

 **BlackBerry** Intelligent Security. Everywhere.

CYLANCE ENDPOINT

November 16, 2023

Prepared for



SAFE HARBOR

Some of the statements made within this presentation constitute forward-looking statements and are made pursuant to the safe harbor provisions of applicable U.S. and Canadian securities laws.

Forward-looking statements are indicated by using words such as expect, will, should, model, intend, believe and similar expressions. Forward-looking statements are based on estimates and assumptions made by the company in light of its experience and its perception of historical trends, current conditions and expected future developments as well as other factors that the company believes are relevant.

Many factors could cause the company's actual results or performance to differ materially from those expressed or implied by the forward-looking statements, including the risk factors that are discussed in the company's annual report on Form 10-K and in our MD&A.

You should not place undue reliance on the company's forward-looking statements. Any forward-looking statements are made only as of the date of publication and the company has no intention and undertakes no obligation to update or revise any of them, except as required by law.

A fundamental Problem

ATTACKS HAVE BECOME INCREASINGLY COMPLEX OVER TIME. SO HAVE THE ENDPOINT SOLUTIONS USED TO DEFEND AGAINST THEM.



The world doesn't need more security noise.

Endpoint Security Complications

**Detection displacing
prevention**



**Require too many
people**



**Exposed and
Inflexible**



There's a better approach

From:

Detection displacing prevention

Require too many people

Delicate and Inflexible

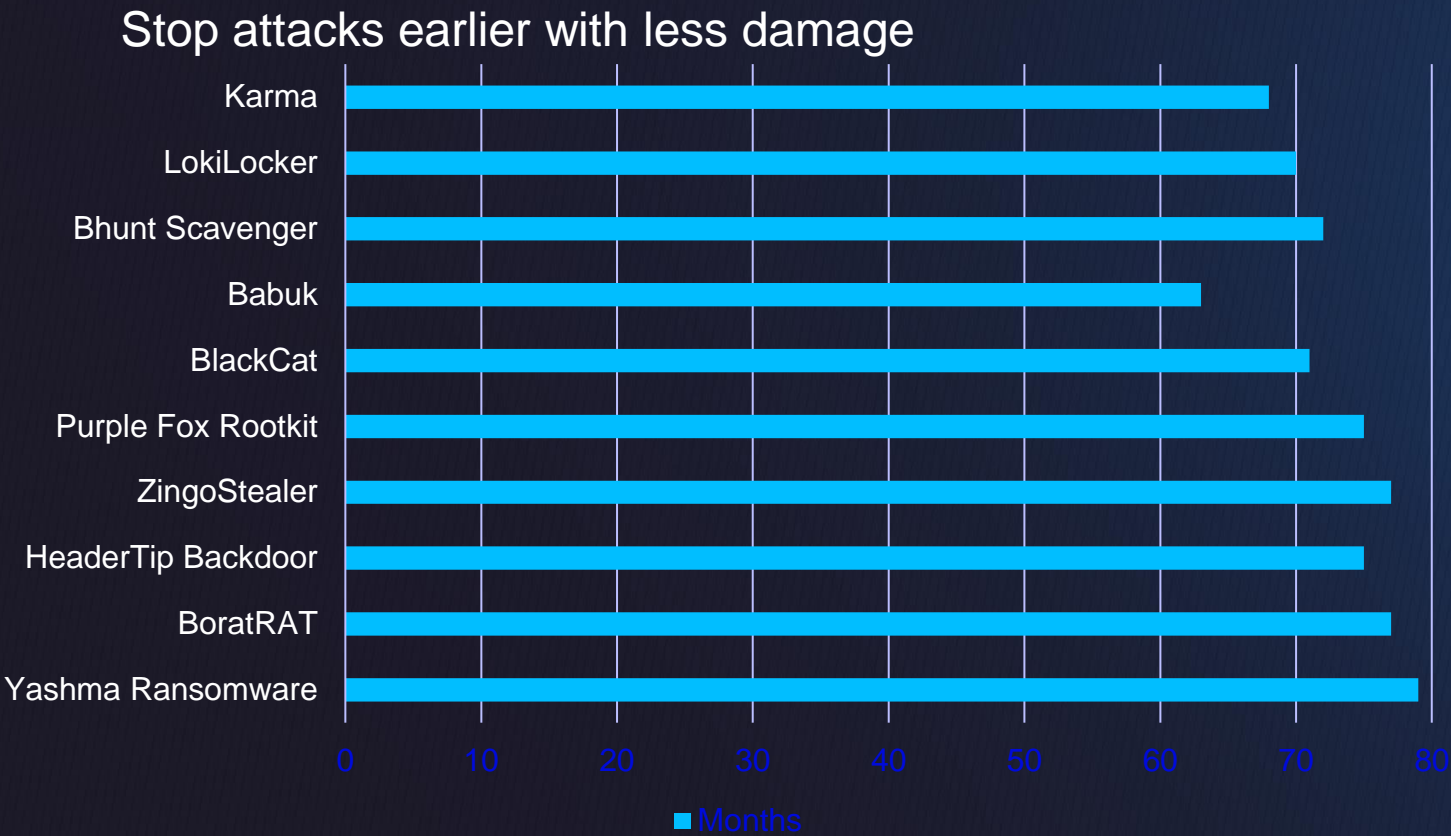
To:

Blocking attacks with a self-defending AI before wide-spread damage can occur

Less overall noise to sift through combined with simplified workflows to increase capacity for investigation and response

Effective defense in “less-than-perfect” environments and situations – in both connected, disconnected, resource constrained,

Self-Defending AI



Battle-Proven, Autonomous Prevention

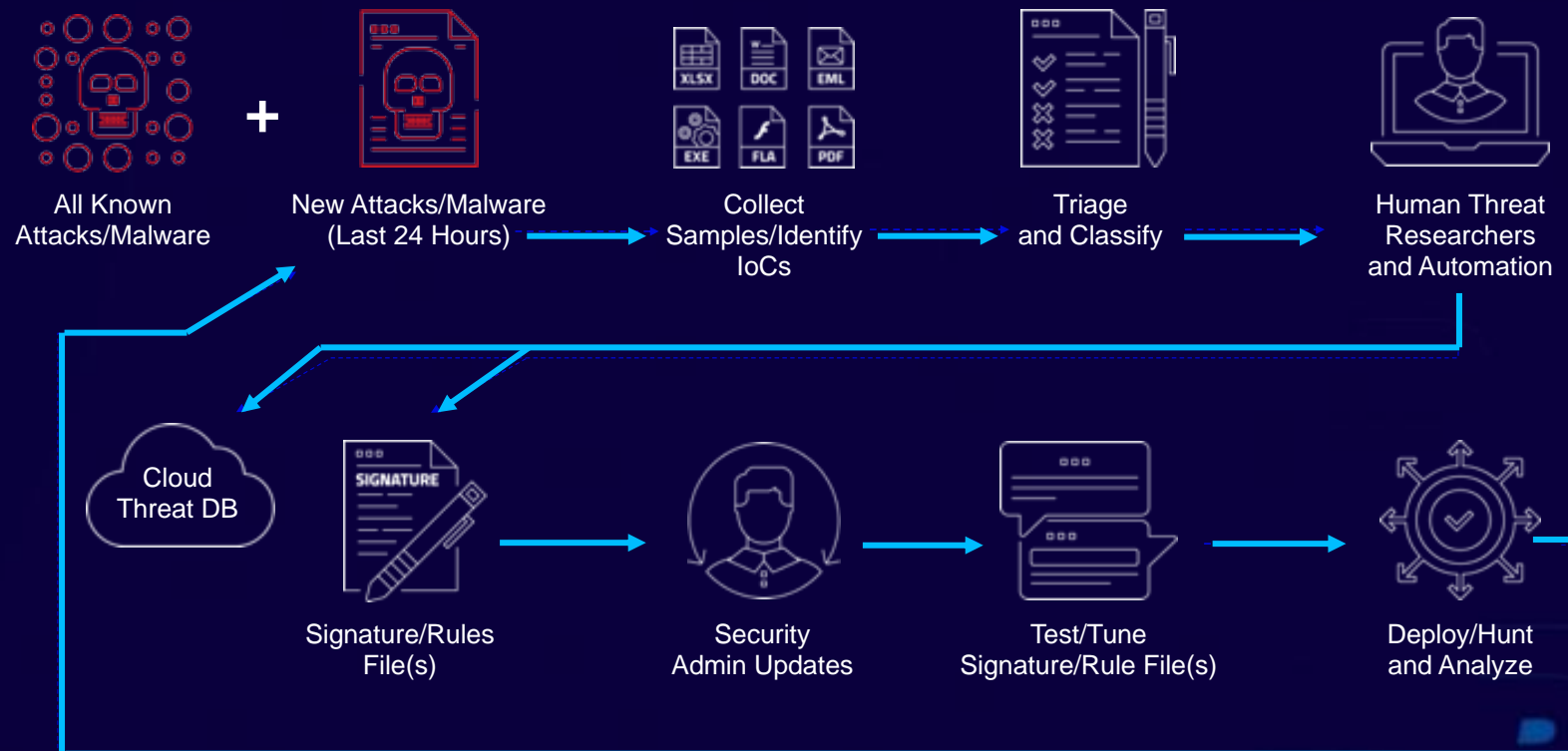
- Effective even when systems are offline
- Minimal tuning, negligible false-positives

Consistently demonstrates the ability to block the most serious of threats years before they appear¹

1. Internal testing conducted by running specific threats with an AI model in the past, test results for each outlined attack has been published on our BlackBerry Threat Vector Blog

Reactive Approach

REACTIVE APPROACH



LEARNING FROM HISTORY – COLONIAL PIPELINE

Predictive Cylance AI - Providing Prevention for over 67 months (about 5 and a half years)!

WITH AI



OCT 14, 2015

Cylance AI Model Blocks



MAR 29, 2016

Cylance AI Model Blocks



FEB 6, 2017

Cylance AI Model Blocks



OCT 15, 2020

Cylance AI Model Blocks



MAY 7, 2021

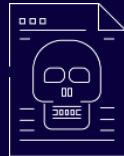
Current Cylance AI Blocks

WITHOUT AI



MAY 6, 2021

Corporate VPN Used



MAY 7, 2021

Zero-Day Ransomware
begins destroying data

Pipeline shutdown



MAY 7, 2021

Obtain samples and issue
signature/rule updates for
DarkSide



MAY 12, 2021

Pipeline resumes operation



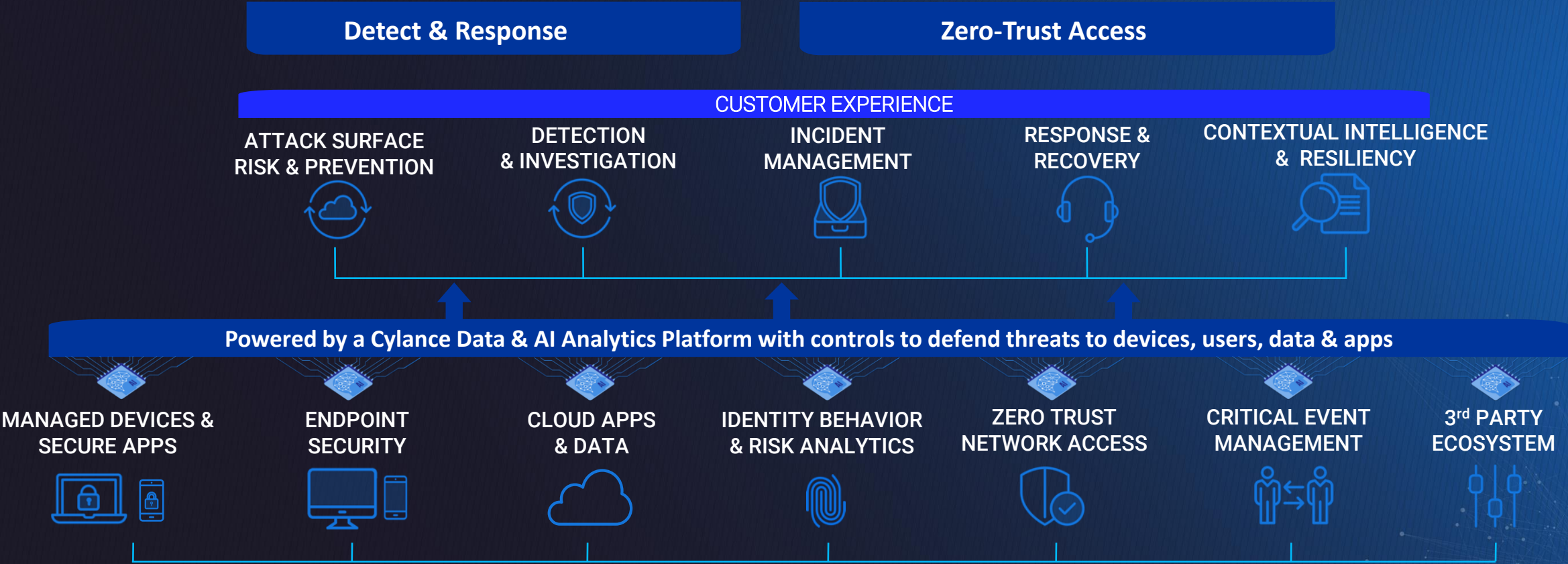
ONGOING

Vendors monitor for new
samples

Customers must continue
to hunt for IoCs

Cybersecurity Vision

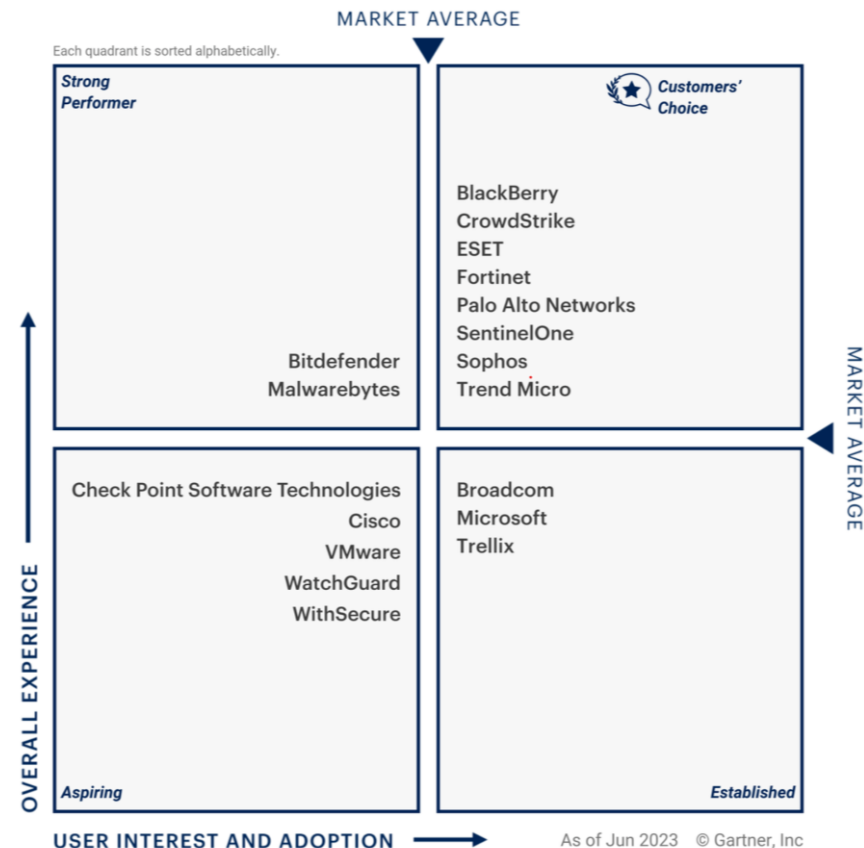
Our Mission: To enable businesses to operate with clarity on their cyber risk and have autonomous resilience and continuity when attacked.





CylanceENDPOINT Overall Rating

4.7 ★★★★★



2023 Gartner, Inc. The Gartner Peer Insights Customers' Choice badge is a trademark of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner® Peer Insights™ content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties

36%
More malware Stopped

up to 12x
Faster to detect

20x
Less overhead

(*based on preliminary Tolly Group performance & efficacy testing)

Improved Threat Resiliency: AI and Classification

The Role of AI in Defensive Cybersecurity

Predictive

(Machine Learning / Deep Learning)

***Stops attacks automatically.
Doesn't chat with people.***

Good for automating
defense early in kill-chain

Prevents zero-day attacks | Stops lateral movement | Organizes alerts

Generative

(Large Language Models like ChatGPT)

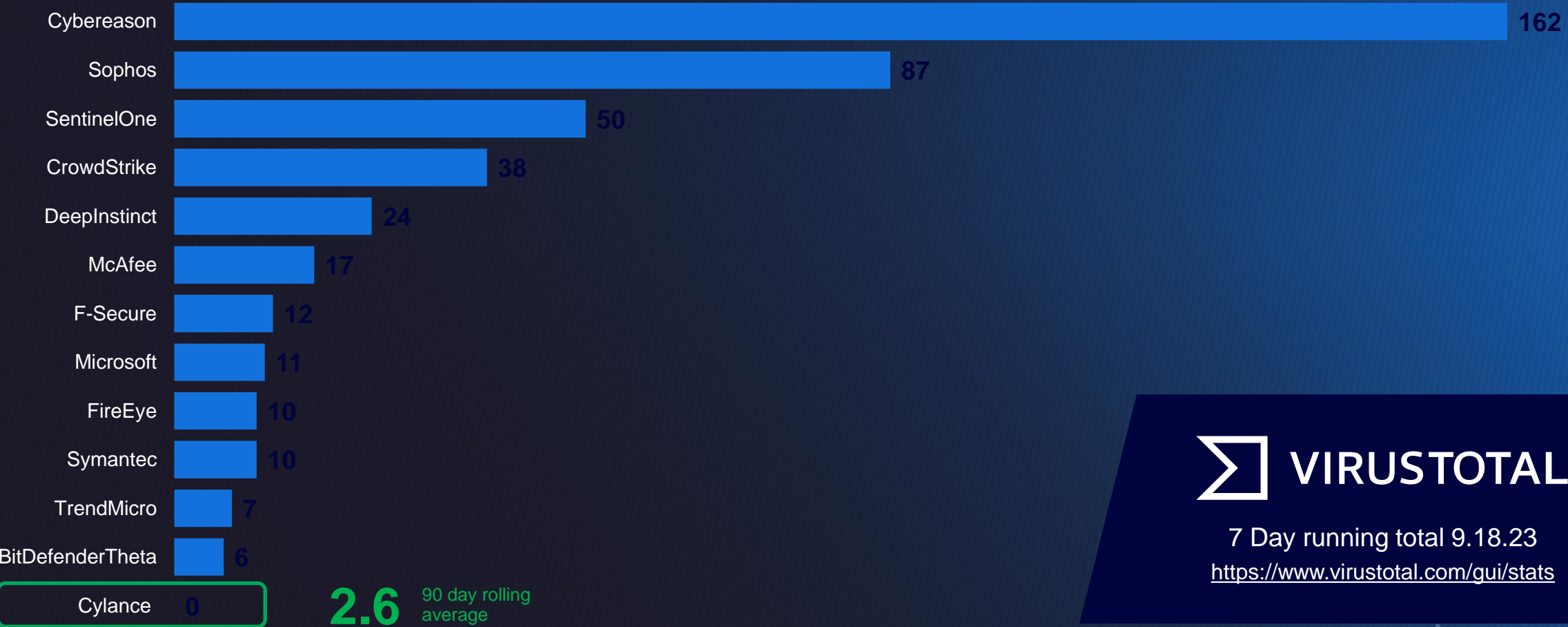
***Chats with people to speed up work.
Doesn't stop attacks.***

Good for helping make sense of
incidents that have already occurred

Product assistance | Threat intelligence context | Incident summarization

Consistently Low False Positives By Design

7-day Total False Positives



7 Day running total 9.18.23

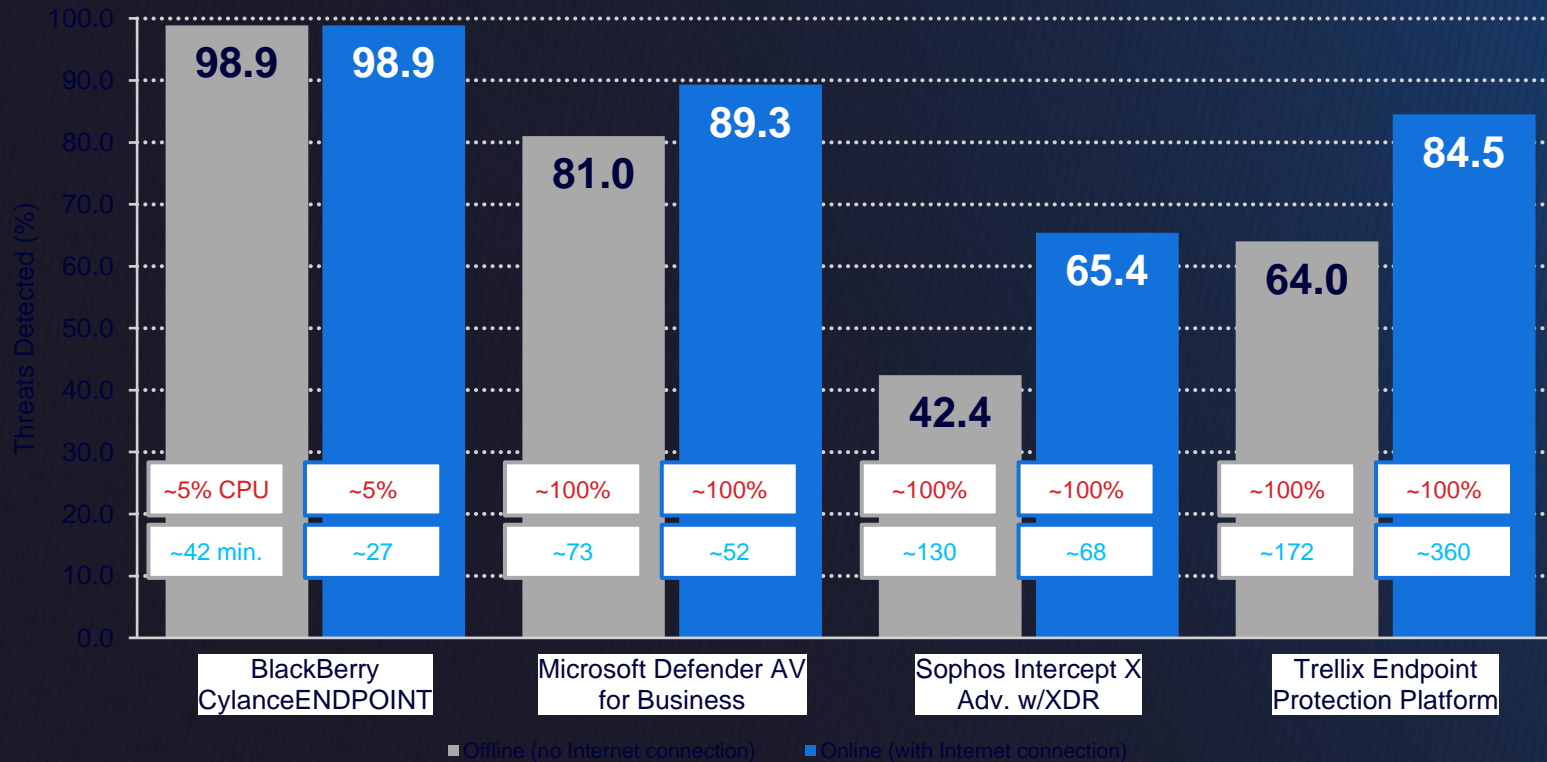
<https://www.virustotal.com/gui/stats>

Delivering Outcomes that Matter



Windows 10 Endpoint Protection Efficacy & Response Utilization

Scanning Two Collections of 1,000 Recent VirusTotal Samples
(Detection % determined by number of files remaining in folder after scan)



Stops More Attacks

18% more than Microsoft

35% more than Trellix

57% more than Sophos

Faster Detection

1.9x faster than Microsoft

13x faster than Trellix

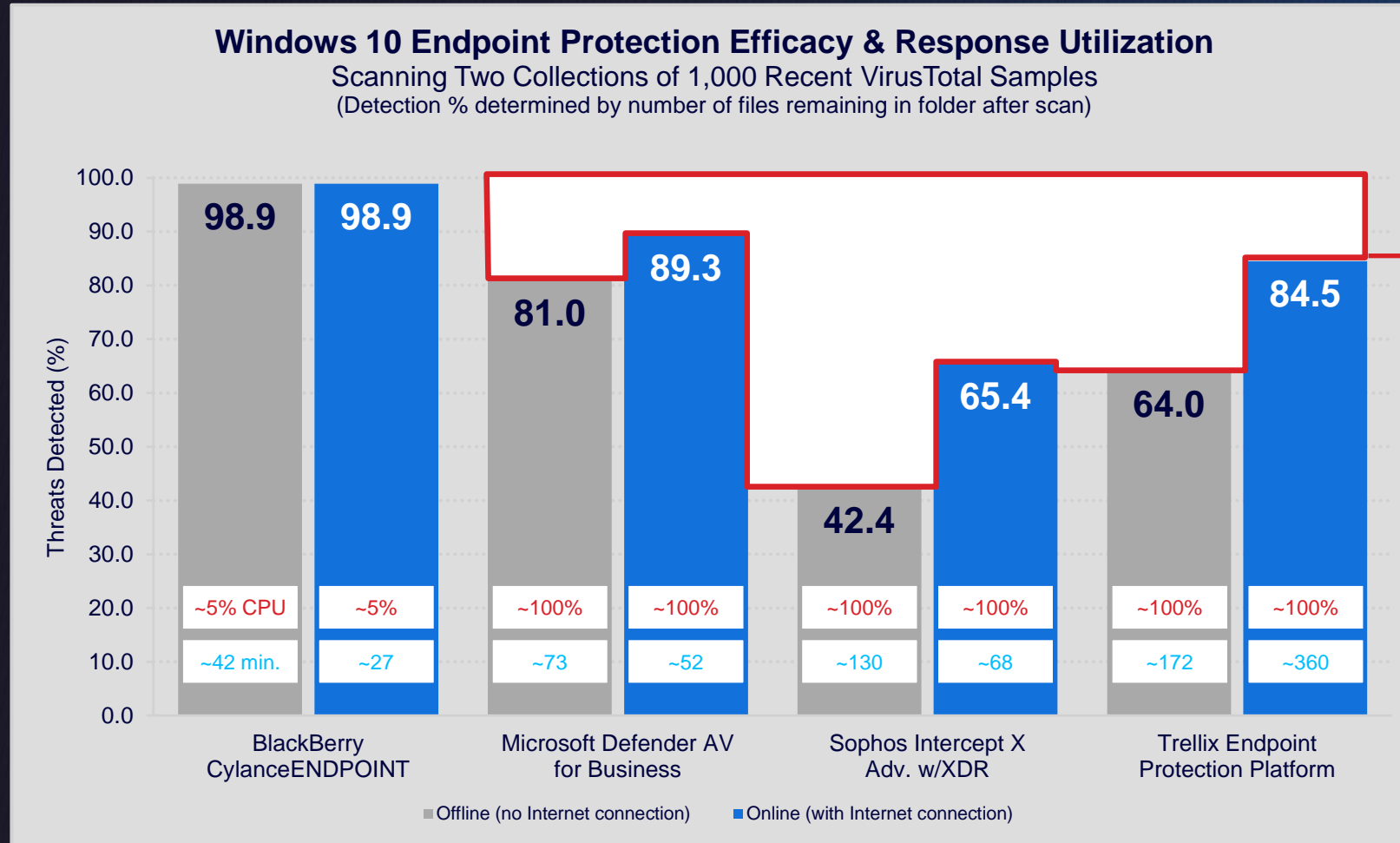
2.5x faster than Sophos

90% Less CPU Utilization

than other vendors in the same comparative test

Without Depending on Internet Connection

Unpacking the Whitespace – What Does This Difference Mean?



- ↑ More security incidents
- ↑ More SOC burden
- ↑ More IT burden
- ↑ More wasted end-user time
- ↑ More energy consumption

How Can We Help You?



Demo

BlackBerry Points of Contact

Danny Sanok – Principal Product Manager, dsanok@blackberry.com, 904-540-9980
Tab Holder – Director, US DoD Federal Sales, tholder@blackberry.com, 703-943-0556
Kevin Campbell – DoD Account Manager, kecampbell@blackberry.com, 571-214-6144
Raj Thakore – Senior Sales Engineer, rthakore@BlackBerry.com, 267-315-1731