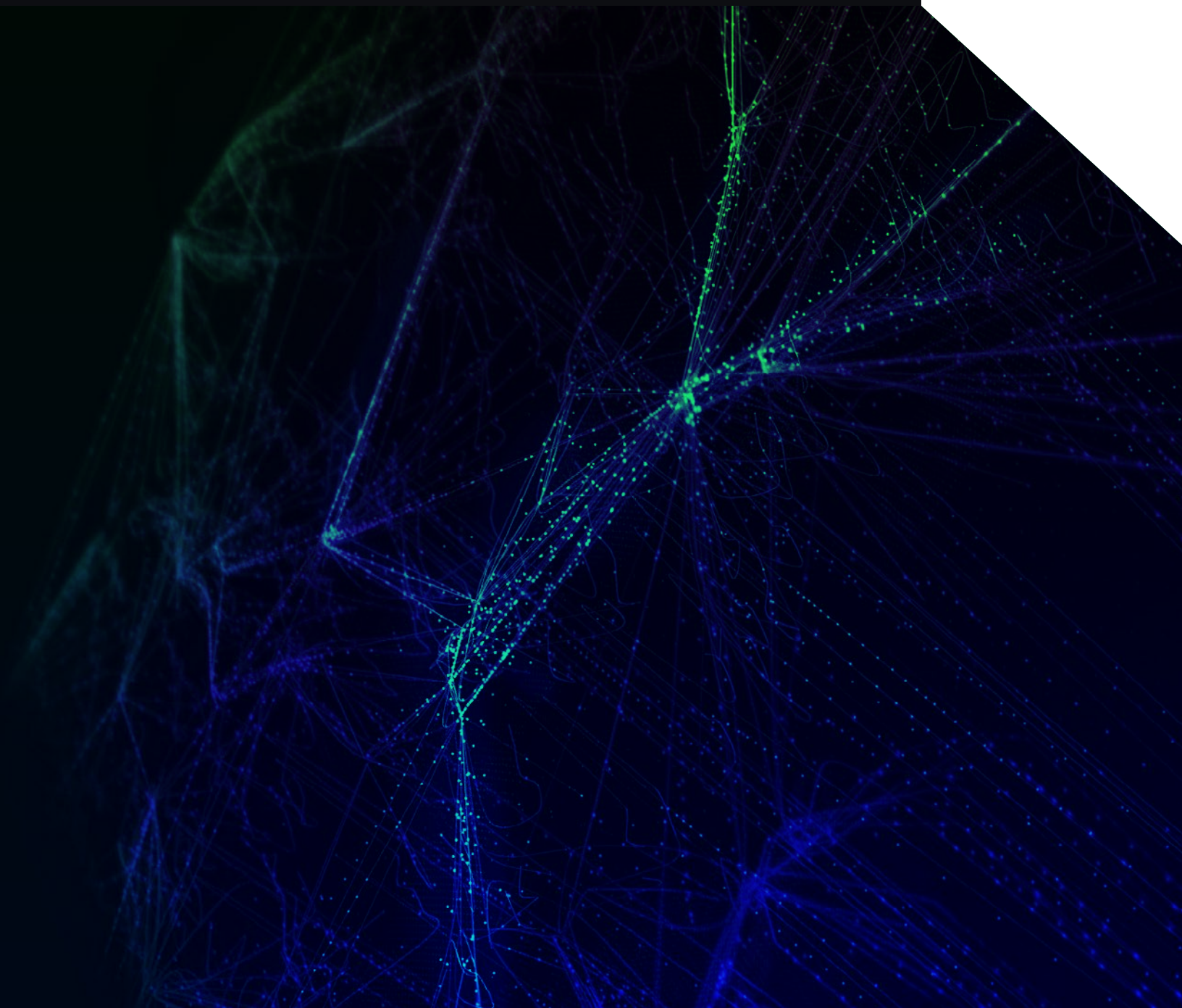
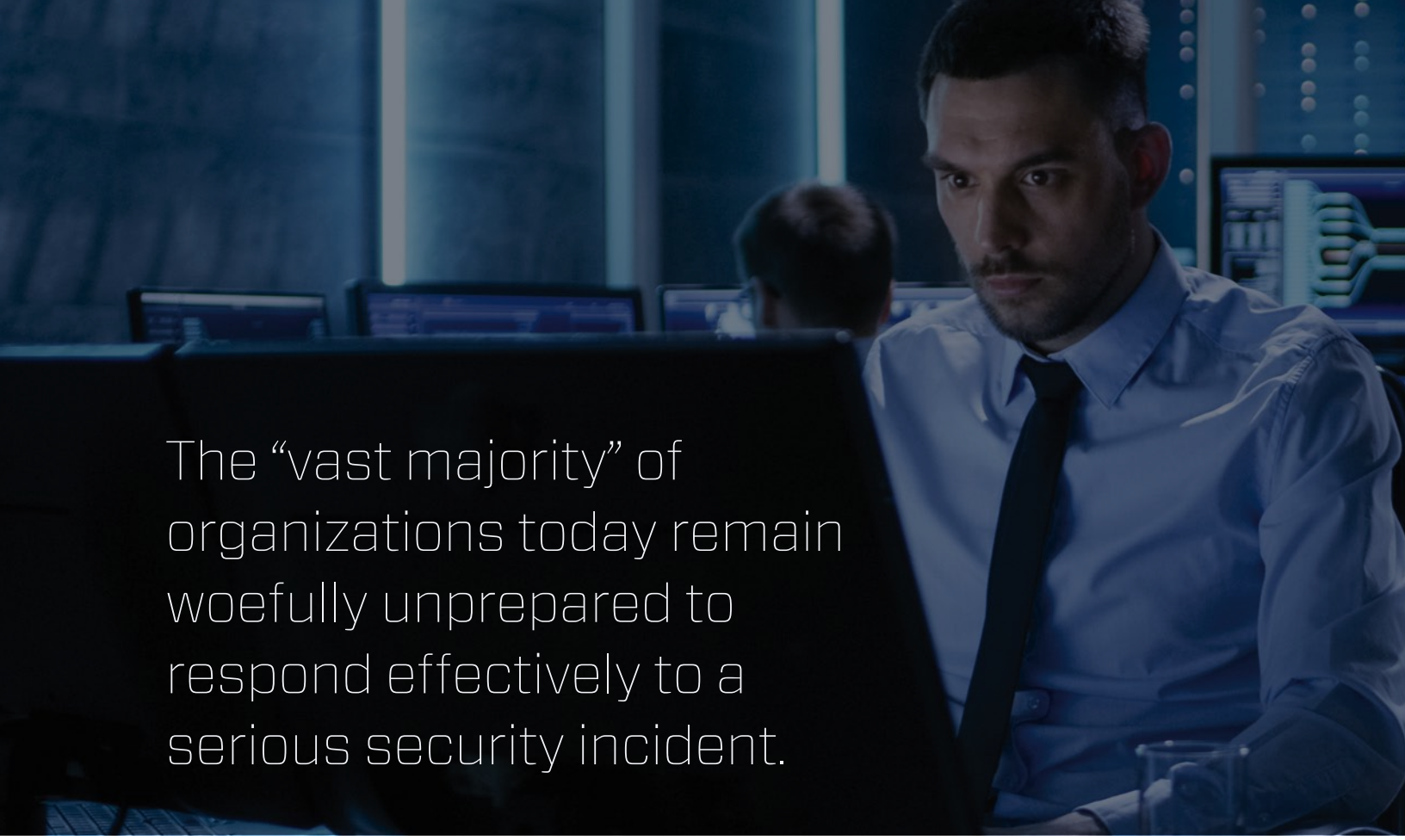
BlackBerry | CYLANCE®

SOLUTION BRIEF

Incident Response





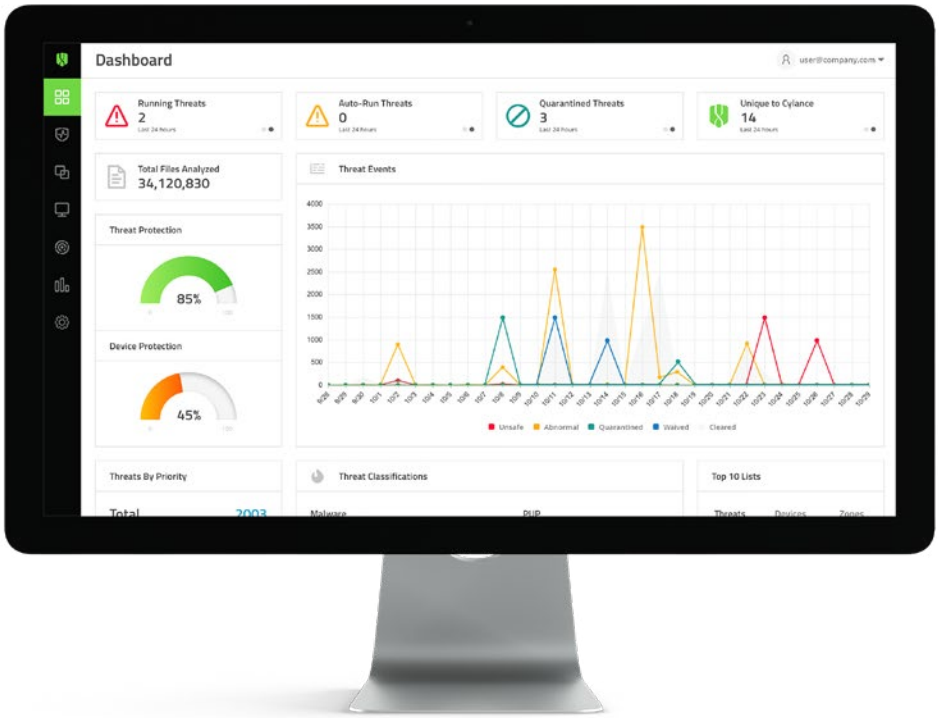
The “vast majority” of organizations today remain woefully unprepared to respond effectively to a serious security incident.

Business Challenge

According to an IBM study[1], the “vast majority” of organizations today remain woefully 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]

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



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

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 Cylance's consulting team stands ready to help. Our artificial intelligence (AI) technology, proven expertise, and strategic support services empower organizations to efficiently investigate, contain, and remediate security breaches.

BlackBerry Cylance Approach To Incident Response

Every IR engagement proceeds through five distinct phases that fully-leverage our native AI platform technology and the decades of security experience of our global IR teams. We begin with a kickoff meeting to scope the engagement, review the initial indicators of compromise (IOCs), develop a project plan and preliminary timeline, and align the BlackBerry Cylance's consulting team and customer IR teams. At the conclusion of the meeting, we will have established:

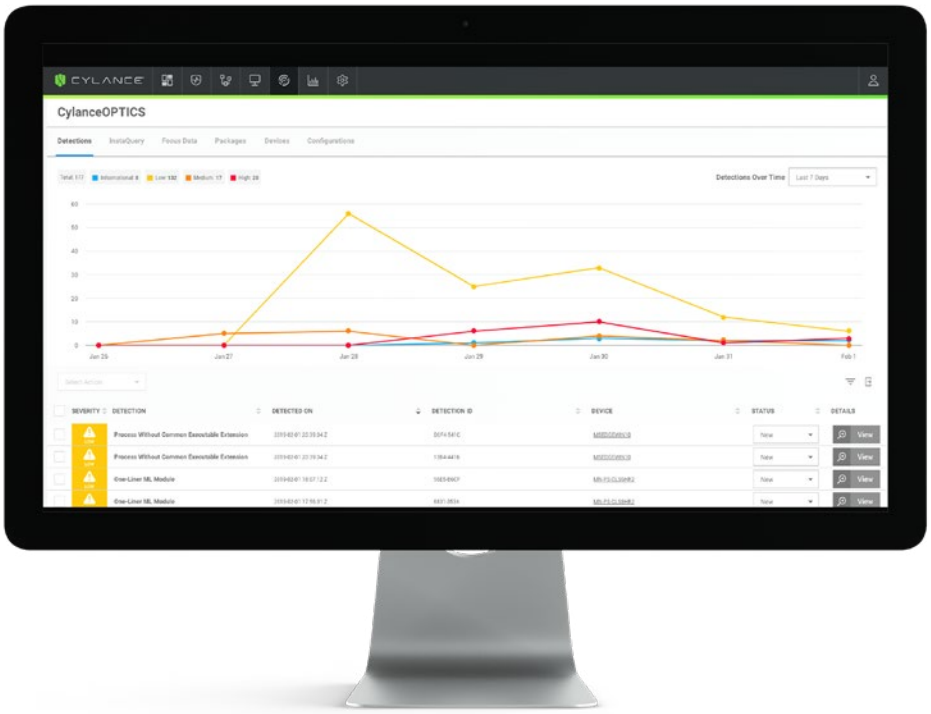
- How the attack was initially detected.
- The data that's been collected.
- A preliminary threat profile.
- Actions taken so far to mitigate the damage.
- The customer's project priorities and goals.

After that, we're ready to begin the deployment phase.

Phase 1: Deployment

When an incident occurs, it's essential to identify all IOCs as quickly as possible. This begins with deploying CylancePROTECT and CylanceOPTICS® on endpoints throughout the environment. Both solutions require minimal system resources to run efficiently.

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



CylanceOPTICS 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.

CylanceOPTICS 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, CylancePROTECT and CylanceOPTICS accelerate the process of resolving incidents and remediating compromised systems.

Phase 2: Collection

Once deployment is complete, our IR team specifies the raw data we will need for analysis and assists the customer 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, we utilize proprietary cloud-based tools and methodologies to normalize, contextualize, enrich, and format the data. All customer data is securely stored in the BlackBerry® Cylance® cloud for off-site analysis by our IR team.

Phase 3: Analysis

During the analysis phase, our IR team utilizes:

- CylancePROTECT to detect and terminate malware, malicious PowerShell scripts, memory injection attacks, and more.
- CylanceOPTICS 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.
- CylanceINFINITY™, our extensive threat intelligence database, to search customer data for evidence of known-bad IOCs. In many cases, CylanceINFINITY IOCs are so unique and specific that our team can attribute responsibility for an attack to a particular threat actor group.

Our findings are then prioritized, shared with the customer, and incorporated into detailed action plans for immediate remediation and cleanup.

Phase 4: Remediation

Our remediation action plans specify the particular 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. We must first disable the associated persistence mechanisms, such as a scheduled task that loads malicious code concealed within the system registry. CylanceOPTICS plays an essential role here by initiating automated playbook rulesets to perform these actions in the proper sequence and gather environmental data to verify that no artifacts

remain. We may also create general-purpose rules 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.

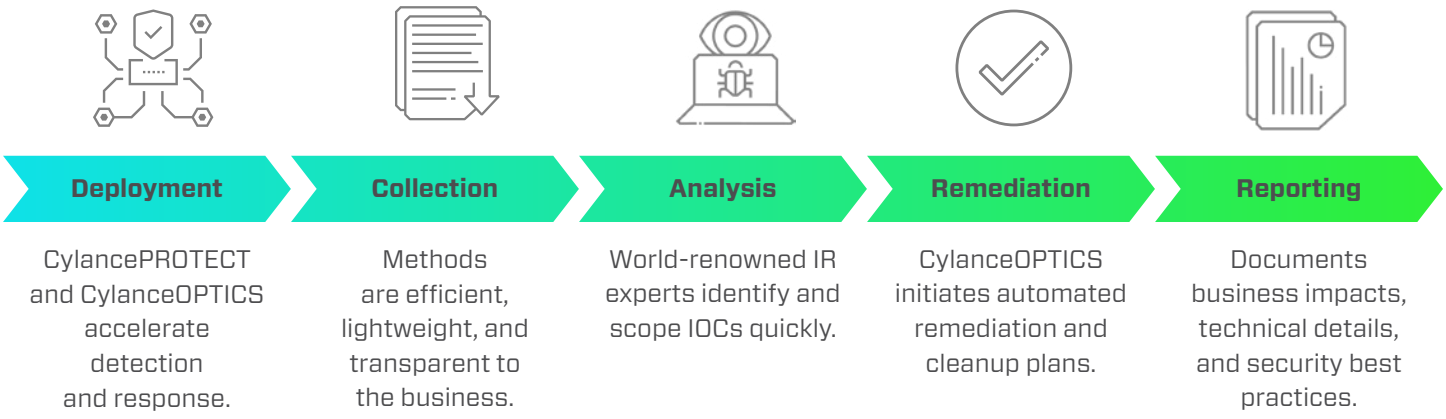
Phase 5: Reporting

At the conclusion of the IR engagement, we submit a two-part report. Part 1 is an executive summary that reviews our key findings in non-technical terms appropriate for business stakeholders. Part 2 details every step in our investigation and lists the artifacts we 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. We conclude with both tactical and strategic recommendations, not only for preventing similar attacks in the future, but also for strengthening the customer'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.

Expected Business Benefits

Our multi-faceted approach to IR offers customers several direct benefits.

- **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. Our world-renowned experts are available at a moment's notice to deliver consistent, best-in-class services anywhere in the world.
- **Low-Touch Data Collection.** Our data collection methods are efficient and transparent. For example, we don't require hardware or appliances at Internet egress points or on host systems. Instead, we provide CylancePROTECT and CylanceOPTICS agile agent software for clients to install on each endpoint utilizing their existing deployment methods. Alternately, we can provide lightweight scripts that run for two to five minutes on each endpoint and then terminate, leaving no artifacts behind.
- **Efficient with Costs and Resources.** Unless clients request otherwise, our IR teams work remotely, eliminating costly travel expenses, or the need for resources to be provided on-site.
- **Rapid Detection.** Our proven methodologies leverage AI for better and faster results. We typically identify and scope incidents within hours, rather than days, weeks, or months.
- **Rapid Remediation.** As soon as CylancePROTECT is deployed, malware will be prevented from executing on infected systems and from spreading laterally across the network. CylanceOPTICS can then initiate a sequence of automated remediation responses that efficiently neutralize the threat and clean up the environment.
- **Prevention-First Defense.** At the conclusion of an IR engagement, customers have the option to maintain their endpoint protection by purchasing one-year or three-year licenses for CylancePROTECT and CylanceOPTICS. Our ThreatZERO® consultants can help customers transition to a prevention-first security posture by fully enabling CylancePROTECT security controls for malware prevention, application and script control, memory protection, and device policy enforcement.



To Learn More

Whatever security challenge you may be facing, our team of experts can help. For more information about BlackBerry Cylance's consulting IR services, please visit our Emergency Incident Response and Containment web page or call +1-888-808-3119 for immediate assistance.

Our IR consulting services portfolio also includes:

- Incident Response Retainer Service
- Incident Readiness Assessment
- Incident Response Policy Review/Creation
- Incident Response Program Review/Development
- Incident Response Tabletop and War Game Exercise
- Incident Response Technical Training
- Forensic Investigation and Analysis
- Compromise Assessments
- Business Email (Office 365) Compromise Assessment
- Business Email Compromise Response and Investigation

Please visit our consulting landing zone for the complete list of BlackBerry Cylance's consulting solutions.

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.

BlackBerry CYLANCE

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

MKTG 20-0023-20200127