Moving Your Environment into a State of PREVENTION

DAVE ALFARO
MANAGING DIRECTOR, THREATZERO

SAFE HARBOR

The information in this presentation is confidential and proprietary to Cylance® and may not be disclosed without the permission of Cylance. This presentation is not subject to your license agreement or any other service or subscription agreement with Cylance. Cylance has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation and Cylance's strategy and possible future development, product, and/or platform direction and functionality are all subject to change and may be changed by Cylance at any time for any reason without notice. The information on this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is for informational purposes and may not be incorporated into a contract. Cylance assumes no responsibility for errors or omissions in this document.

PRESENTER

DAVE ALFARO

MANAGING DIRECTOR, THREATZERO

- 18+ year security career
- Career spans security and network engineering, penetration testing, firewall design and implementation, enterprise security architecture, privileged identity management, vulnerability management, and Endpoint security.
- Managed the design and implementation of one of the world’s largest scale DoD vulnerability management solutions (US Army)
- Managed and grew successful consulting practices for several security vendors and firms.

TIME

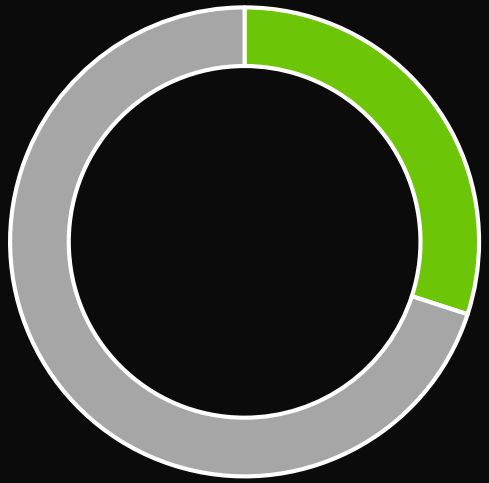
Time is truly a finite resource

BlackBerry | CYLANCE.

TIME TO VALUE

- Skilled resources?
- Subject matter expertise?
- Implied risk?

What is the true cost?



30%

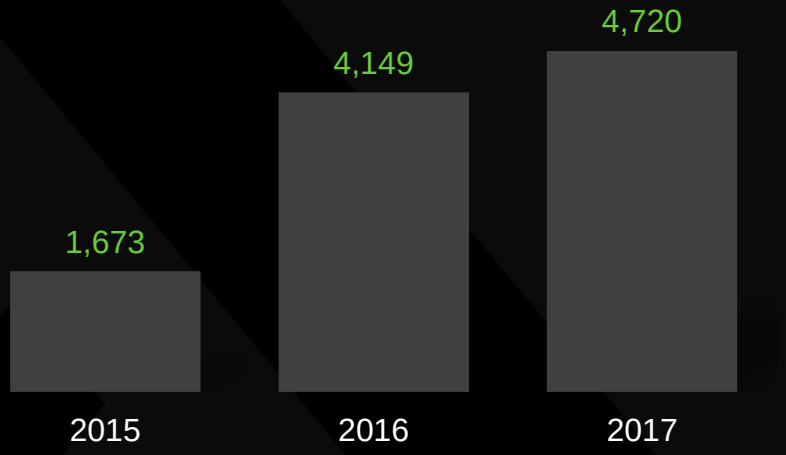
of all new security investments were not being used at all or were underutilized[1]

"Target supposedly **spent over $1 million** on an anti-malware solution poorly configured at the time of its 2013 data breach."

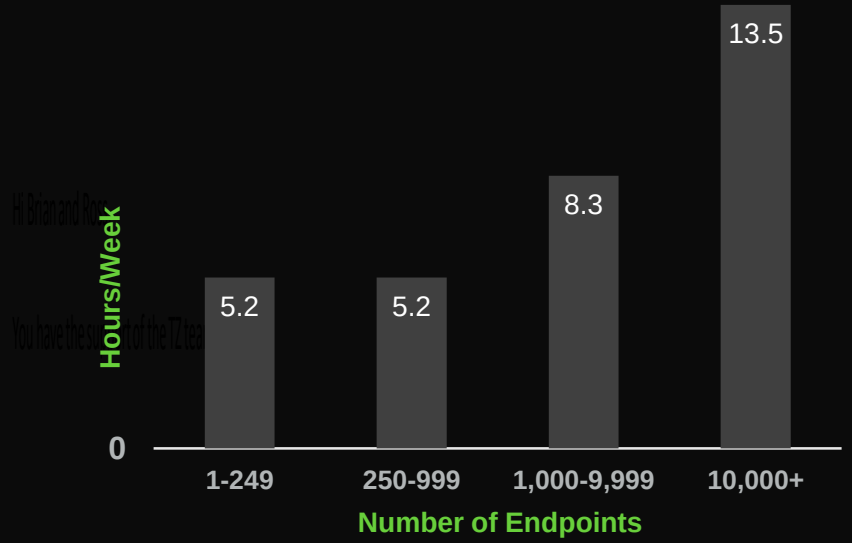
[1]Source: www.csoonline.com, "How to stop wasting money on security shelfware"

TIME IS NOT ON OUR SIDE

The number of incidents and the resource requirements to handle them..



Number of Reported Breaches



Man hours to respond to compromised hosts

PREVENTION

Deployment vs. Prevention

BlackBerry | CYLANCE

CYLANCE

Report Card

Grading Scale:

95 – 100% - A

94 – 85% - B

84 and Less - C

Files Analyzed	787,688,185
C	Overall Grade: 45.89%

Coverage Breakdown:

*Report generated as of 08/16/2016

Category	# Of Hosts/Files Under Category	Percentage Of Category	Description
Malware	5,374/7,098	75.71%	*The number of malware threats that have been quarantined.*
Potentially Unwanted Programs (PUPs)	22,067/34,259	64.41%	*The number of PUPs that have been quarantined/removed or whitelisted.*
Auto-Quarantine	543/13,452	4.04%	*The number of devices with Auto-Quarantine enabled for Unsafe and Abnormal threats.*
Memory Protection	0/13,452	0.00%	*The number of devices using Memory Protection in Block or Terminate mode.*
Script Control	0/13,452	0.00%	*The number of devices using Script Control in Block mode.*
Asset Inventory	11,644/13,452	86.56%	*The number of devices that have been online in the last 30 days.*
Upgrade Management	12,171/13,452	90.48%	*The number of devices on either of the two most recent versions of CylancePROTECT.*

VALUE OF CYLANCEPROTECT

- Full Auto-Quarantine
- Expert Handling of Discovered Threats
- Memory Protection Blocking Exclusion Handling
- Script Control / Macro Protection Handling
- Best Practices Training
- Accelerated Implementation, Minimal Impact

SUBSCRIPTION THREATZERO

- Quarterly HealthCheck Reports
- Threat Status Review
- Feature and ROI Status Review
- Updates of Agent Version
- Maintains Prevention Status

BlackBerry | CYLANCE

CYLANCE

Report Card

Grading Scale:

95 – 100% - A

94 – 85% - B

84 and Less - C

Files Analyzed	787,688,185
A	Overall Grade: 95.94%

Coverage Breakdown:

*Report generated as of 08/16/2016

Category	# Of Hosts/Files Under Category	Percentage Of Category	Description
Malware	7,022/7,098	98.92%	*The number of malware threats that have been quarantined.*
Potentially Unwanted Programs (PUPs)	33,745/34,259	98.50%	*The number of PUPs that have been quarantined/removed or whitelisted.*
Auto-Quarantine	13,355/13,452	99.28%	*The number of devices with Auto-Quarantine enabled for Unsafe and Abnormal threats.*
Memory Protection	13,060/13,452	97.08%	*The number of devices using Memory Protection in Block or Terminate mode.*
Script Control	12,904/13,452	95.93%	*The number of devices using Script Control in Block mode.*
Asset Inventory	11,679/13,452	86.82%	*The number of devices that have been online in the last 30 days.*
Upgrade Management	12,783/13,452	95.03%	*The number of devices on either of the two most recent versions of CylancePROTECT.*

THREATZERO SERVICES

Foundational ThreatZERO

Outcome-based provable prevention services

Subscription ThreatZERO

Foundational implementation and quarterly maintenance program

Partner-Delivered ThreatZERO

Accredited partners leveraging ThreatZERO tools, processes, and methodologies

Resident Expert

Dedicated long term staff augmentation

BlackBerry | CYLANCE

CASE STUDY: MID-SIZED US BANK

- Customer: Mid-sized US bank
- Number of endpoints: 13,000
- Full protection used throughout the bank
  - **Standard remote engagement**
  - **Agents Deployed: 13,780**
  - **13,780 in AQT (100%)**
  - **13,761 in Memory Defense**
  - **~12,000 in Script Alert**
- Multiple renewals Client since 2016

CASE STUDY: RAPID DEVELOPMENT

- Customer: Global consumer brand company
- Number of endpoints: 120,000K
- Very Aggressive timeline
  - **Standard Remote engagement 7M**
  - **Agents Deployed: 107,000 (80K in one weekend)**
  - **107,000 in AQT**
  - **107,000 in Memory Defense**
  - **70,000 in Script Control Blocking**
  - **OPTICS fully deployed**
- Highly motivated team and executives
- Organization-wide buy in

DELIVERING PREVENTION-BASED SECURITY SOLUTIONS

Integrated Practice Areas

Dedicated Engagement Manager

Holistic Approach

Customized Solutions

World-Renowned Security Authorities

Global Coverage with Local Attention

IOT / EMBEDDED SYSTEMS

INCIDENT CONTAINMENT & FORENSICS

RED TEAM SERVICES

ThreatZERO™

INDUSTRIAL CONTROL SYSTEMS

STRATEGIC SERVICES

EDUCATION

BlackBerry | CYLANCE

Let us prove it to you.

ThreatZERO is ready to help YOU move to a state of PREVENTION.

proservices@cylance.com
+1-877-973-3336

Learn more about our ThreatZERO Services

Contact us

- Your account manager
- Dave Alfaro at **dalfaro@cylance.com**

THANK YOU