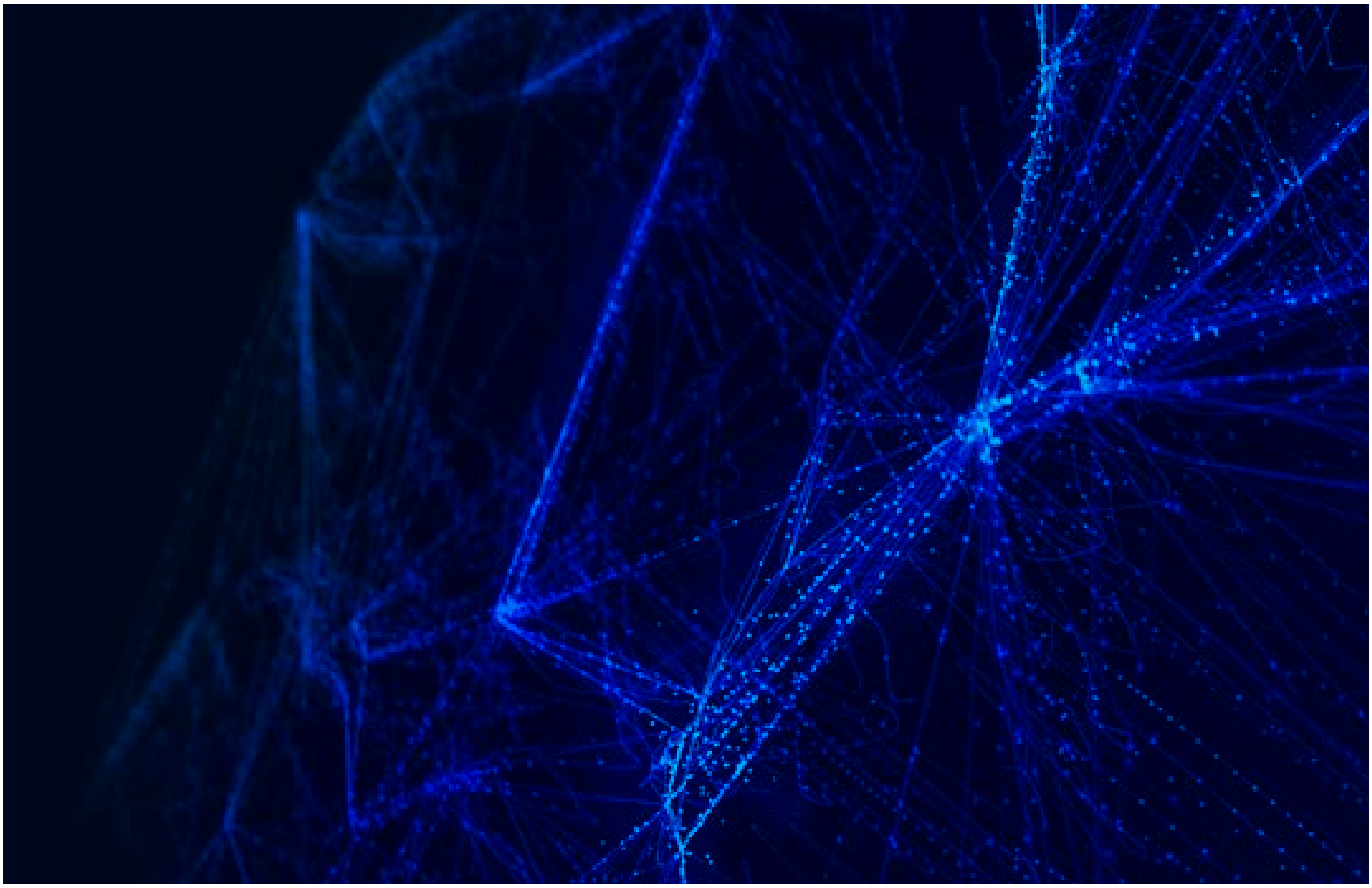
BlackBerry

Intelligent Security. Everywhere.

Solution Brief



ThreatZero Services

Optimize Your BlackBerry Security Solutions

Business Challenge

All too often, the expected benefits of an endpoint security investment are slow to materialize and near impossible to verify. Security teams quickly discover that the time and effort required to stand up the new solution are much greater than they were led to believe. Every step in the implementation process causes unexpected problems. Critical systems suddenly become unstable or unresponsive. Employees flood the support team with complaints. Analysts are deluged with cryptic alerts emanating from systems they only partially understand how to operate and manage. Project deadlines are stretched to the breaking point. And when the deployment finally ends, there may be little evidence of a significant improvement in the firm's cyber risk exposure. Where is the promised return on investment (ROI)?

At BlackBerry, we believe that the best way to reduce risks and accrue a significant ROI is to transition efficiently from a reactive to a prevention-first security posture. This cannot be accomplished simply by decommissioning a legacy signature-based product and installing BlackBerry® Protect and BlackBerry® Optics. New endpoint security policies must be created that reflect the evolving needs of the business and its IT infrastructure. New security controls must be implemented that are effective against current and emerging adversary tactics, techniques, and procedures (TTPs).

This requires an in-depth understanding of the BlackBerry native artificial intelligence (AI) platform and a firm grasp of security best practices. The implementation process must be logical, efficient, transparent to employees, and frictionless for the business. Finally, achieving the state of prevention must be a provable event that can be demonstrated with objective metrics. It's precisely this expertise and field-proven methodology that BlackBerry consultants bring to every ThreatZero engagement.

> Every step in the implementation process causes unexpected problems.

The BlackBerry Consulting Approach

ThreatZero implementations enable clients to achieve a state of prevention quickly without overburdening internal security teams or disrupting key systems and business processes. This milestone occurs when all project goals have been met and objective measures of endpoint protection reach a ThreatZero report card score of 95% or better. This score is a composite of several key metrics that include:

- The percentage of endpoints running BlackBerry Protect with malware prevention activated in auto-quarantine mode.
- The extent to which BlackBerry Protect script and memory exploitation controls have been enabled in full blocking mode.
- The percentage of endpoints with BlackBerry Optics enabled and optimized based on ThreatZero best practices.

The report card also functions as a set of key performance indicators that CISOs can monitor on an ongoing basis to assess the organization's cyber risk exposure and incident preparedness.

ThreatZero Engagement Process

Every ThreatZero engagement proceeds through three distinct phases that fully leverage BlackBerry's native AI platform technology and the expertise of the company's ThreatZero consultants. The process begins with a kickoff meeting to set expectations and align the BlackBerry and client implementation teams. This includes:

- Developing a preliminary project plan and timeline.
- Reviewing options for deploying BlackBerry agile agent technology.
- BlackBerry Protect management console installation and training.
- BlackBerry Optics installation and training.
- A briefing on best practices approaches for achieving the state of prevention.

Once agents are deployed on the client's endpoints, the ThreatZero team begins operationalizing BlackBerry Protect by initiating a sequence of passive to active policy moves.

- **Passive move:** Enable a security control in scanning mode, capture and categorize all resulting alerts, and then recommend actions to be taken for each of them.
- **Decision review:** Review findings and recommendations with the client implementation team to ensure that only malicious files or activities are targeted for prevention.
- **Active move:** Configure security policies in theBlackBerry Protect console that automate and enable these prevention decisions.

This process repeats three times, once for each of the three ThreatZero phases.

Phase 1

Malware Prevention

In this phase, the goal is to baseline the environment and identify existing threats by enabling BlackBerry Protect malware prevention capabilities in alert-only mode. Analysis results are reviewed with the client to identify files that appear to be suspect but may actually be utilized for legitimate business purposes. Once this process concludes, the console is used to incorporate all necessary exceptions into device security policies and enable BlackBerry Protect malware prevention in auto-quarantine mode.

Phase 2

Memory Exploit Protection

In this phase, the console is monitored for evidence of potential memory exploits, and findings and recommendations are documented. Once all memory exploit prevention decisions have been made, the necessary security policies are configured in the console and memory protection in full blocking mode is enabled. It's customary, at this point, for the client and ThreatZero teams to monitor the environment for a week or more to ensure that memory exploit protection is effective and transparent to end-users and the client's core business processes.

Phase 3

BlackBerry Protect Script Control and BlackBerry Optics Optimization

Many BlackBerry clients utilize custom scripts to perform routine business functions. In this phase, all BlackBerry Protect script control alerts are captured and prevention recommendations are provided to the client. Once the review is completed, device security policies are updated to permit all legitimate scripts to execute and then script control in full blocking mode is enabled. As occurred with memory protection, the environment is closely monitored for a week or more to ensure that script controls are working as expected without any negative impacts on end-users or the client's core business processes. In this phase, best practice optimizations for BlackBerry Optics endpoint detection and response (EDR) features are applied by tuning the Context Analysis Engine (CAE). The client is also empowered to create Insta-Queries that capture forensic data, and implement BlackBerry Optics playbooks that initiate automated incident responses whenever static or AI-based rulesets are triggered.

Once all tasks are completed and the state of prevention is achieved, the ThreatZero engagement is concluded with a final review meeting and closeout call.

> ThreatZero implementations enable clients to achieve the state of prevention quickly without overburdening internal security teams or disrupting key systems and business processes.

Expected Business Benefits

Clients typically accrue the following business benefits from a ThreatZero engagement:

- **Field-proven methodology:** BlackBerry has helped thousands of companies of all sizes and in virtually every industry sector achieve a state of prevention quickly and efficiently with minimal impact on their internal systems and resources.
- **Provable prevention:** ThreatZero report cards track the key metrics that determine when a state of prevention is achieved.

Phase 1	Phase 2	Phase 3
Malware Prevention Review alerts about suspect files before enabling malware prevention in auto-quarantine mode.	**Memory Exploit Protection** Review alerts about suspect memory operations before enabling memory exploit protection in full blocking mode.	**BlackBerry Protect Script Control and BlackBerry Optics Optimization** Review alerts about suspect script operations before enabling script control in full blocking mode, and apply best practice optimizations for BlackBerry Optics.

- **Access to world-class consultants:** BlackBerry teams are composed exclusively of senior-level security consultants that provide the technical expertise and personalized white glove service organizations need to maximize their endpoint security ROI.
- **Broad spectrum protection:** Every ThreatZero implementation addresses the full spectrum of file-based and fileless threat vectors.
- **Full lifecycle project management:** A dedicated ThreatZero engagement manager helps ensure that every implementation proceeds efficiently by coordinating resources, sharing best practices, training security teams, and tracking progress goals in weekly status meetings. The engagement manager can also assist the client in remediating any pre-existing security threats that may surface during the implementation process.
- **Cost-efficiency:** Unless clients request otherwise, ThreatZero teams work remotely, eliminating costly travel expenses and the need for resources to be provided on-site. And since ThreatZero is an objectives-based, rather than time-based, engagement, work doesn't stop until a state of prevention is achieved.
- **Transfer of knowledge:** Client teams receive extensive solution training and learn best practices for responding to threats and maintaining the organization's prevention status.
- **Simplified EDR:** BlackBerry Optics' InstaQuery and Focus Views features make it easy to visualize activity and track TTPs and other interesting artifacts. The Context Analysis Engine can take action on one endpoint, a group of systems, or the entire environment.
- **On-demand incident response assessment:** During engagements, sometimes indicators of compromise that a significant breach may be underway are discovered. If so, BlackBerry has incident response and containment experts available to help identify, trace, and remediate the incursion, as well as prevent it from recurring.

To Learn More

Whatever security challenge an organization may be facing, BlackBerry's team of experts can help. For more information about the complete portfolio of ThreatZero services, please view the ThreatZero Services Line Card, visit the ThreatZero web page, or **call +1-877-973-3336**.

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.