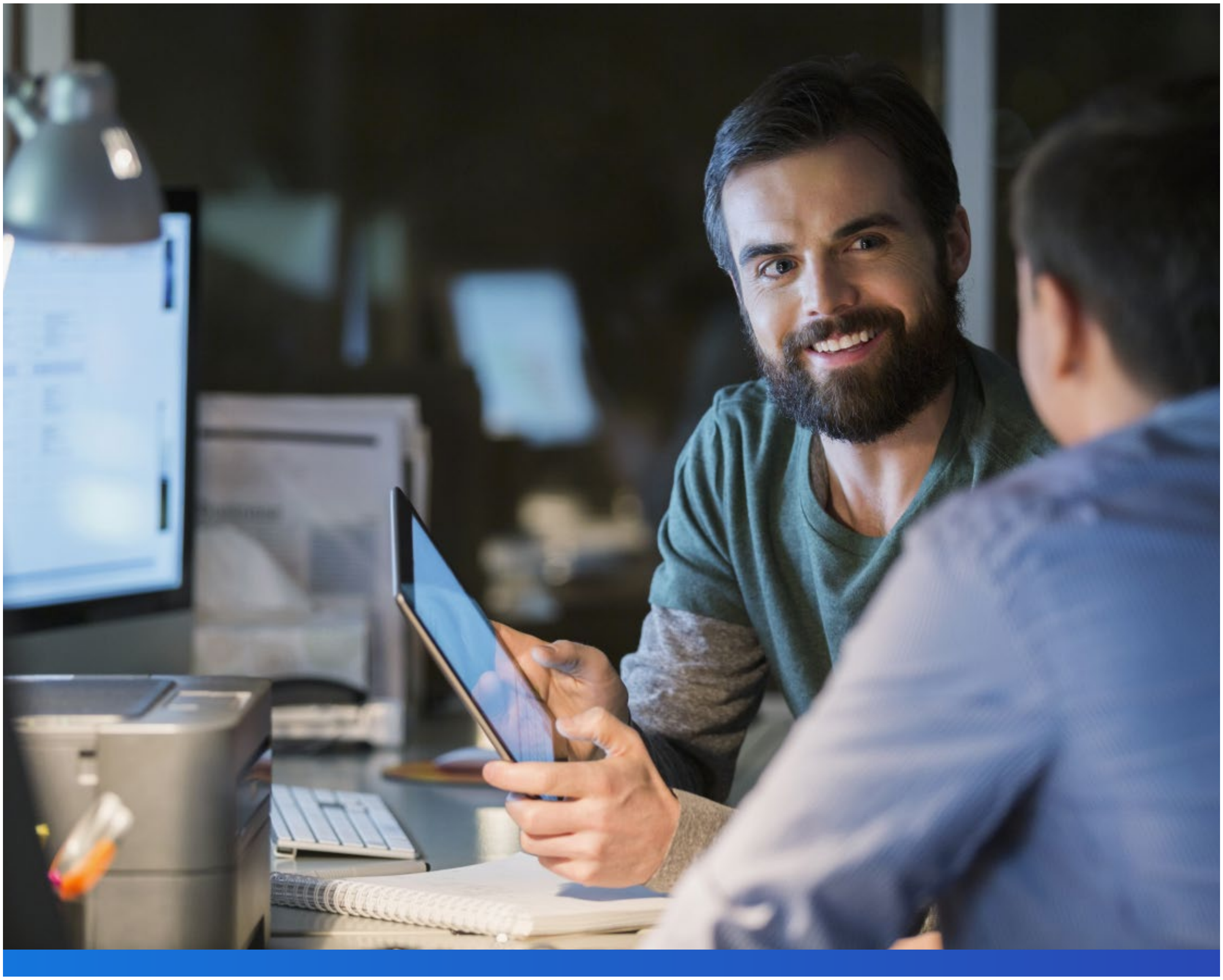
SOLUTION BRIEF

BlackBerry Endpoint Security Solutions for SMBs



Introduction

Cyber criminals are attacking small and medium-sized businesses (SMBs) today with more success than ever before. According to a 2019 SMB survey conducted by the Ponemon Institute[1]:

- 66% of the respondents had been attacked within the previous 12 months.
- Data breaches increased from 54% in 2017 to 63% in 2019.
- The average cost to recover from business disruptions caused by these incidents rose from $1.21M in 2017 to $1.9M in 2019.
- Only 26% of respondents managed to decrease attack response times. Another 39% reported that response times had increased.

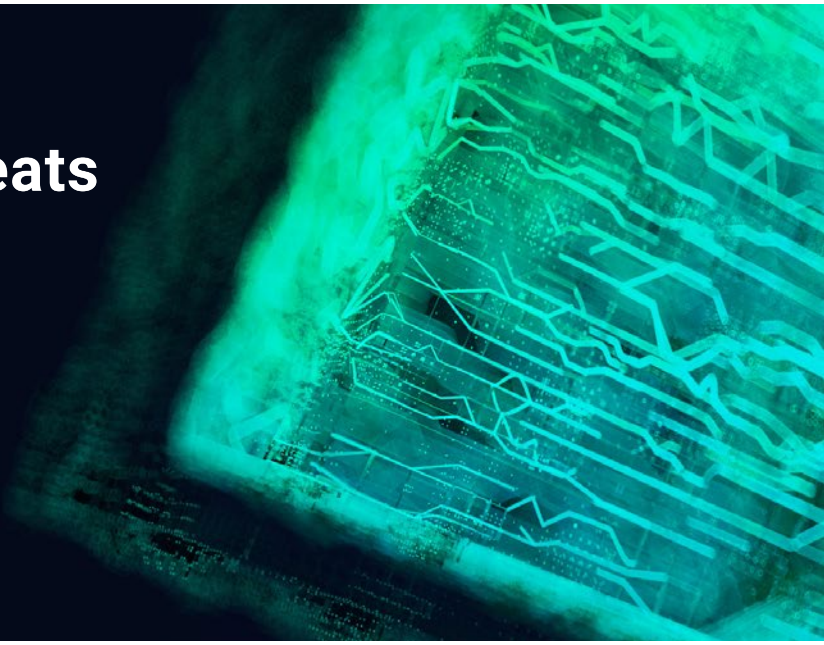
The financial and operational damage of a major breach can be devastating. Despite this, many SMBs remain vulnerable due to chronic budget constraints and difficulties in recruiting and retaining skilled security professionals. As a result, only 30% of the survey respondents gave their organizations very high marks for effectiveness in mitigating risks, vulnerabilities, and attacks, citing insufficient personnel (77%) and insufficient budgets (55%) as among the chief causes.

What This Means for SMBs

BlackBerry recognizes that SMB endpoint security solutions must not only deliver uncompromising protection, but also be:

- **Simple to deploy.** IT staff should be able to deploy the solution independently by following a clear and straightforward sequence of installation procedures. Alternately, the security vendor should offer affordable turnkey implementation services.
- **Easy to manage.** The solution should provide a set-it-and-forget-it experience by eliminating the need for signatures, dedicated hardware, frequent updates, and complex rulesets. Alternately, affordable managed detection and response (MDR) services should be available that off-load cybersecurity administration tasks from internal staff.
- **Efficient with computing resources.** The solution should have a small footprint and work quietly in the background, eliminating intrusive scans that degrade system performance and impede worker productivity.
- **Protective of employee-owned systems.** The solution should prevent malware from compromising systems used by workers to access company resources while at home.
- **Cost-effective.** The vendor should be able to demonstrate a return on investment that earns sponsorship and support from the organization’s IT and executive management.

Preventing Security Threats with BlackBerry Protect



BlackBerry® Protect is an enterprise-class threat prevention solution that combines the power of AI to block malware infections with additional security controls that safeguard against script-based, fileless, memory, and external device-based attacks. Unlike traditional endpoint security products that rely on signatures and behavior analysis to detect threats, BlackBerry Protect:

- Uses AI to identify and prevent the execution of both known and zero-day malware.
- Works independently on each endpoint without needing updates or a cloud connection.
- Protects endpoints without scans that degrade performance or inconvenience end-users.

BlackBerry Protect stops both known and unknown attacks from compromising endpoints with unmatched effectiveness, ease of use, and minimal system impact.

Key Features

BlackBerry Protect provides full-spectrum threat prevention. Key features include:

- **AI-Driven Malware Prevention.** Within a matter of milliseconds, the BlackBerry prevention model analyzes and classifies millions of characteristics per file, breaking them down to an atomic level to discern whether an object is good or bad and preventing malware from executing on endpoints.

- ✓ **Prevention of Unknown and Zero-Day Malware.** Testing performed by SE Labs showed that BlackBerry Protect prevents the execution of malware that will not be identified by threat researchers for years to come, with an average Predictive Advantage of 25 months.[2]
- ✓ **Memory Exploitation Detection and Prevention.** Identifies and stops fileless attacks with immediate, automated prevention responses.
- ✓ **Script Management.** Enforces policies that determine when and where scripts are allowed to run and who is allowed to run them.
- ✓ **Device Usage Policy Enforcement.** Imposes access rules on external devices, such as USB drives, thereby eliminating them as possible attack vectors.
- ✓ **Application Control for Fixed-Function Devices.** Ensures fixed-function devices remain in a pristine state, eliminating the drift that occurs with unmanaged devices.

This automated AI-based approach to endpoint protection can eliminate 99.1%[3] of threats, freeing up IT budgets and resources for other strategic business initiatives.

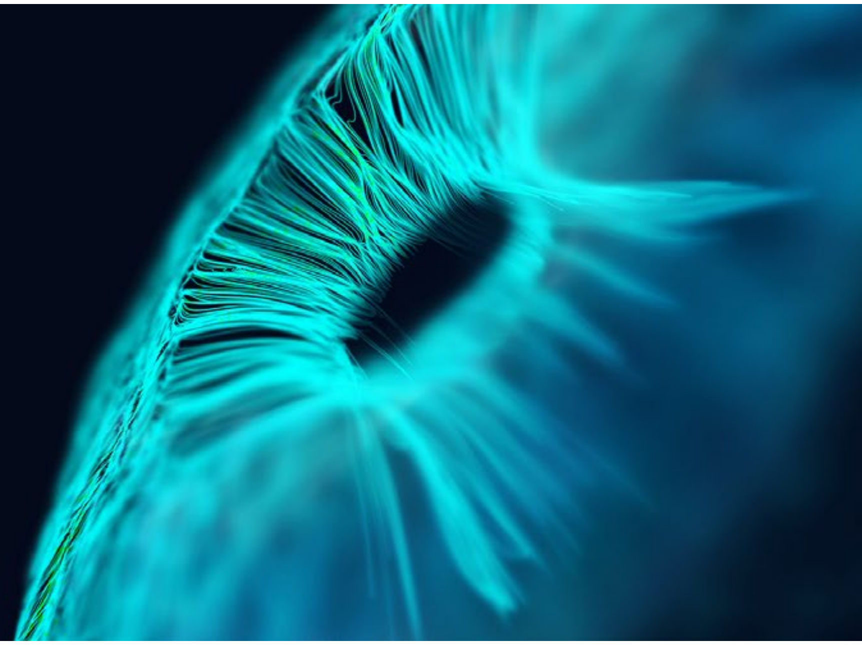
Common Use Cases

BlackBerry Protect is the right choice for SMBs that need to:

- ✓ Detect and prevent malicious executables and zero-day attacks.
- ✓ Thwart ransomware such as NotPetya, WannaCry, Goldeneye, and Satan from executing and hijacking their data.
- ✓ Prevent malicious email attachments from detonating their payloads.
- ✓ Stop adversaries from misusing common system management tools to compromise memory with fileless attacks.
- ✓ Stop employees from running unauthorized and potentially malicious scripts.
- ✓ Prohibit unauthorized access to external devices.
- ✓ Implement security policies that meet specific business needs. For example, one BlackBerry customer operationalized BlackBerry Protect to allow only members of its IT department to run scripts and utilize USB devices.

To learn more, download BlackBerry Protect. Continuous Threat Prevention Powered by Artificial Intelligence.

Preventing Widespread Security Incidents with BlackBerry Optics



BlackBerry® Optics is an endpoint detection and response (EDR) solution that extends the threat prevention delivered by BlackBerry Protect by applying artificial intelligence (AI) to prevent widespread security incidents. BlackBerry Optics provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities. Unlike other EDR products, BlackBerry Optics doesn't require significant investments in on-premises infrastructure or need to stream data continuously to the cloud for storage and analysis. Instead, all BlackBerry Optics threat detection and response actions are initiated at the endpoint. This lightweight architecture means organizations can adopt EDR capabilities both quickly and efficiently.

Key Features

BlackBerry Optics helps organizations keep their system and data assets secure, with features that include:

- **AI-Driven Incident Prevention.** Predictive models uncover threats that would be difficult to identify with behavior rules.
- **Consistent Cross-Platform Visibility.** Detects and prevents incidents across Microsoft® Windows® and Apple® MacOS® platforms.
- **On-Demand Root Cause Analysis.** Enables analysts to determine how threats entered the environment so corrective actions can be taken.
- **Enterprise-Wide Threat Hunting.** Helps analysts uncover hidden threats by searching endpoint data for suspicious or malicious activity.

- ✓ **Dynamic Threat Detection.** Automates threat detection in real time using custom and curated behavior rules that run exclusively on the endpoint.
- ✓ **Rapid Automated Responses.** Initiates customized automated responses that contain threats and minimize the risks of a widespread incident.

Common Use Cases

BlackBerry Optics is the right choice for SMBs running BlackBerry Protect that need to:

- ✓ **Investigate Attack and Alert Data.** Analysts can retrieve useful information from BlackBerry Protect and other security controls to quickly and intuitively visualize alert activity.
- ✓ **Hunt for Indicators of Compromise (IOCs).** Analysts can quickly search all network endpoints for files, executables, hash values, and other IOCs to uncover hidden threats.
- ✓ **Initiate Rapid, Automated, Playbook-Driven Incident Responses.** Playbooks can automatically initiate a variety of response actions ranging from collecting critical forensic data to taking compromised systems offline.

To learn more, download BlackBerry Optics. AI-Powered Endpoint Detection and Response.

Protecting Employee-Owned Systems with BlackBerry Smart Antivirus

BlackBerry® Smart Antivirus extends the AI-driven malware prevention features of BlackBerry Protect to systems owned by employees and their families, thereby reducing the risk of malware spreading from their homes to their employer's corporate network.

Key Features

BlackBerry Smart Antivirus key features include:

- ✓ AI-Driven Malware Prevention.
- ✓ Prevention of Unknown and Zero-Day Malware.
- ✓ Consumer-Friendly Simplicity. BlackBerry Smart Antivirus updates itself automatically and is easy to install, configure, and manage.

BlackBerry Smart Antivirus lets consumers benefit from BlackBerry's AI technology without having to set up and manage the extensive set of security controls BlackBerry Protect provides for enterprise-level environments. Thus, BlackBerry Smart Antivirus alone cannot provide the foundation for a business to achieve the state of prevention.

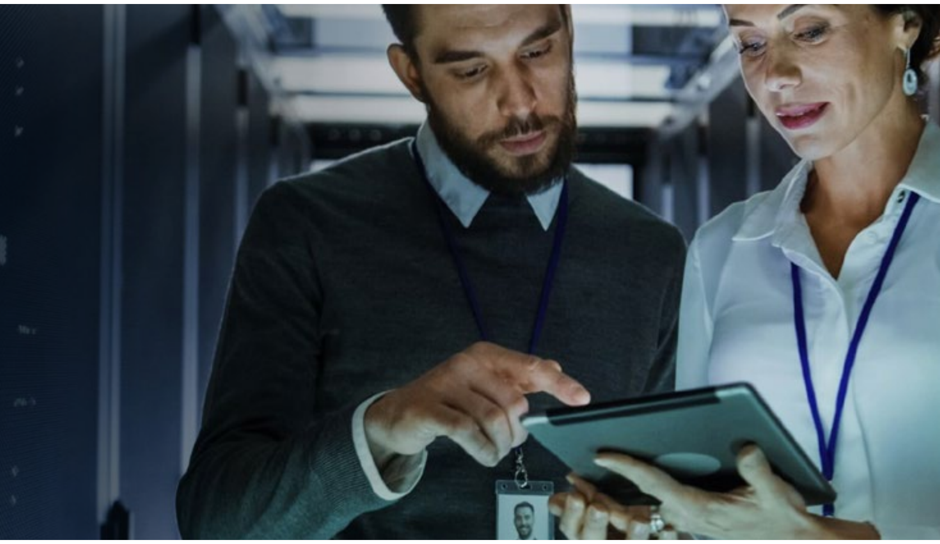
Common Use Cases

BlackBerry Smart Antivirus is the right choice for SMBs that want to:

- ✓ Protect employee-owned Windows and Mac® devices from being compromised by malware.
- ✓ Reduce their security risks and exposure to threats originating from employees' homes.

To learn more, download the BlackBerry Smart Antivirus Data Sheet.

Consulting Services Solutions



BlackBerry Consulting offers a portfolio of services that help SMBs strengthen and close gaps in their security architecture.

ThreatZERO® is an objectives-based engagement to operationalize and optimize BlackBerry Protect and BlackBerry Optics in the client's environment. ThreatZERO experts deliver the technological expertise, personalized white glove service, and project management skills needed to proceed efficiently through a series of measurable progress goals that culminate in a state of zero threats and ongoing prevention.

To learn more, download BlackBerry Protect + ThreatZERO.

BlackBerry® Guard is a subscription-based MDR solution for businesses of any size that need enterprise-class security but have limited internal security resources. It includes:

- ✓ A deployment of BlackBerry Protect and BlackBerry Optics that is operationalized and optimized by ThreatZERO consultants.
- ✓ 24x7 support from a team of BlackBerry incident responders and prevention experts who utilize AI to triage alerts, investigate IOCs, and help remediate breaches. BlackBerry Guard can implement effective countermeasures quickly, limiting the impact of a breach and initiating playbook-driven automated responses ranging from taking infected systems offline to restoring known-safe system configurations.

To learn more, download BlackBerry Guard 24x7 Managed Detection and Response

Other BlackBerry Consulting practice areas include Incident Response, Red Team Services, Industrial Control Systems, IoT/Embedded System Security, Strategic Services, and Education.

Ready to learn more? Then contact us today to request a Return on Investment Analysis for your transition from a reactive to a prevention-first security posture.

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 150M 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.

BlackBerry. Intelligent Security. Everywhere.

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

[1] 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses

[2] Cylance vs. Future Threats: The Predictive Advantage

[3] Cylance Achieves 99.1% Efficacy in NSS Labs Advanced Endpoint Protection Test.