BlackBerry
Intelligent Security. Everywhere.

Evaluation Guide

BlackBerry Cybersecurity Maturity Evaluation Guide

A Four-Tiered Framework for Achieving Cyber Resilience

Introduction

Are your security controls capable of preventing threats from breaching your defenses? What investments should you make to close gaps in your security architecture? Should you acquire security tools and resources internally or outsource to a managed security service provider (MSSP)? How will you adapt as threat actors introduce new tactics, techniques, and procedures (TTPs) to their arsenals? Every organization will answer differently based on its goals, security posture, and overall risk tolerance.

In this guide, we provide a methodology and roadmap for organizations of all sizes to use in assessing and advancing the maturity of their cyber risk management programs. We employ a four-tiered framework that encompasses endpoint protection platforms (EPP), endpoint detection and response (EDR), security operations centers (SOCs), and threat hunting. We also consider the resource requirements and criteria for making these security investments at each stage of overall maturity.

In this guide, we provide a methodology and roadmap for organizations of all sizes to use in assessing and advancing the maturity of their cyber risk management programs.

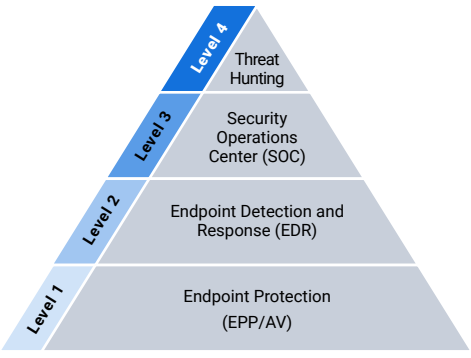
Security Maturity Model

Level 1: Relevant and applicable as a strategy for all organizations, regardless of size

Level 2: Relevant and applicable as a strategy for all organizations, regardless of size, though smaller organizations may choose to use an MSSP to manage

Level 3: More relevant for larger organizations and multi-national corporations due to resources required to staff and manage

Level 4: Only relevant for large organizations and multi-national corporations due to the specialized skillset required to staff and maintain, though some organizations may choose to use a managed detection and response (MDR) solution provider



LEVEL 1

Endpoint Protection Platform (EPP)[1]

Virtually every organization today has some form of endpoint protection in place. This is essential since more than 90% of malware is delivered to endpoints by phishing and spear phishing exploits.[2] Increasingly, however, firms are discovering that legacy antivirus (AV) products are ineffective against today's sophisticated file-based and fileless threats due to their reliance on obsolete signature-matching technologies.

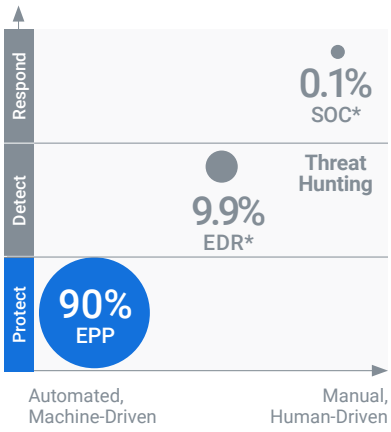
A signature is a unique string of bits that functions as a malware file's digital fingerprint. Each time a traditional AV product encounters a new file, it compares a byte in the file to bytes in its signature database. If a match is found, the AV product continues this sequential byte-by-byte matching process until the entire file has been inspected. To be flagged as malware, every byte in the examined file must match every byte in the signature exactly. However, signature-based tools can easily be evaded if an attacker modifies or obfuscates their code or if the AV vendor has yet to complete the tedious manual process of creating and distributing signature updates for one of the 350,000 new malware variants released in the wild each day.[3]

This byte-by-byte matching process is often so resource-intensive that endpoints can become unresponsive or unstable during scans, inconveniencing end-users and reducing their productivity. Signature-based AV is also management-intensive, requiring staff to download, install, distribute, and audit an ongoing stream of signature file updates.

Fortunately, smarter next-gen endpoint solutions are now available that utilize more advanced capabilities for malware defense. BlackBerry® Protect, for example, harnesses algorithmic science to detect malware and prevent it from executing. BlackBerry Protect scrutinizes every file, whether it's attached to a weaponized document or copied from an employee's flash drive. Sophisticated machine learning models analyze 2.7 million file properties[4], disassembling each file into its constituent DNA to discern whether it's malicious or benign. This deep analysis is performed in milliseconds by an agile lightweight agent that operates independently on each host, without any reliance on a signature database, Internet access, or cloud connectivity.

BlackBerry Protect also provides application and script control, memory protection, and device policy enforcement features that prevent cyber attacks from succeeding. This automated AI-based approach to endpoint protection can eliminate 99.1%[5] of threats, freeing up IT budgets and resources for other more strategic security initiatives.

AI-Based EPP should be contributing at least 90% to your endpoint security strategy

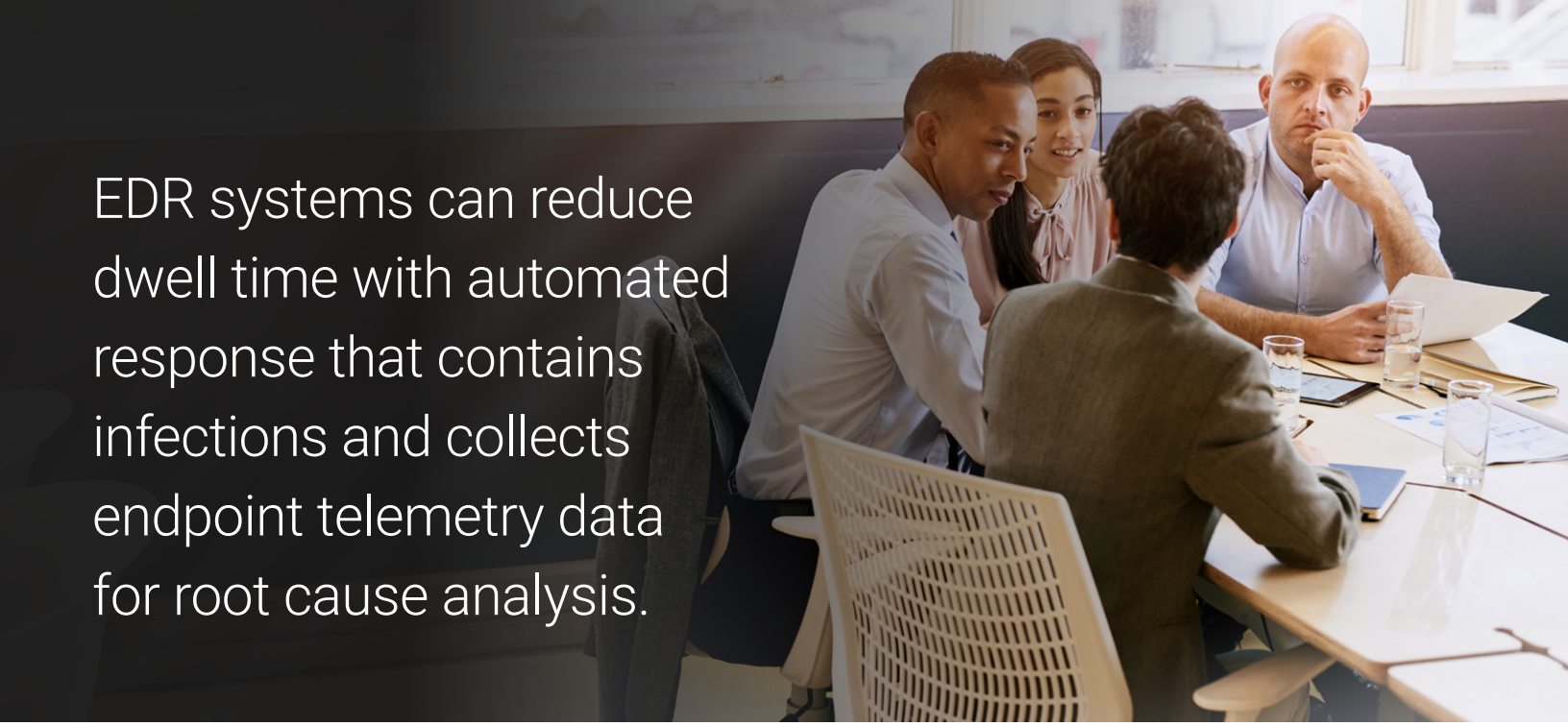


**Percent of overall threats you're mitigating via different security approaches*

AI-Driven Threat Prevention Benefits

Download our white paper, *BlackBerry vs. Traditional Security Approaches,* to learn more about the benefits of AI-based threat prevention, and if you haven't already decommissioned your legacy AV, learn about the benefits of upgrading to AI-driven threat prevention.

Sophisticated machine learning models analyze 2.7 million file properties, disassembling each file into its constituent DNA to discern whether it's malicious or benign.



EDR systems can reduce dwell time with automated response that contains infections and collects endpoint telemetry data for root cause analysis.

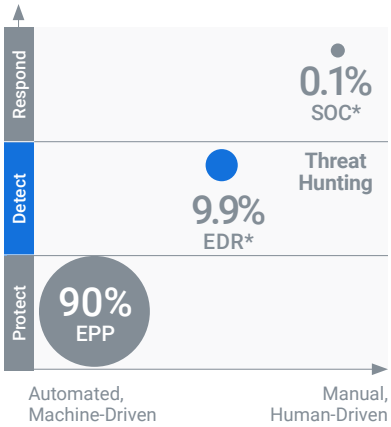
LEVEL 2

Endpoint Detection and Response (EDR)

Endpoint detection and response (EDR) solutions occupy the next maturity tier of our security framework. EDR systems can reduce dwell time with automated response that contains infections and collects endpoint telemetry data for root cause analysis. However, there are a few key considerations when determining whether an investment in EDR is right for your organization.

- **Signal To Noise Ratio:** It can be challenging to discern the signal of an attack from within the mass of noisy EDR data. A single data point may only be significant based on the context in which it appears and its correlation with other security events.
- **Enforcement at the Endpoint:** Many traditional EDR products rely on cloud-based analysis to uncover threats. That said, more advanced EDR solutions can now push all detection and response decisions down to the endpoint, eliminating the response latency that can make the difference between a minor security event and a major uncontrolled security incident.
- **Breaking the Rules:** Adversaries are constantly developing new TTPs that are expressly designed to evade traditional rules-based EDR systems, rendering them as ineffective and obsolete as signature-based EPPs. Modern EDR solutions incorporate multiple detection methods, including context-driven threat detection and machine learning threat identification.
- **Consistent Automated Responses:** Response and remediation routines should be initiated automatically and performed consistently across the environment.

An EDR solution should address almost all threats that evade your EPP



**Percent of overall threats you're mitigating via different security approaches*

BlackBerry EDR Benefits

To learn more about the benefits of AI-based EDR, visit our dedicated page for more information, or download our white paper entitled *AI-Based Prevention: The Evolution of Endpoint Prevention and Detection*.

Setting up and maintaining an SOC is an expensive proposition, so there are many factors to consider when evaluating potential SOC investments.

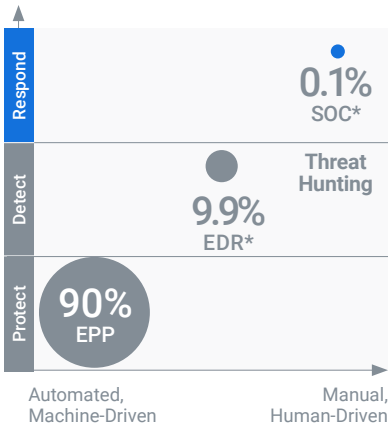
LEVEL 3

Security Operations Center (SOC)

The next tier of security maturity, the security operations center (SOC), is populated primarily by enterprises making significant investments in infrastructure and staff to reduce cyber risks and preserve business agility. SOC analysts are responsible for selecting and implementing security controls, collecting and contextualizing event data, triaging alerts, assessing indicators of compromise (IOCs), and initiating incident response (IR) plans that limit the damage of a successful attack. Setting up and maintaining an SOC is an expensive proposition, so organizations should consider these factors when evaluating potential SOC investments.

- **Availability of Skilled Cybersecurity Staff:** Even large organizations with deep pockets struggle to recruit and retain SOC teams with the requisite skills and experience in endpoint security, perimeter security, networking, programming, and forensic analysis. According to a recent Frost and Sullivan research study[6], two-thirds of the organizations surveyed reported they had too few cybersecurity workers to meet their present needs, a global shortage of security talent that shows no signs of abating. As a result, many SOC analysts are recent college graduates or workers with comparatively little practical experience dealing with complex security challenges. Staffing issues are exacerbated by the need for SOCs at global enterprises to operate around the clock every day of the year, since adversaries don't keep office hours and often launch attacks from locations overseas. Allowing for vacation and sick days, a fully-staffed SOC may need a minimum of 12 to 15 full-time analysts simply to obtain the desired coverage.
- **Analyst Burnout Due To Alert Fatigue:** SOC analysts are subject to alert fatigue and burnout due to the sheer volume of security alerts most of them end up having to triage each day. A large enterprise may have as many as 50 different security solutions that collectively generate tens of thousands of alerts[7] daily.

The SOC should be directly handling no more than 0.1% of threats manually



**Percent of overall threats you're mitigating via different security approaches*

More than half of security alerts are false positives, according to Ponemon Institute research[8], wasting 425 hours of analyst time each week pursuing fruitless investigations. As a result, 44% of alerts are never investigated at all because of alert fatigue and only half of the remaining legitimate alerts are remediated, according to Cisco[9] research. Modern security controls can sharply reduce alert volumes and improve alert fidelity by utilizing advanced AI and automation techniques, and by incorporating detection rules mapped to the MITRE ATT&CK® Framework. However, smaller, less-resourced organizations may find it more cost-effective to leverage subscription-based managed detection and response (MDR) solutions, such as BlackBerry® Guard, which require no upfront investments in security software and implementation services.

- **Investments in Big Data Platforms:** SOC analysts need seamless access to security event and alert data in order to trace suspect activity and identify threat actors. This requires investments in big data platforms that extract, parse, normalize, and store raw log data from endpoints, servers, perimeter defenses, and network management products. Storage costs can rise quickly, whether an organization opts to host the data locally or utilize a cloud service such as Amazon Web Services. The most significant data can then be extracted from the log store to a security information and event management (SIEM) platform, where it can be filtered, contextualized, enriched with analytics, and correlated with data from external threat intelligence feeds such as VirusTotal. SIEM costs can also rise quickly, since many vendors price their solutions on an events-captured-per-second basis. SOC staff must monitor and manage these platforms to ensure data is being continuously updated and validated.
- **The Critical Importance of Incident Response Plans and Processes:** Far too often, organizations invest in SOC infrastructure and staffing only to fall short when it comes to developing plans and processes for incident response, an oversight equivalent to sending military forces into battle without a plan of attack. In fact, according to a 2018 Telstra study[10], a quarter of the respondents either didn't have, or didn't know if they had, an IR plan in place. An IR plan should specify every action to be taken when an incident occurs, beginning with the assignment of members to the IR team. This will typically include not only the most experienced SOC analysts, but also senior security staff with expertise in evidence collection, endpoint and network forensics, and malware analysis, as well as an incident manager to lead the team and provide status updates to the key business and technology stakeholders. IR processes must be sufficiently granular to define such things as the procedures for accessing memory, hard drive, and network data, and the decisions to be taken when compromised systems are identified. For example, the process may specify whether the system should be taken offline or left connected to preserve access to its network stack data. All processes and decision criteria must be specified in advance through close collaboration between C-level executives (including the CISO), security specialists with relevant experience, and the business owners of the pertinent applications or data. Security professionals should offer technical input, but IR plans must be defined based on an organization's strategic goals and risk appetite, rather than on theoretical security best practices. Ultimately, it's essential for everyone involved, from the C-suite to business line management, to accept the risks and results of IR decisions.

Alert Fatigue

50

Security Solutions

×

Thousands of Alerts

425

Wasted Hours

44%

of Alerts Are Not Investigated Because of Alert Fatigue

LEVEL 4

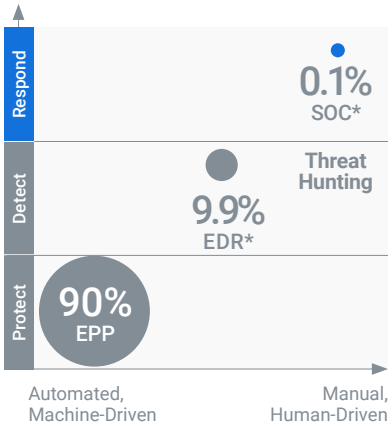
Threat Hunting

Threat hunting occupies the fourth and final tier of our security framework. At this stage of development, the most successful and mature organizations have achieved a prevention-first security posture, which means that over 90% of threats are being deflected and/or neutralized automatically. Security policies are enforced with effective security controls and big data platforms are collecting and contextualizing data for alert management and post-incident analysis. Incident response plans and processes are well-defined and ensure that serious incursions are remediated rapidly and efficiently.

With these resources in place, senior analysts with specialized skills and experience can be assigned to proactively hunt for evidence of previously undetected malicious activity. Threat hunters utilize both intelligence and methodology-based processes to identify anomalous security events and patterns of behavior that combine to indicate an adversary may be actively engaged in one or more stages of the kill-chain. While threat hunting can benefit any organization, it's wise to consider the following requirements before making threat hunting investments.

- **Risk-Prioritized Objectives:** Threat hunting employs the same iterative hypothesis testing methods utilized in scientific inquiry. For example, to test the hypothesis that an exfiltration attack may be underway, a threat hunter might search for IOCs associated with anomalous network flows or suspicious data access and staging behaviors by end-users. Threat hunting objectives should be defined in advance and prioritized based on an organization's risk profile and business strategy.

Threat hunting is a high-value but largely manual process for addressing the small percentage of malicious activity that evades EDRs and EPPs



**Percent of overall threats you're mitigating via different security approaches*

- **Staff Recruitment and Retention Challenges:** The global shortage of skilled security professionals is even more acute for analysts with the specialized skills and broad experience required for threat hunting. Organizations may find it near impossible to recruit and retain expert threat hunters attracted by the higher salaries and more favorable working conditions often offered by MSSPs and security consulting firms.
- **Ongoing Training and Skills Augmentation:** Just as businesses continually evolve their core processes to optimize profits, so too do threat actors with their TTPs and attack vectors. To maintain parity, organizations must invest in ongoing training to ensure that threat hunters are technically proficient, business fluent, and highly attuned to the risks presented by the organization's evolving goals, attack surfaces, and business processes.
- **Fear of Exposing Internal Data:** Organizations that lack internal threat hunting resources may be reluctant to outsource threat hunting operations out of fear that exposing internal data may present unknown and unacceptable risks of exposure.

Security Maturity Is an Ongoing Process

We hope you've found this four-tiered maturity model useful in assessing your current and future security needs. Each tier introduces new and important capabilities for strengthening an organization's security posture. However, it's not necessary for every organization to source solutions in all four tiers, or to attempt to build out capabilities in each tier internally.

If you're a small to medium-sized business, it may not be practical for you to invest in an SOC to triage alerts or implement a big data platform to facilitate threat hunting. You may find it more cost-effective, instead, to leverage the staff and expertise of MDR and threat hunting services, such as BlackBerry Guard, or enter into consultant retainer relationships for periodic penetration testing and incident response assessments. Others may benefit from outsourcing routine SOC functions to an MSSP so that internal staff can focus on security projects that support and advance business goals. As always, it's the quality of execution that matters, not where the expertise is sourced. Most of all, maturity means committing to an ongoing program of cybersecurity self-improvement and responsible risk governance.

Learn More

To learn more about the BlackBerry Guard MDR and threat hunting solution, visit *our dedicated page for more information*, or *download our data sheet*.

To Learn More

BlackBerry stands ready to be your partner, with a comprehensive portfolio of solutions and services suitable for organizations at every stage of cybersecurity maturity.

BlackBerry Protect delivers malware prevention powered by artificial intelligence, combined with application and script control, memory protection, and device policy enforcement to identify and prevent threats before they can execute.

BlackBerry® Optics is an EDR solution that extends the threat prevention delivered by BlackBerry Protect by providing true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities.

BlackBerry Guard is a subscription-based MDR solution that leverages our native AI platform and the 24x7 support of a team of BlackBerry incident responders and prevention experts.

Incident Readiness Assessments: Our team will help you craft an IR plan and set of processes that align with your risk management goals and help demonstrate regulatory compliance.

Incident Containment and Forensics: If an incident occurs, we'll help you trace it, contain it, and remediate it quickly, before it becomes a major event.

Red Team Services: We'll probe for gaps and vulnerabilities in your security fabric that can be exploited by internal and external threat actors.

1 To learn more, download our eBook entitled, *Artificial Intelligence: The Smarter Approach To Information Security*.
2 *5 Cybersecurity Statistics Every Small Business Should Know in 2018*. Alert Logic.
3 Signatures Can't Keep Up
4 *The Numbers and Results Don't Lie*
5 *NSS Labs Advanced Endpoint Protection: Cylance Security Value Map,* April 2018. The BlackBerry Protect solution was formerly known as CylancePROTECT®.
6 *2017 Global Information Security Workforce Study (GISWS)*
7 *Dark Reading. Fighting Alert Fatigue with Actionable Intelligence.* Article cites Ponemon Study entitled, The Cost of Insecure Endpoints
8 *Dark Reading. Fighting Alert Fatigue with Actionable Intelligence.* Article cites Ponemon Study entitled, The Cost of Insecure Endpoints
9 *Cisco 2018 Annual Cybersecurity Report* | The defender landscape.
10 *Telstra Security Report* 2018.

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.

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

BlackBerry
Intelligent Security. Everywhere.

MK20-0266 | 200520