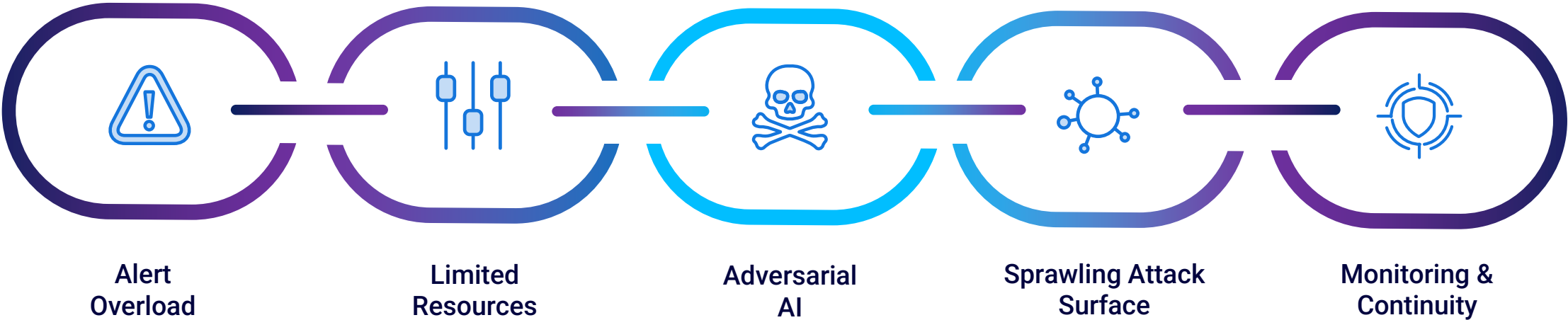# CYLANCEMDR

BlackBerry | Cybersecurity

Elevating SOC Operations

Matthew Kaatz
IntegraOne – Channel Development Manager

Common Interlinking Challenges
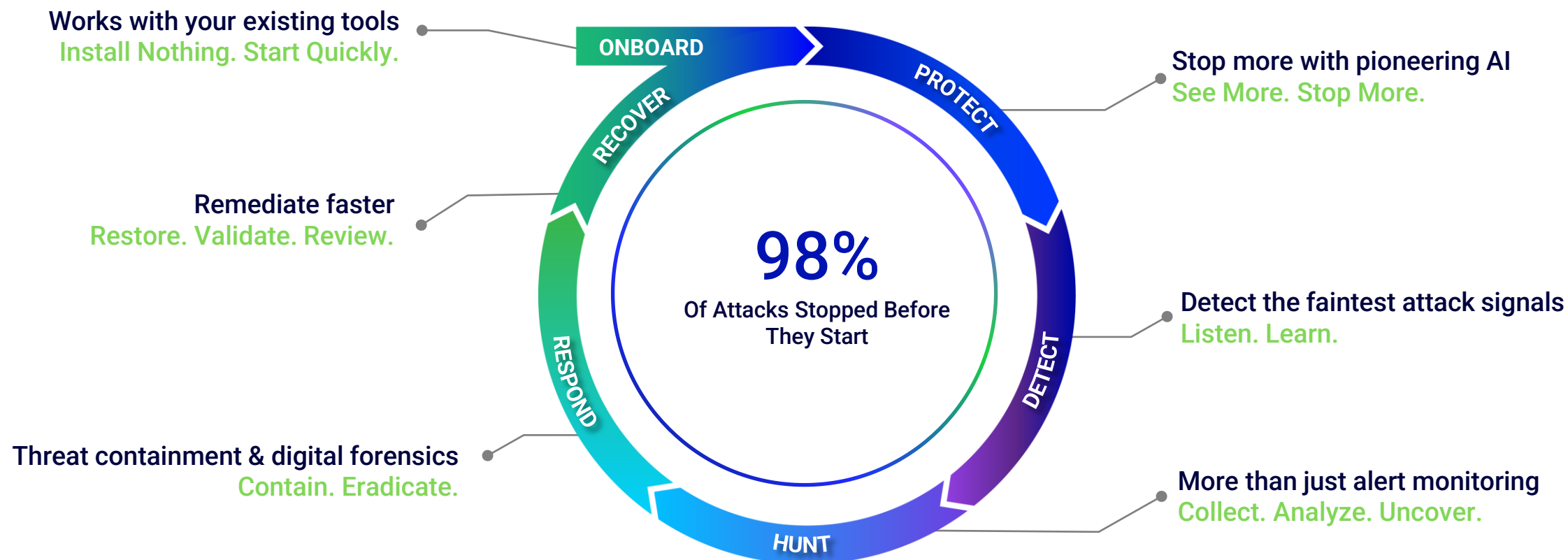
Organizations and security professionals face interconnected challenges that can impact outcomes if not addressed.

Alert Overload — **Limited Resources** — **Adversarial AI** — **Sprawling Attack Surface** — **Monitoring & Continuity**
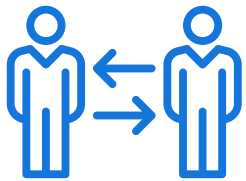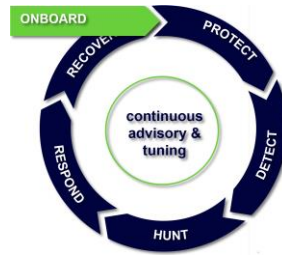
More Spending ≠ More Confidence

A Continuous, Full-Service Engagement

Our always-on engagement model ensures continuous monitoring and response to threats.

Works with your existing tools
Install Nothing. Start Quickly.

Stop more with pioneering AI
See More. Stop More.

Remediate faster
Restore. Validate. Review.

Detect the faintest attack signals
Listen. Learn.

Threat containment & digital forensics
Contain. Eradicate.

More than just alert monitoring
Collect. Analyze. Uncover.

ONBOARD · PROTECT · DETECT · HUNT · RESPOND · RECOVER

98%
Of Attacks Stopped Before
They Start

White-Glove Onboarding

Close-collaboration to ensure your environment is ready

Full-service agent deployment

Configuration and finetuning
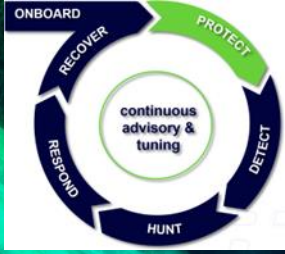
Seamless handover to Cylance SOC

Continuous fine-tune & keep drift from occurring

BlackBerry Protect – Preventing Bad Code

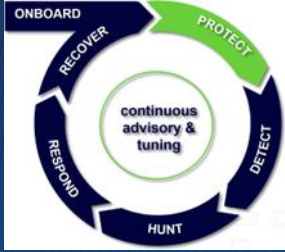AI-Based Pre-Execution Prevention

Memory Exploit Protection

Script Control
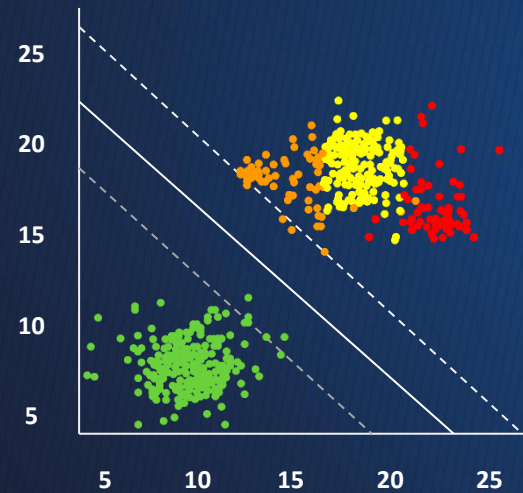
Powered By The Industry's Most Effective AI
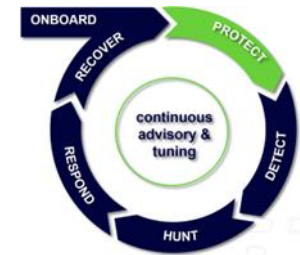
25% more threats stopped

8x less resources used

5x more patented technology
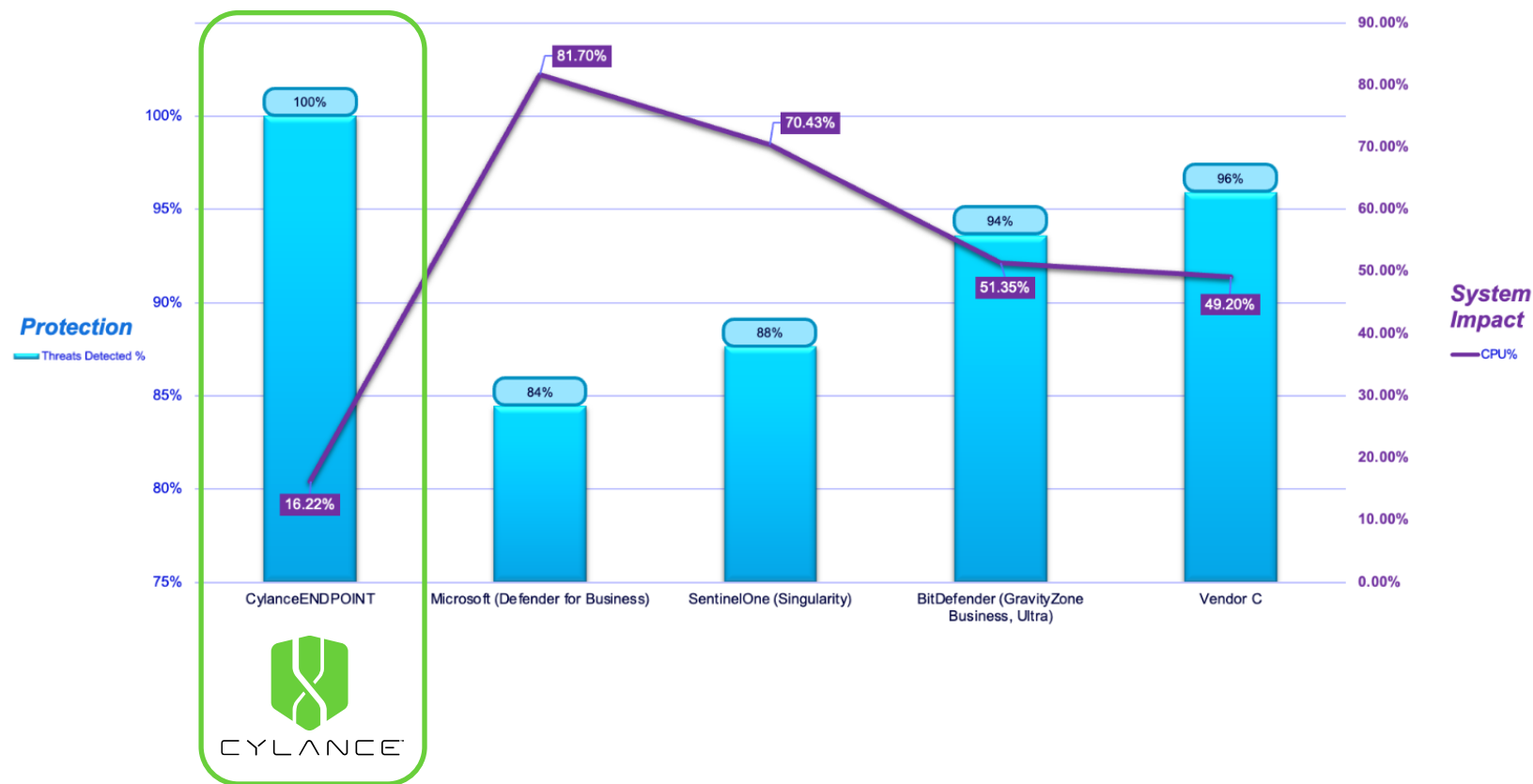
Tolly Group - Endpoint Security Testing

BlackBerry Optics – Prevention-First "EDR"

IOA/IOC Based Detections

Auto-Respond and Context

Works Online & Offline
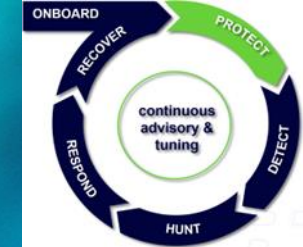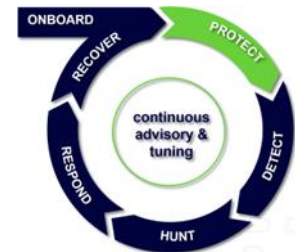
More Pioneering AI/ML Patents Than Others

Current Published G06N 20/00 Machine Learning Family Patents as defined by Cooperative Patent Classification (CPC) Sept 2023.

Bit9 (VMWARE)

SentinelOne

2
DeepInstinct

4
BitDefender

11
CrowdStrike
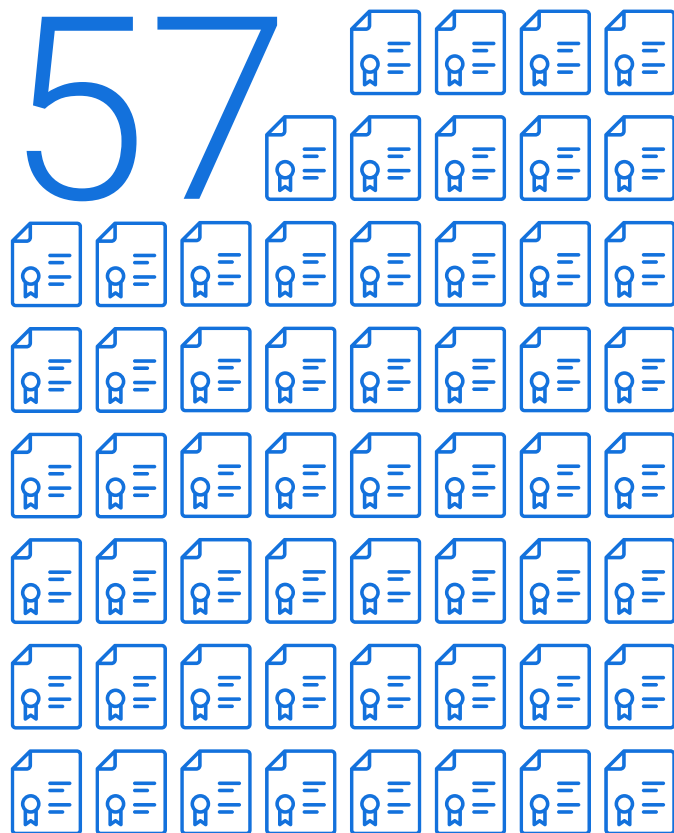
57
Cylance

AI-Driven, Extensible Platform

The flexibility you need, enabling you to keep your tools, improve visibility, and enhance your security posture.

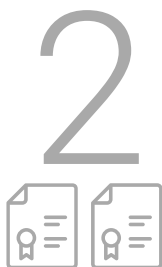**Advanced AI at the Core**
Cylance AI detects attack signals through alert noise to proactively stop threats.

Cybersecurity Experts
Eliminate the complexity of cybersecurity so you can focus on running your business.

Compatible With All Your Tools
Install nothing. Keep your security tools and improve security outcomes.

Collect & Enrich Your Data
Add context, improve clarity, and inform actions across all your entire attack surface.

24/7 Managed SOC

Cylance Security Teams

Cylance AI

Incident Response

Managed Threat Hunting

Collect Telemetry

Enrich with Intel

Open XDR Architecture

SOPHOS
Microsoft Defender
SentinelOne
CROWDSTRIKE
Endpoint

Network

zscaler
netskope
paloalto NETWORKS
Cloud

Azure
Google Cloud
aws

Identity
okta
RSA

SaaS

Google Workspace
Microsoft 365
mimecast

Email

The Backend Infrastructure – Build vs Buy
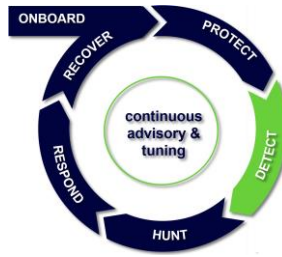
Tools & Telemetry

- NDR
- Threat Intelligence Platform
- EPP/EDR
- CLOUD
- SAAS
- ZTNA
- Mobile
- VM

Collect

(NG-SIEM)

- Ingest
- Normalize
- Enrich
- Data Lake

Detect

- ML Alerts
- Rule Based Alerts
- Threat Hunting

Correlate

- Correlated Incidents

Investigate & Respond

- Automated Response
- Workflow Integrations
- Recommended Remediations
- Reporting
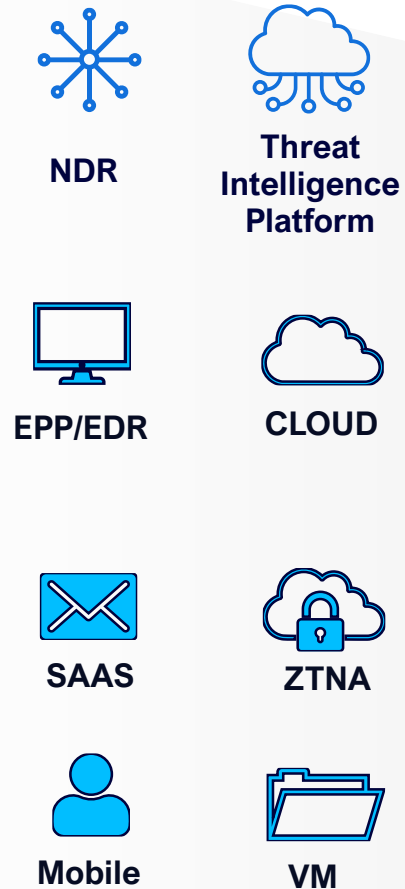
Detection & Response across all Tools & Telemetry

ONBOARD
PROTECT
DETECT
HUNT
RESPOND
RECOVER
continuous advisory & tuning

High-fidelity Detection & Triage With Dramatically Less Noise
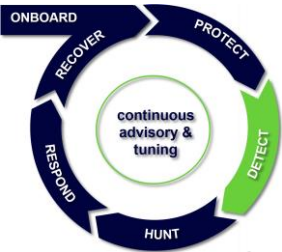
Event Triage & Investigation Flow

All Events
~90% Of Common Alert Noise Eliminated

Environment Specific
~10% Customer-Specific Events Validated

Low-fidelity signals
~1% Deep Investigation

Escalated to Customer
~0.1% Need Attention

Collect, correlate & enrich file, process, network, & identity telemetry with proprietary threat intelligence
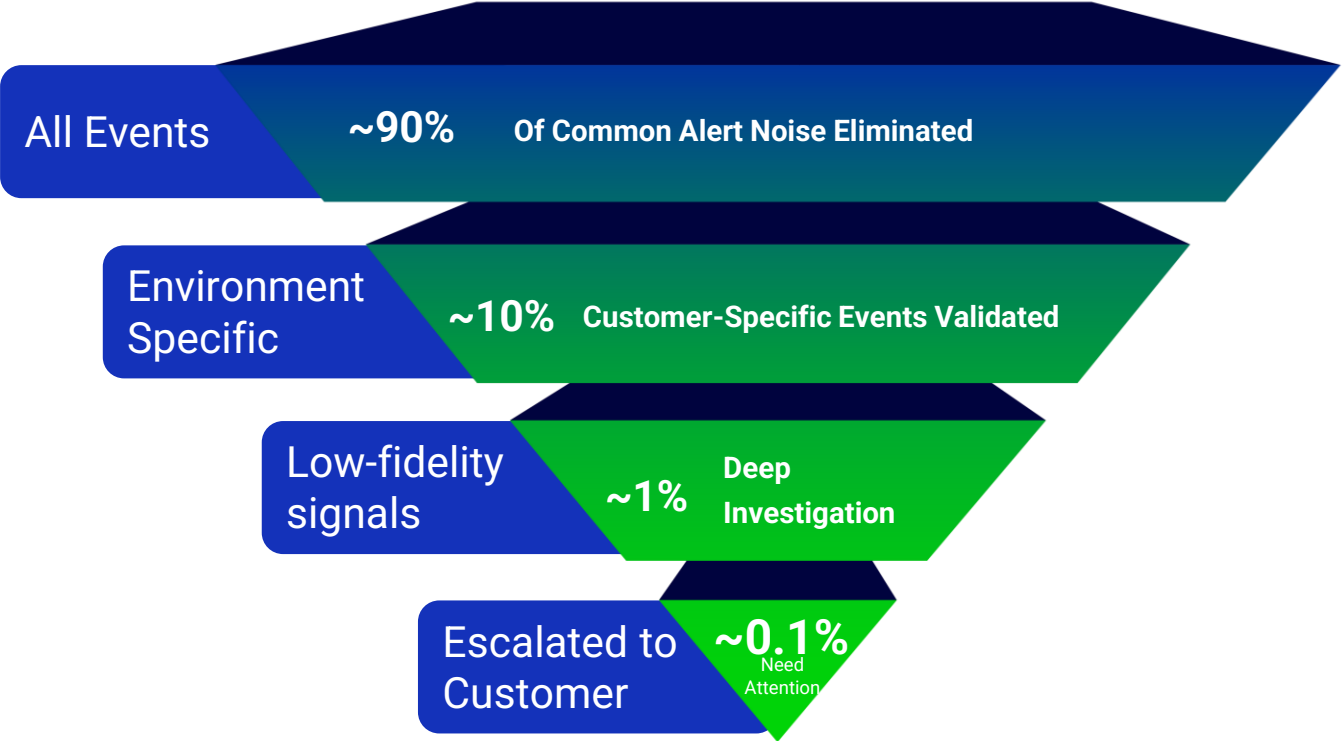
99.5% Alert management efficiency

90% Reduction of internal security ops efforts

FORRESTER®
Total Economic Impact Report

Cyber Threat Intelligence Is In Our DNA

CylanceMDR experts collaborate with BlackBerry's Threat Research team by using in-house and open-source threat intelligence to uncover and take action against the world's most sophisticated adversarial threats.

Proactive, human-led threat hunting

Retrospective analysis 30-day view plane

Strategic Threat Intelligence
Provides a broad overview of the threat landscape and potential long-term impacts on an organization.

Operational Threat Intel
Focuses on potential near-term attacks to enable an organization's preparedness and response.

Tactical Threat Intel
Provides organizations with immediate, actionable information to detect and respond to specific threats.

Expert-Led Digital Forensics

Documentation and unbroken trail that records the handling, transfer, analysis, and storage of digital evidence.

Investigations of data stored in cloud environments like AWS, Azure, and Google Cloud.

Digital Forensics
Full forensic lab supporting data recovery, investigations, evidence analysis, and breach studies.

Incident Containment

Chain of Custody

Computer Forensics

Cloud Forensics

Network Forensics

Immediate and sustained containment to limit the impact and spread of a security incident.

Monitoring and analysis of network traffic and activities across a network.

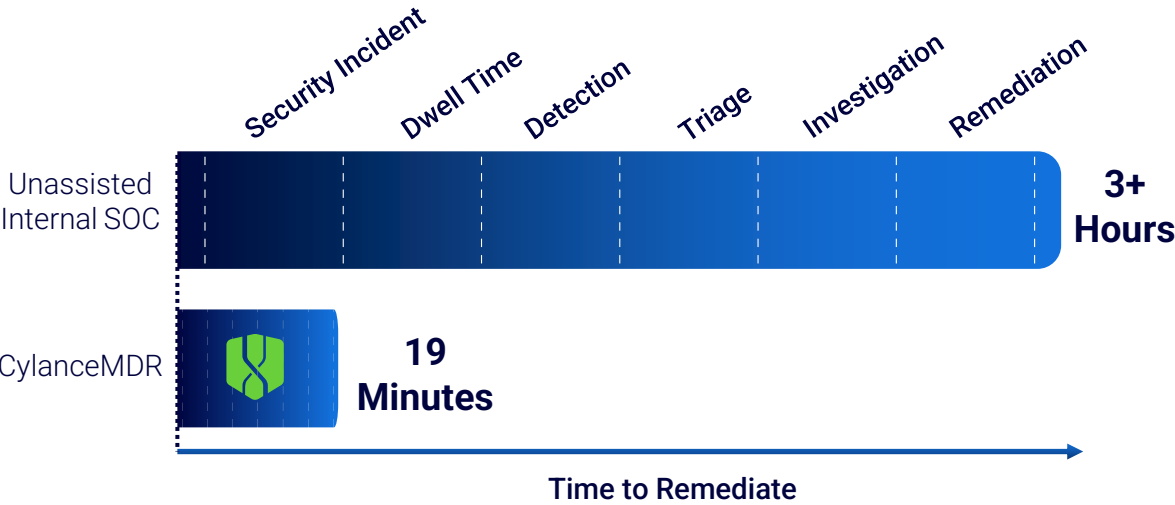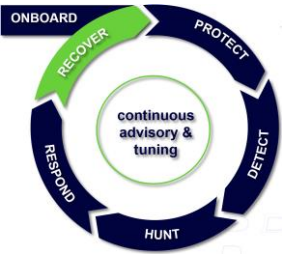Analysis of data stored on physical devices like desktops, laptops, and mobile devices.

Did you know?

BlackBerry digital forensic investigators also serve as expert witnesses in a court of law.

Full-Service Incident Response to Recover Quickly

CylanceMDR is proven to prevent more threats quickly. It utilizes advanced threat-blocking predictive AI and award-winning threat-hunting experts to respond and recover rapidly.

Security Incident | Dwell Time | Detection | Triage | Investigation | Remediation

Unassisted Internal SOC — **3+ Hours**

CylanceMDR — **19 Minutes**

Time to Remediate

Automated
Leverage tools and advanced AI to automatically detect, analyze, and respond to security events without human intervention.
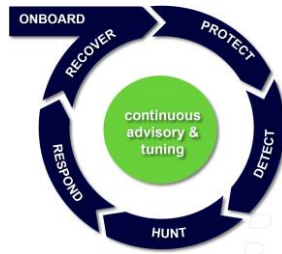
Guided
Use automation and recommendations from CylanceMDR experts to assist your human analysts in stopping and remediating threats.

Active
Hands-on, manual intervention by CylanceMDR experts to investigate, contain, and remediate security incidents.

ONBOARD · PROTECT · DETECT · HUNT · RESPOND · RECOVER
continuous advisory & tuning

Continuous Advisory

ONBOARD

RECOVER

PROTECT

RESPOND

DETECT

HUNT

24x7

Onboarding
weekly
get your environment ready

Tailored Activity & Protection Validation
monthly
constant situational awareness

Advisory Sessions
quarterly
strategic advice & posture review

Our Experts Become Trusted Members of Your Team

The best cybersecurity pros from around the world will secure your business 24/7.

15 years average SOC experience per analyst

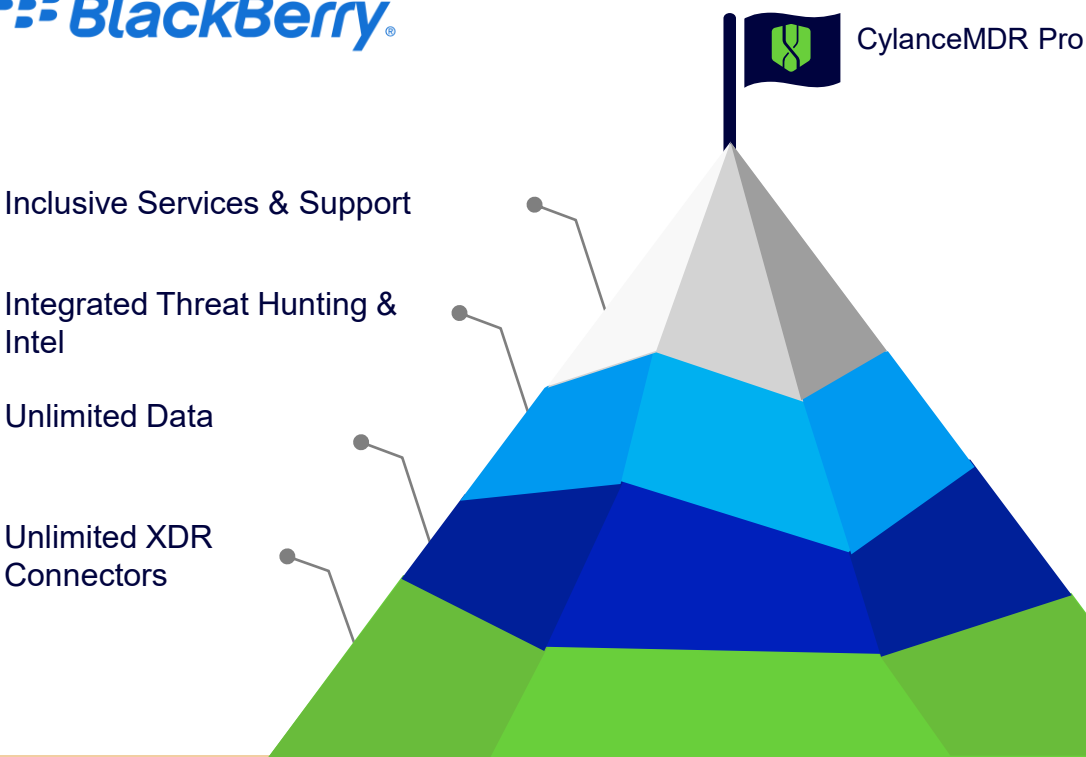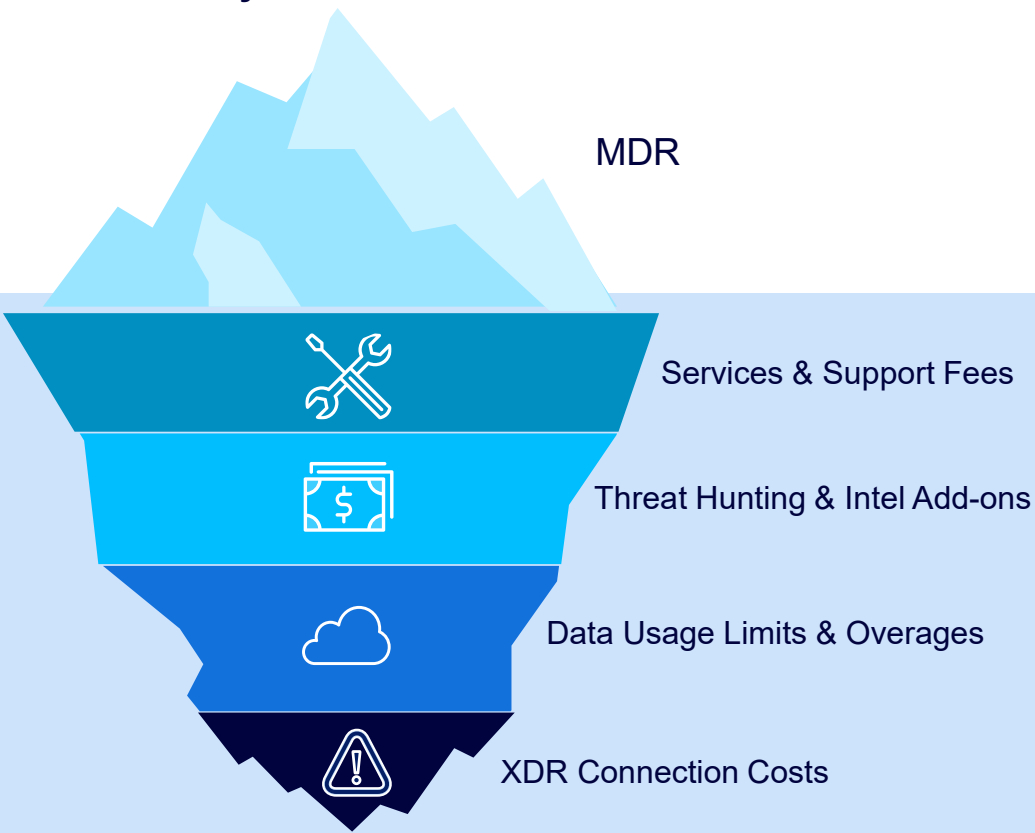Proven to disrupt APT-level threats in MITRE ATT&CK evaluations

APT Response Service Provider

Strategic consulting guiding your cybersecurity journey

Simple Pricing With No Hidden Costs

With CylanceMDR, you'll know exactly what you're getting with your investment.

The Other Guys

MDR

Services & Support Fees

Threat Hunting & Intel Add-ons

Data Usage Limits & Overages

XDR Connection Costs

Hidden Costs Under the Surface

BlackBerry

CylanceMDR Pro

Inclusive Services & Support

Integrated Threat Hunting & Intel

Unlimited Data

Unlimited XDR Connectors

No Hidden Costs

Outcomes That Matter

AI-Driven MDR
Highly-rated efficacy

293% ROI
Forrester Total Economic Impact Study

5x
more patents

15
avg years of experience

85%
less expensive than building your own SOC

98%
faster threat detection

99.5%
alert management efficiency

Ultimate Peace of Mind

$1M WARRANTY

Recover up to one million USD covering:

- Forensic investigation
- Cyber extortion payments
- Post-security incident expenses

No minimum license count requirements!

Flexible Tiers Align To Your Needs

We've got you covered with access to experts whenever you need them and round-the-clock support for your existing stack.

	ON-DEMAND Access CylanceMDR experts with a single click to find and stop threats.	**STANDARD** Essential MDR services supporting Cylance solutions to build cyber resilience.	**ADVANCED** Full access to our full breadth of MDR services for Cylance solutions to harden your defenses.	**PRO** Complete access to CylanceMDR experts and services, along with unrestricted access an expansive ecosystem for seamless integration with your current security tools.
24/7 Detection & Response	✓	✓	✓	✓
24/7 Threat Hunting	✗	✓	✓	✓
Advisory Services and Reporting	✗	✓	✓	✓
Incident Response & Forensic Investigations	Add-On	Add-On	✓	✓
$1M Guarantee	✗	✗	✓	✓
Open XDR Ecosystem	✗	✗	✗	✓

Thank you

BlackBerry® Intelligent Security. Everywhere.