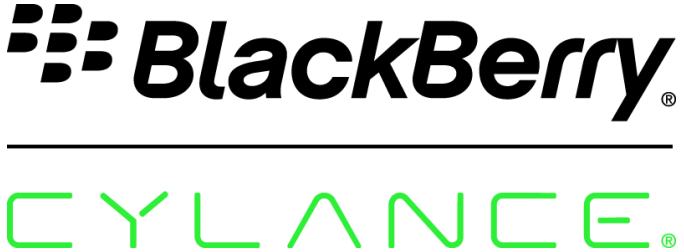
The AI Advantage



Jon Oltsik
Senior Principal Analyst and Fellow

Bret Lenmark
Senior Product Marketing Manager

The webinar will start momentarily

Enterprise Strategy Group | Getting to the bigger truth.™

Leveraging Machine Learning for Endpoint Security

Jon Oltsik, Senior Principal Analyst and Fellow

May 16, 2019

PREPARED BY ESG FOR

BlackBerry

CYLANCE

AGENDA

- Situational analysis
- Toward artificial intelligence/machine learning
- Optimized endpoint security
- The Bigger Truth

Legacy Endpoint Security Solutions are Failing

Most enterprise organizations use an assortment of point tools for endpoint security, but this strategy has proven to be inefficient and ineffective

Poor Efficacy

- Traditional AV can miss 50% or more of today's attacks
- Security analysts suffer from alert fatigue
- Too many false positives

Too Much Complexity

- Multiple agents slows endpoints
- Disparate datasets
- Too many vendors

Lack of Integration

- Analysts manually correlate data wasting time
- Prevention, detection and response not working together

Complexity is Driving Consolidation

91% of orgs surveyed are either actively consolidating endpoint management vendors or considering doing so

Source: ESG Research: Modern Endpoint Management Research (Dec 2018)

AI, Machine Learning is Changing the Game

51% of organizations are either currently or planning on investing in Big-data analytics/ML/Predictive Analytics [1]

- Machine Learning (ML) has been widely recognized as a valuable approach to detecting attacks
- ML can prevent both known and unknown attacks reducing the likelihood of a successful attacks
- ML threat detection minimizes the need for static behavioral rules

Better protection, reduced signal to noise ratio, increased productivity for the security team

[1] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

Machine Learning in Security

Prevention: Properly applied, ML can provide the context we need to **reduce the risks of a breach** while significantly increasing the "cost of attack."

Detection: ML systems make it possible for analysts to discern how events widely dispersed in time and across disparate hosts, users, and networks are related.

Optimizing Endpoint Security

The Power of AI / Machine Learning

Attack Surface Protection

Unified Architecture

Self-Contained Security

Attack Surface Protection

1. Prevent malware from executing
2. Control how and where scripts are run
3. Detect attempts to exploit memory
4. Control use of USB devices
5. **Protect fixed function devices** from being compromised by unauthorized/unapproved application installs

Unified Architecture

- **An analytics foundation** built ground-up on AI/ML supporting all functions including prevention, detection and response
- **A single agent** designed for low overhead, requiring fewer memory, processing, and storage resources.
- **Tightly integrated endpoint security applications** designed as micro-services that communicate with one another and the core platform through an open API set
- **Simplified deployment and management** offering a single console and the ability to easily add modules without additional deployment

Self-Contained Security

- Security that does not require signatures, the cloud, or any information not located on the endpoint to protect itself.

- Capable of making autonomous security decisions using data stored on each individual endpoint

AI / Machine Learning makes this possible

The Bigger Truth

- Endpoint security is broken
- Disparate tools are difficult to deploy and operate
- Point tools are increasingly ineffective at preventing, detecting and responding
- Endpoint security platforms should offer a single, modern platform using open APIs, microservices and a single agent.
- Machine learning has become a foundation for endpoint security platforms and beyond…

Enterprise Strategy Group | **Getting to the bigger truth.**™

Thank You

Jon Oltsik, Senior Principal Analyst and Fellow
jon.oltsik@esg-global.com

FOLLOW ESG

http://www.twitter.com/esg_global

http://www.facebook.com/ESGglobal

http://www.linkedin.com/company/44337

http://www.youtube.com/user/ESGglobal

“So…what is BlackBerry Cylance doing about it?”

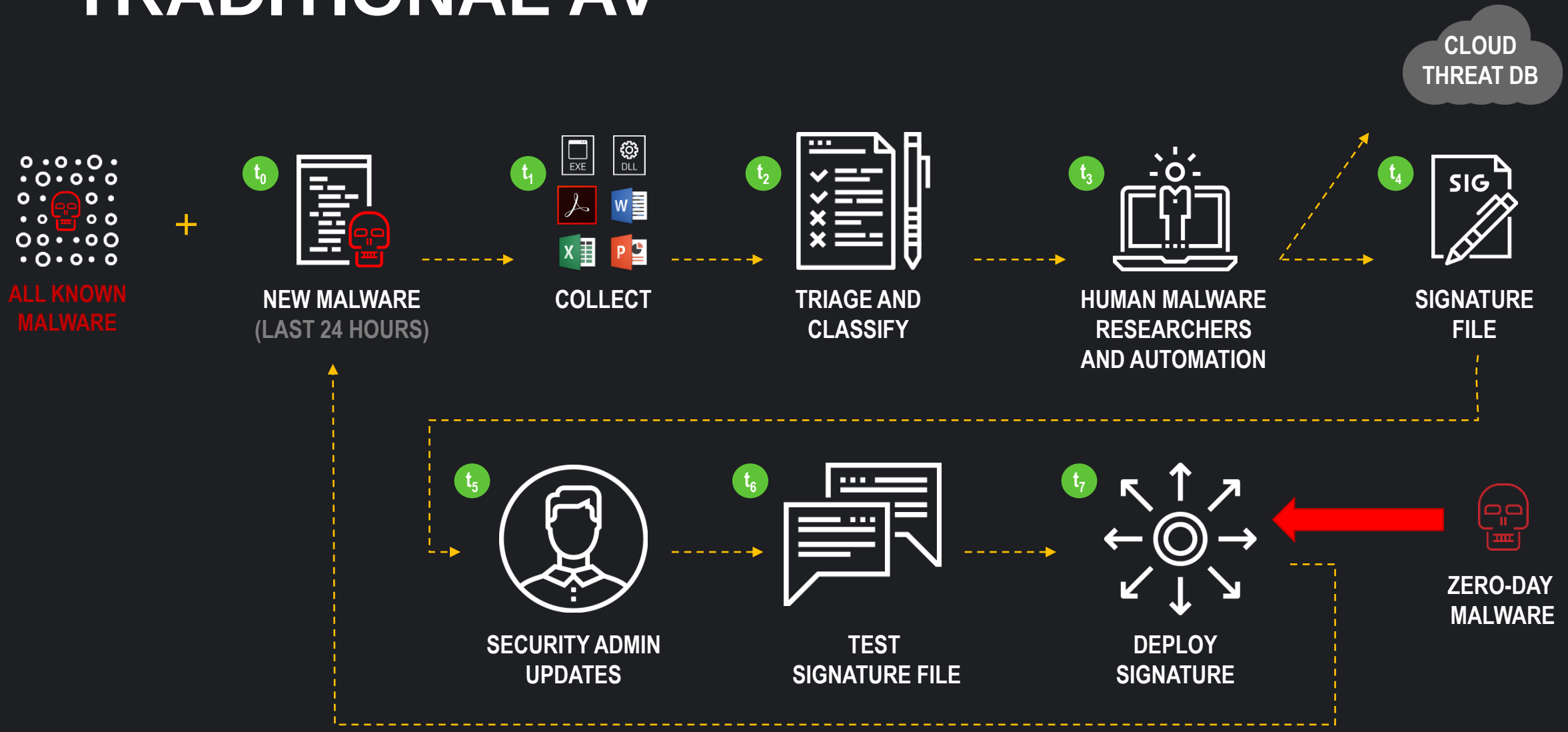
Bret Lenmark

blenmark@cylance.com
Senior Product Marketing Manager


WE MAKE SOFTWARE THAT PREDICTS,
then blocks, cyber attacks on the endpoint in real time using
pre-execution artificial intelligence algorithms.
CYLANCE

“Our antivirus software is unable to detect and prevent new and unknown threats”

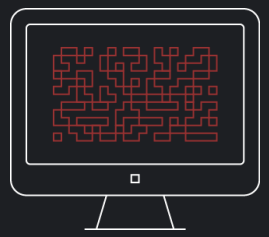
TRADITIONAL AV



BlackBerry | CYLANCE

BLACKBERRY CYLANCE NEXT GENERATION AI / AV

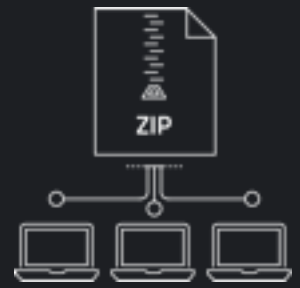
Good Files



Bad Files

Machine Learning

AI Math Model



Deploy To Endpoints

Every few months

BLACKBERRY CYLANCE NEXT GENERATION AI / AV

BlackBerry | CYLANCE

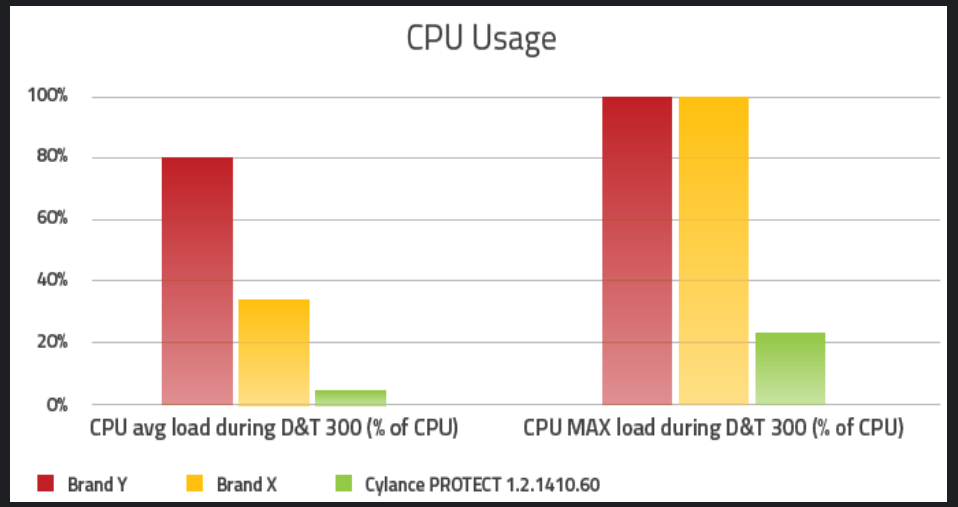
“Endpoint security agents slow down endpoint devices impeding end-user productivity”

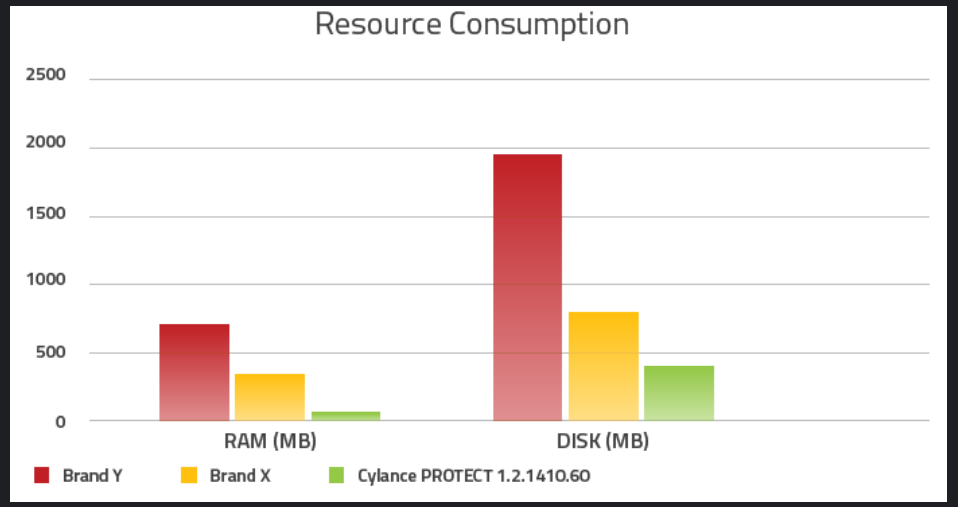
13X

Resource Consumption

5X

CPU Usage





BlackBerry | CYLANCE

If you're using a bloated antivirus program, you're likely losing over **$1,000 a year per employee!**

The average worker works **5 days** a week, **50 weeks** a year.

5 days
× 50 weeks
250 days

Let's assume the average knowledge worker looses **10 minutes** a day.

10 minutes
× 250 days
2,500 mins. / 42.67 hours

The average American worker earns **$26.00** an hour.

$26.00
× 42.67 hours
$1,109 .42

Source: https://www.bls.gov/news.release/empsit.t19.htm

BlackBerry | CYLANCE

“We regularly re-image infected endpoint devices creating work for our help desk and impeding end-user productivity”

Quantifying the Value of Prevention + EDR

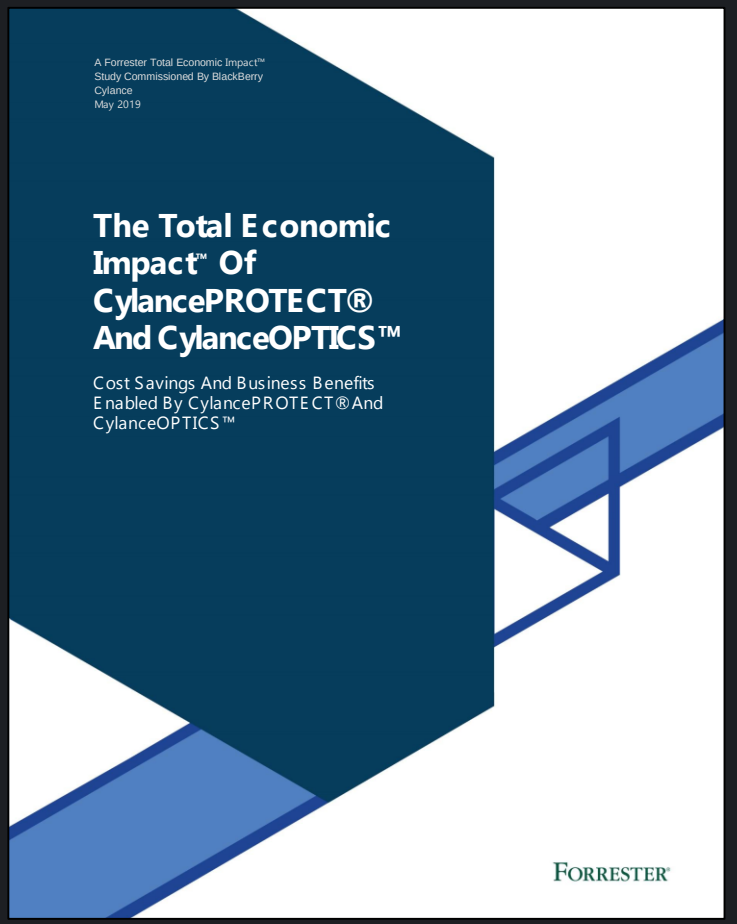
- Multi-national manufacturing
- Corporation 500 locations in 14 countries
- HQ in Europe
- $14B annual revenue
- 45,000 employees

Due Diligence
Interviewed BlackBerry Cylance Stakeholders.

Customer Interview
Interviewed one organization using CylancePROTECT® and CylanceOPTIC™ to obtain data.

Financial Model Framework
Constructed a financial model representative of the interview using TEI methodology.

Case Study
Employed four fundamental elements of TEI in modeling CylancePROTECT's and CylanceOPTIC's impact.



BlackBerry | CYLANCE

Quantified Benefits

The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

Reduce the expected cost of a major security breach by 25 percentage points with more effective malware detection and protection. Cylance uses AI to block potentially malicious applications and to stop attacks. The interviewee found Cylance to be more effective at threat blocking and protection vs. the legacy endpoint security solution, minimizing the likelihood and potential cost of a major security breach.

Faster investigation and remediation reduce lost time by 95%.
With Cylance fewer end-users are compromised. Faster threat investigation and remediation allows end-users to quickly resume productive work.

Cut machine reimaging by 97%.
With Cylance fewer machines were taken offline for reimaging. Less reimaging meant less lost end-user time and less IT time needed to reimage.

Eliminate manual software audits.
With Cylance, the cybersecurity team has more control over employee software downloads. If an employee downloads software that could be malicious, Cylance sends an alert to the security team. The software is blocked and the employee must ask for approval before running the software. This eliminates the need for manual software audits.

ROI 99%

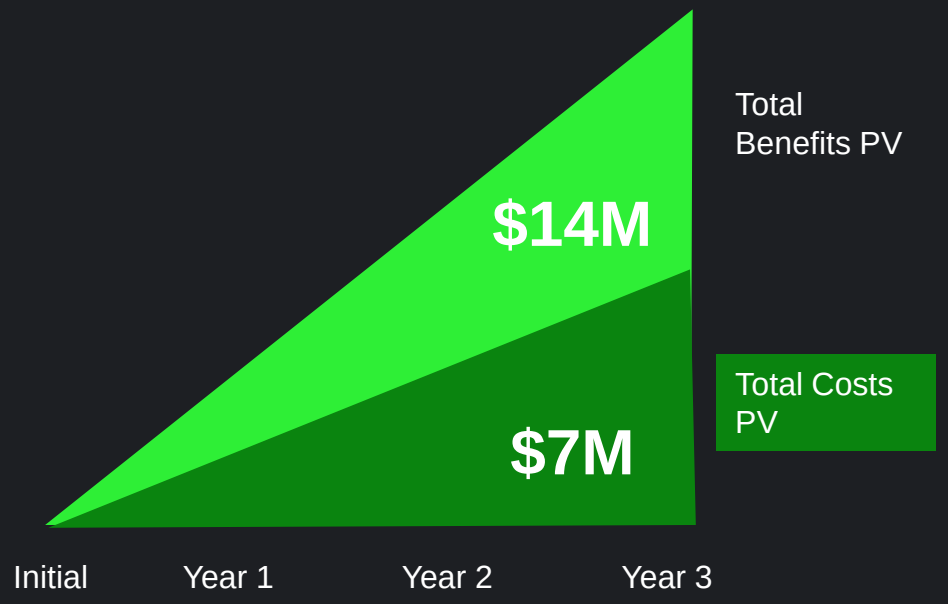
Benefits
$14 million

NPV
$7 million

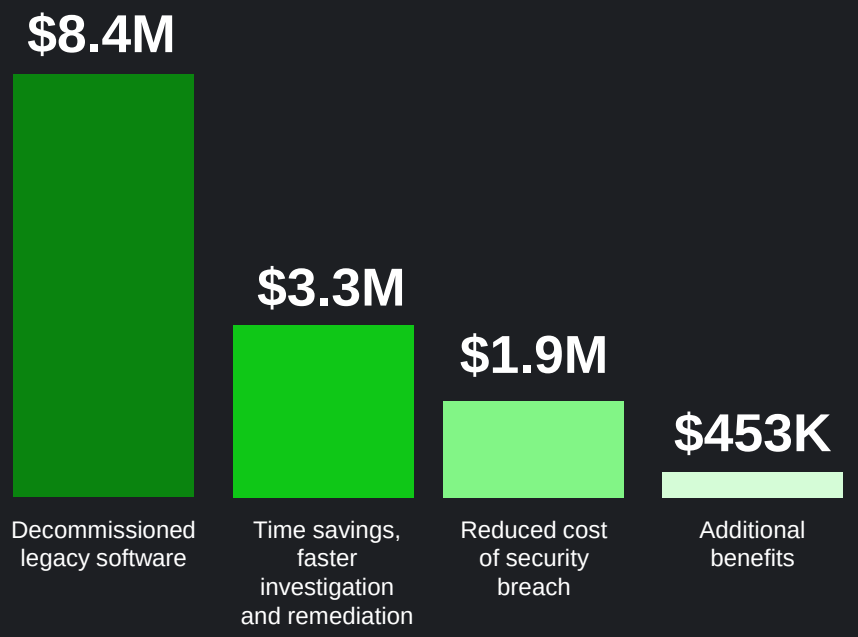
BlackBerry | CYLANCE

Financial Benefits

Financial Summary



Benefits (Three-Year)



BlackBerry | CYLANCE

“We have gone from around 50 compromised users each day to around zero or one somedays. The situation has totally changed for us.”

“Now with Cylance, if we detect something, we are able to look into the clients, preempt and deploy the mitigation protection just within minutes.”

“As we have lowered the number of infected machines, we are able to investigate where it’s coming from and what harm it’s doing to the machine instead of just remediating. Now we are able to find a root cause.”

CylancePROTECT leverages the power of machines, not humans, to dissect malware's DNA. Artificial intelligence then determines if the code is safe to run.

Microsoft

Mac

WHAT WE DO

- RELY ON AI & ML
- ANALYZE MALWARE AT THE DNA-LEVEL
- ADVANCED THREAT PREVENTION
- MINIMAL UPDATES
- WORK ON AIR GAPPED NETWORKS
- PREDICT AND PREVENT

WHAT WE DO NOT

- RELY ON HUMAN CLASSIFICATIONS
- REQUIRE ON-PREMISE INFRASTRUCTURE
- WAIT FOR THREATS TO EXECUTE
- REQUIRE CONSTANT UPDATES
- SIGNATURES
- HEURISTICS
- BEHAVIORAL ANALYSIS
- MICRO-VIRTUALIZATION
- SANDBOXING

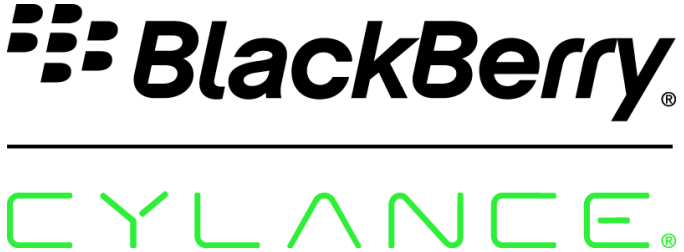
BlackBerry | CYLANCE

Questions

+

Answers

The AI Advantage



Jon Oltsik
Senior Principal Analyst and Fellow
jon.oltsik@esg-global.com

Bret Lenmark
Senior Product Marketing Manager
blenmark@cylance.com

Thank You