BlackBerry

Predict and Prevent vs. Monitor and Manage

What every MSSP should know

A Growing Threat Landscape

Organizations are embracing digital transformation and work-from-anywhere initiatives, dramatically increasing the stakes for cybersecurity professionals. Furthermore, organizations seeking greater efficiency and lower operational costs are driving the convergence of IT, IoT (Internet of Things), and OT (operational technology) environments, which have increased the complexity and vulnerability of previously isolated OT/ICS networks. Legacy systems, equipment, and devices are tempting targets for cybercriminals. In the face of escalating threats, a global skills shortage, and vendor/security product complexity, **the demand for managed security services is increasing.**

Endpoints Are Proliferating Worldwide

554M	1.23B	6.5B
Edge-enabled enterprise devices in 2022	Edge-enabled enterprise devices by 2030	Connected consumer devices by 2030

Source: Statista, Nov. 23, 2021

MSSPs: Essential Cybersecurity Partners

Endpoints are proliferating. So are the cyberattacks against them. To ensure operational security and workforce flexibility, companies are looking for MSSPs who can simplify the complexity of cyber defense without sacrificing effectiveness. Deploying next-generation cybersecurity protection, detection, and response is critical. With prevention-first, predictive cybersecurity, MSSPs can help clients.

The Advantages of Predictive Cybersecurity

An ounce of prevention is worth a pound of cure. While monitoring and managing threats are absolutely essential to a robust cyber defense, they're only half the battle. That's because security solutions driven by endpoint detection and response (EDR) require bad code to execute before they become effective. Conversely, AI-powered, intelligent cybersecurity solutions predict and prevent malicious code execution before it happens. But not all AI is created equal. Advanced AI/ML-based algorithms can proactively discover and stop known and never-before-seen threats, enabling protection even in closed environments with limited or no Internet connectivity.

> In 2021, *43% of businesses indicated focusing on attack prevention* in regard to their cybersecurity investments over the next 12 months. Overall, most companies committed to improving their security to proactively address the issue of future attacks.
>
> – Statista, Feb. 14, 2022

Assessing Cybersecurity Solutions

Detecting and reacting very quickly to abnormal behavior requires visibility, constant monitoring and deep learning working in parallel. Automated, sophisticated cybersecurity makes it possible for MSSPs to safeguard clients against even the most nefarious threats—no human intervention, Internet connection, signature files, heuristics, or sandboxes required. When assessing cybersecurity solutions to add to their portfolio, MSSPs should consider:

AI/ML Sophistication

AI-based endpoint protection platforms (EPPs) can prevent breaches and provide added controls to ward off sophisticated cyberthreats even without human intervention. Does the solution utilize advanced AI/ML algorithms that protect against known and never-before-seen threats?

Threat Hunting

Before is better. Does the solution enable deep insight for threat hunting and forensics along with custom and built-in playbooks that automate incident responses? Mitigating and containing ransomware and other threats at the endpoints drastically minimizes attack surfaces and potential lateral movement.

Visibility

Increasing situational awareness, providing real-time insight into potential attacks, and deploying a prevention-first EDR solution can effectively eliminate response latency, identifying and acting to stop cyberattacks in milliseconds—before any damage is done. Does the solution provide holistic, integrated visibility for cloud-enabled EDR and threat intelligence?

Online/Offline Protection

Does the solution offer fully cloud-enabled and on-premises network deployment? Those that do provide flexibility and ensure uninterrupted protection whether the device is connected to the cloud or not.

Integration

Does the solution require standalone services to provide integration across endpoints? Does it integrate easily across existing technology stacks? Those that fully integrate all endpoints—including applications and mobile devices—into the cybersecurity platform, and that integrate across tech stacks, secure an entire infrastructure with a unified solution.

Zero-Day Payloads

Proactive cybersecurity prevents malware and suspicious payloads from executing, and can proactively identify and respond in milliseconds to malicious use of memory in fileless attacks. Does the solution predict and stop zero-day attacks and ransomware before they execute?

Compute Power

Lightweight agents that limit the use of system processing resources at the endpoint ensure that more power is reserved for operational and business-critical tasks. It is also more cost effective, especially for organizations who cannot afford to upgrade annually, because the infrastructure is being preserved. Does the solution preserve network bandwidth and compute power?

Bandwidth

Security teams are stretched thin in many organizations. Does the solution enable them to focus on key security initiatives rather than spending time and resources attempting to make sense of data, triaging alerts, or recovering from attacks? Does it provide 24x7x365 protection? Managed extended detection and response (XDR) services staffed with expert analysts can act as an extension of the cybersecurity team.

IT/OT Environments

Does the solution protect existing systems as well as it does new ones? Keeping legacy operating systems and embedded operating systems running safely in managed IT/OT environments is imperative. Companies are unlikely to rip and replace expensive technology that's still working well for them—but that doesn't make securing it any less important. Furthermore, securing air-gapped environments reduces the risk of insider malfeasance.

BlackBerry delivers cybersecurity and Zero Trust with a zero-touch end-user experience through a single console and offers the end-to-end solution with a broad set of AI-based security capabilities and visibility across mobile, desktop, apps, and people.

Adopting a Well-Rounded Approach

MSSPs that offer their clients a predictive, human, and holistic approach position themselves to become trusted partners in the war against cyber crime, giving them unlimited opportunity for profitable growth as cyberthreats and cyber defenses evolve.

Predictive

By leveraging advanced AI models across all endpoints to detect and eliminate more types of threats before a breach occurs, MSSPs can simply and efficiently minimize incidents that require action.

Human

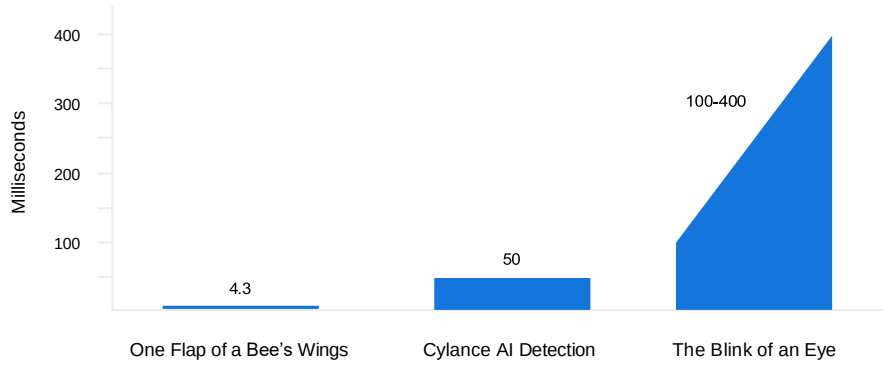
Augmenting your offerings and your clients' security posture with skilled human experience, expert threat intelligence, proactive hunting and prevention, immediate support, and exceptional expertise gives them peace of mind in an increasingly risky world.

Holistic

Providing a coordinated and composed defensive management and control strategy across devices, users, applications, and data, reinforced with the visibility to detect and respond to cyberattacks from any angle, ensures the continuity of business in the face of any critical event.

Between a Bee and a Blink

Cylance® AI detects and prevents potentially harmful code in less than 50 milliseconds. That's between the time it takes for a bee to flap its wings and the blink of an eye.



Why Choose BlackBerry

Powered by Cylance AI technology, BlackBerry was first to market with AI for cybersecurity that has since been trained on trillions of safe and harmful files to protect clients against known and never-before-seen threats. Sophisticated BlackBerry® protection, detection, and response solutions can prevent even the most insidious attacks 99.1% of the time.

In fact, in a commissioned study conducted by Forrester Consulting on behalf of BlackBerry comprising four customer interviews and data aggregation, Forrester concluded that CylancePROTECT® has the following three-year financial impact:

Source: The Total Economic Impact™ of CylancePROTECT From BlackBerry, A Forrester Total Economic Impact Study Commissioned by BlackBerry, October 2022

Zero
Cybersecurity breaches

$1.3M
Reduction in the cost of security breaches

$806K
Decommissioned software subscription costs

100%
Return on investment

The BlackBerry MSSP Partner Program

At BlackBerry, our goal is to increase MSSPs' capabilities and customer confidence by offering advanced, predictive Cylance AI-driven cybersecurity. The award-winning BlackBerry MSSP Partner Program enables MSSPs to keep their clients secure and productive with intelligent cybersecurity solutions that are easy to deploy, connect, scale, and manage across any environment.

Start Fast
Provide advanced, prevention-first cybersecurity services, even with limited experience or bandwidth, with an intuitive, low-touch platform.

Scale Quickly
Add clients, integrate endpoints, and move into new markets fast utilizing on-demand and instantaneous deployment capabilities.

Automate Effortlessly
Provide prevention-first security faster and more cost-efficiently vs. semi-automated or manual detect and response.

Adapt Instantly
Continuously adapt to an ever-changing threat landscape while supporting client growth, innovation, and business transformation.

Pay for Actual Usage
Pay for consumption only using subscription licensing and automated billing (monthly or annually)—no minimums, no commitments.

Protect 24x7x365
Partner with the BlackBerry SOC to offer clients subscription-based, managed XDR service around the clock in any geography.

Preserve Resources
Eliminate daily malware signature updates, spend less time triaging alerts, and reduce the need for attack remediation.

Broaden Capabilities
Augment prevention and incident response capabilities or incorporate a turnkey, end-to-end security solution without staffing up.

Through the BlackBerry MSSP Partner Programs, partners can offer clients sophisticated, layered cybersecurity protection with an award-winning program focused on driving mutual success through profitable growth opportunities, cybersecurity innovation, and partner enablement.

MSSP Partner Program benefits include:

- Deal protection, discounts, incentives, and rewards for new opportunities
- Collaboration with BlackBerry sales, marketing, and engineering experts
- Joint selling initiatives, marketing development funds, and quarterly business planning
- Sales and technical training

Cybersecurity solutions from BlackBerry include:

CylancePERSONA™
Behavior and risk analytics

CylanceOPTICS®
Threat detection and hunting

CylancePROTECT®
Endpoint device protection

CylanceGATEWAY™
Secure network access

CylanceGUARD®
Security operations center (SOC) offering 24x7x365 monitoring

Cylance® AI
AI-enhanced Compromise Assessments

CylanceAVERT™
Information protection

Build your business while you protect theirs with the BlackBerry MSSP Partner Program ⟶