively to a serious security incident. Most often, this is due to chronic resource issues and inadequate planning.

- In 2019, it took organizations an average of 206 days to identify a data breach and another 73 days to contain it, a nearly 5% increase over the year before.[2]
- The total average cost of a data breach for the largest organizations was $5.11 million (about $204 per employee). For smaller organizations, the average was $2.65 million (about $3,533 per employee). The higher proportional costs for smaller firms can "hamper their ability to recover financially from the incident".[3]
- Less than a quarter of those surveyed have a cybersecurity incident response plan (CSIRP) that is applied consistently across the entire enterprise. Another 49% say they either don't have a CSIRP at all or that their CSIRP is informal or "ad hoc".[4]
- Of those organizations that do have CSIRPs, more than half fail to test and maintain them on a regular basis due to ongoing team staffing issues.[5]

There is no quick fix to resolve these challenges. The acute global shortage of experienced cybersecurity talent shows no signs of abating. Overstressed security workers contending with alert fatigue struggle to keep systems patched and updated, leaving organizations vulnerable to attacks that could otherwise be easily prevented. Attempts to close gaps by adding security layers can result in a defense infrastructure that is overly complex and difficult to manage. Meanwhile, threat actors continue to innovate, developing tactics, techniques, and procedures (TTPs) designed explicitly to evade legacy signature-based defenses by obfuscating malicious code, utilizing polymorphism, or exploiting dozens of other techniques.

BlackBerry® Security Services stands ready to help, providing artificial intelligence (AI) technology, proven expertise, and strategic support services that empower organizations to efficiently investigate, contain, and remediate security breaches. There is no requirement to be an existing BlackBerry customer. BlackBerry Security Services are available to every organization.

In 2019, it took organizations an average of 206 days to identify a data breach and another 73 days to contain it, a nearly 5% increase over the year before.

Source: 2019 Cost of a Data Breach Report. IBM Security

1 IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them
2 2019 Cost of a Data Breach Report. IBM Security
3 2019 Cost of a Data Breach Report. IBM Security
4 Fourth Annual Study on The Cyber Resilient Organization
5 IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them

BlackBerry Security Services Approach To Incident Response

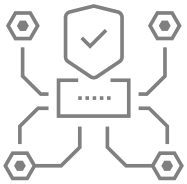
Every BlackBerry Security Services Incident Response (IR) engagement proceeds through five distinct phases that fully-leverage BlackBerry AI technology and the expertise of its global IR teams. These five phases run concurrently, enabling dynamic, rapid responses to evolving incidents, and shortening the critical path to containment.

During the kickoff meeting, the BlackBerry and client IR teams align to scope the engagement, review the initial indicators of compromise (IOCs), and develop a project plan and preliminary timeline. At the conclusion of the meeting, the following will have been established:

- How the attack was initially detected
- The data that's been collected
- A preliminary threat profile
- Actions taken so far to mitigate the damage
- The client's project priorities and goals

PHASE 1

Deployment



When an incident occurs, it's essential to identify all IOCs as quickly as possible. To begin, the BlackBerry IR team provides the client with a suite of software tools for collecting forensic data and scanning for malware across the enterprise. This includes a set of lightweight triage scripts and the unified agile agent for BlackBerry® Protect and BlackBerry® Optics. The tool installation and execution processes are transparent to end-users since the agent consumes minimal system resources and the scripts run for only five to fifteen minutes before terminating.

BlackBerry Protect is an enterprise-class endpoint protection solution that utilizes AI to prevent malware from executing with proven 99.1% efficacy. On many engagements, activating BlackBerry Protect in auto-quarantine mode can halt an ongoing incursion immediately by neutralizing malware on infected systems. BlackBerry Protect also includes security controls that thwart script-based, fileless, memory, and external device-based attacks.

BlackBerry Optics is an AI-driven endpoint detection and response (EDR) solution that provides advanced capabilities for root cause analysis, smart threat hunting, and initiating playbook-driven automated responses that prevent widespread security incidents. Working together, BlackBerry Protect and BlackBerry Optics accelerate the process of resolving incidents and remediating compromised systems.

BlackBerry Protect is an enterprise-class endpoint protection solution that utilizes AI to prevent malware from executing with proven 99.1% efficacy.

PHASE 2

Collection

Once deployment is complete, the BlackBerry IR team specifies the raw data it will need for analysis and assists the client with collection. This typically includes filesystem metadata from endpoints, log data from network devices, event and alert data from ancillary security systems, and more. Next, the BlackBerry team employs proprietary cloud-based tools and methodologies to normalize, contextualize, enrich, and format the data. The resulting forensic artifacts are processed with a proprietary analytics engine and stored securely in the BlackBerry cloud for off-site analysis.

PHASE 3

Analysis

During the analysis phase, the BlackBerry team utilizes:

- BlackBerry Protect to detect and terminate malware, malicious PowerShell scripts, memory injection attacks, and more.
- BlackBerry Optics to hunt for evidence of data exfiltration and sabotage, command and control activities, user authentication abnormalities, malware persistence mechanisms, anomalous network host and application configurations, and more.
- BlackBerry's proprietary threat intelligence database to search client data for known-bad IOCs.

The resulting findings are then prioritized, shared with the client, and incorporated into detailed action plans for efficient remediation and cleanup.

PHASE 4

Remediation

BlackBerry Security Services IR remediation action plans specify the sequence of steps required to terminate the breach and prevent it from recurring. An advanced persistent threat (APT), for example, cannot be resolved simply by deleting malicious files and terminating running processes. Persistence mechanisms must be disabled first, such as scheduled tasks that load malicious code concealed within the system registry. BlackBerry Optics plays an essential role by initiating automated playbook rulesets to perform these actions in the proper sequence and gather environmental data to verify that no artifacts remain. General-purpose rules may also be created to thwart common threat actor TTPs, such as misusing the Windows Event Viewer (wevutil) to evade detection by clearing system logs or shutting down the logging service.

PHASE 5

Reporting

At the conclusion of the IR engagement, the client receives a two-part report. Part 1 is an executive summary that reviews the key findings in non-technical terms appropriate for business stakeholders. Part 2 details every step in the investigation and lists the artifacts discovered, the resulting IOCs, the initial infection vector, the scope and spread of the intrusion, the effects on the environment, and the actions taken to neutralize them. The report concludes with both tactical and strategic recommendations, not only for preventing similar attacks in the future, but also for strengthening the client's overall security posture. These include such things as suggesting additional employee training after a phishing attack, implementing specific upgrades to vulnerable systems, and taking all external RDP system access offline.

Deployment

BlackBerry Protect and BlackBerry Optics accelerate detection and response.

Collection

Methods are efficient, lightweight, and transparent to the business.

Analysis

World-renowned IR experts identify and scope IOCs quickly.

Remediation

BlackBerry Optics initiates automated remediation and cleanup plans.

Reporting

Documents business impacts, technical details, and security best practices.

Expected Business Benefits

The BlackBerry Security Services multi-faceted approach to IR offers clients several direct benefits.

- **Rapid Detection:** By integrating artificial intelligence (AI) into their tools and processes, BlackBerry IR teams produce preliminary results quickly. Detection and containment of ransomware and APTs can begin within hours of completing data collection.
- **Rapid Response:** 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 Security Services IR experts are available at a moment's notice to deliver consistent, best-in-class services.

- **Rapid Remediation:** As soon as BlackBerry Protect is activated in auto-quarantine mode, malware will be prevented from executing on infected systems and spreading laterally across the network. BlackBerry Optics can then initiate a sequence of automated remediation responses that efficiently neutralize the threat and help clean up the environment.
- **Low-Touch Data Collection:** Data collection methods are efficient and transparent. For example, there is no need to dedicate hardware and appliances on host systems or at Internet egress points. Instead, the client is provided with BlackBerry Protect and BlackBerry Optics agile agent software to install on endpoints using their existing deployment methods. Alternately, the client can be furnished with lightweight scripts that run for two to five minutes on each endpoint and then terminate, leaving minimal artifacts behind.
- **Cost and Resource Efficiency:** Unless clients request otherwise, BlackBerry IR teams work remotely, eliminating costs for travel and on-site resources.
- **Prevention-First Defense:** At the conclusion of every BlackBerry Security Services IR engagement, clients have the option to purchase licenses for the BlackBerry Protect and BlackBerry Optics systems installed on their endpoints or subscribe to the BlackBerry® Guard managed detection and response service. In both cases, ThreatZero® consultants are available to help clients transition into the state of prevention by activating BlackBerry Protect security controls for malware prevention, memory exploit protection, device policy enforcement, and application and script control, in full blocking mode.

To Learn More

For more information about BlackBerry Security Services Incident Response and Forensics support, please request a consultation or call **+1-888-808-3119** for immediate assistance.

About BlackBerry Security Services

BlackBerry Security Services consulting engagements enable clients to secure their mission-critical operations and manage their endpoints, workspaces, and identities within a Zero Touch, Zero Trust architecture. Our consultants provide the in-depth knowledge and investigative experience organizations need to minimize their cyber risk exposure and defeat persistent, well-funded attacks. Working together, we help clients address the full spectrum of cybersecurity challenges and construct a strong and effective security posture utilizing prevention-first methodologies. Please visit our consulting landing zone for the complete list of BlackBerry Security Services solutions.

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

BlackBerry
Intelligent Security. Everywhere.

MKTG 20-0023 | 200722