SPCINTERNATIONAL

THE IT BUSINESS BUILDER

ONLINE

Get Ready for Next Generation EndPoint Protection

Your Presenter

Erick Simpson

Vice President & CIO, SPC International Online

A strategic IT business transformation specialist experienced in improving top and bottom-line business performance by increasing operational efficiencies, boosting marketing and lead generation outcomes, accelerating sales velocity, shortening sales cycles and maximizing service efficiencies.

Over 30 years of experience in the IT industry as an Enterprise CIO, MSP, and Business Process Improvement Expert with hundreds of successful IT Solution Provider, MSP and Cloud practice business improvement consulting engagement outcomes, Erick has worked with numerous clients on both the buy and sell side of the M&A process.

A highly sought-after IT, Cloud and Managed Services expert, author and speaker, Erick has authored 40 best practice guides and 4 best-selling books including "The Guide to a Successful Managed Services Practice", “The Best I.T. Sales & Marketing BOOK EVER!”, “The Best I.T. Service Delivery BOOK EVER!” and “The Best NOC and Service Desk Operations BOOK EVER!”.

Erick
Simpson

Vice President & CIO
SPC International Online
www.spc-intl.com

www.linkedin.com/in/ericksimpson
https://amazon.com/author/ericksimpson

IT, MSP and Cloud Business Improvement Expert

- IT Business Improvement Specialist focused on people, process and product
- Experienced buy- and sell-side M&A consultant
- Certified Behavioral Specialist
- IT Solution, Managed Services and Cloud sales optimization and QBR improvement specialist
- Expert IT Solution and Service tiering, packaging, bundling and pricing strategist
- NOC/Service Desk and Dispatch Incident Management Workflow specialist
- Skilled in CRM, PSA and RMM configuration, integration, reporting and analysis
- Project Management specialist
- Skilled Virtual/Interim IT Solution Provider CIO and COO

Copyright 2015 Trend Micro Inc.

Speaker Spotlight

Mike Murphy

Global Integrated Marketing, Trend Micro

Mike is a proven results-oriented business and technical leader with an extensive background in partner/customer business development, execution of marketing programs and solution sales. He excels in developing and implementing channel strategies and programs that consistently result in opening profitable new market segments that increase sales, improve profits and extend market penetration. Mike's specialties include channel marketing, sales, program/project management, business strategy, leadership, drive for results, communication, cross-group collaboration, decision making, influencing others, dealing with ambiguity, computer software, relationship building and contract negotiation.

Mike Murphy
MCSE

Global Integrated Marketing
Trend Micro
www.trendmicro.com

- **Over 20 years experience in the IT Industry**
- **MCSE, CCNA, CNE**
- **Microsoft TS2 Founding Member**
- **Microsoft Across America Trucks**
- **Microsoft Community Connections**

Trend Micro

- 27 years focused on security software
- History of innovation
- 8 consecutive years on Dow Jones Sustainability Indexes
- Customers include 48 of top 50 global corporations
- 5200+ employees, 38 business units worldwide

500k commercial customers &
155M endpoints protected

Consumers

Small Business

Midsize Business

Enterprise

Framing today's conversation

Speaker Spotlight

Andrew Stevens

Director, Global Product Marketing, Endpoint Solutions
Trend Micro

Andrew Stevens is the Director of Endpoint Protection solutions at Trend Micro and has over 20 years' experience in product management and product marketing, leading the strategy for Go-To-Market plans, messaging, pricing & packaging, planning, design, release, and enhancement of innovative technology offerings on a global level.

Thinking about replacing AV with Next Gen Endpoint?

June 1, 2016

Andrew Stevens – Trend Micro

Endpoint Protection Problems

Copyright 2015 Trend Micro Inc.

Too many malware incidents

Fewer boundaries

New apps
New devices
New locations, no VPN
New threats

No protection from on-premise defenses

Cybercrime big business

Cyber-Safe

'Ransomware' crime wave growing

by David Fitzpatrick and Drew Griffin @CNNTech

April 4, 2016: 6:14 PM ET

SC Magazine > News > U.S., Canada issue ransomware alert

Doug Olenick, Online Editor

April 05, 2016

U.S., Canada issue ransomware alert

Ransomware by the Numbers

$200-$10k

Typical Ransom Paid

-FBI, April 2016

>50%

% of US Hospitals hit by Ransomware in 2015

-HIMSS Analytics, 2016

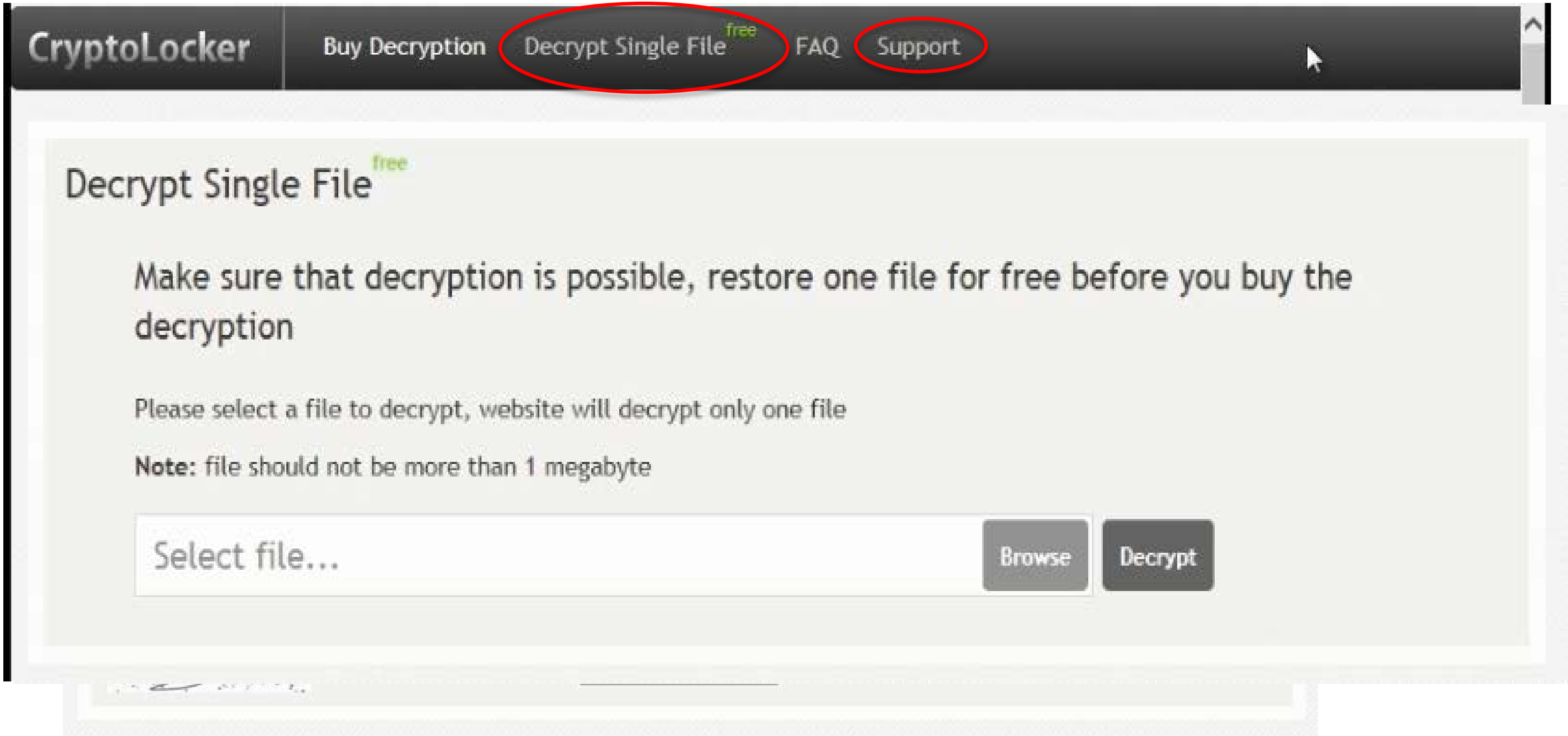
90,000

#of systems per day infected by Locky Ransomware

-Forbes, February 2016

Copyright 2015 Trend Micro Inc.

Ransom Practices

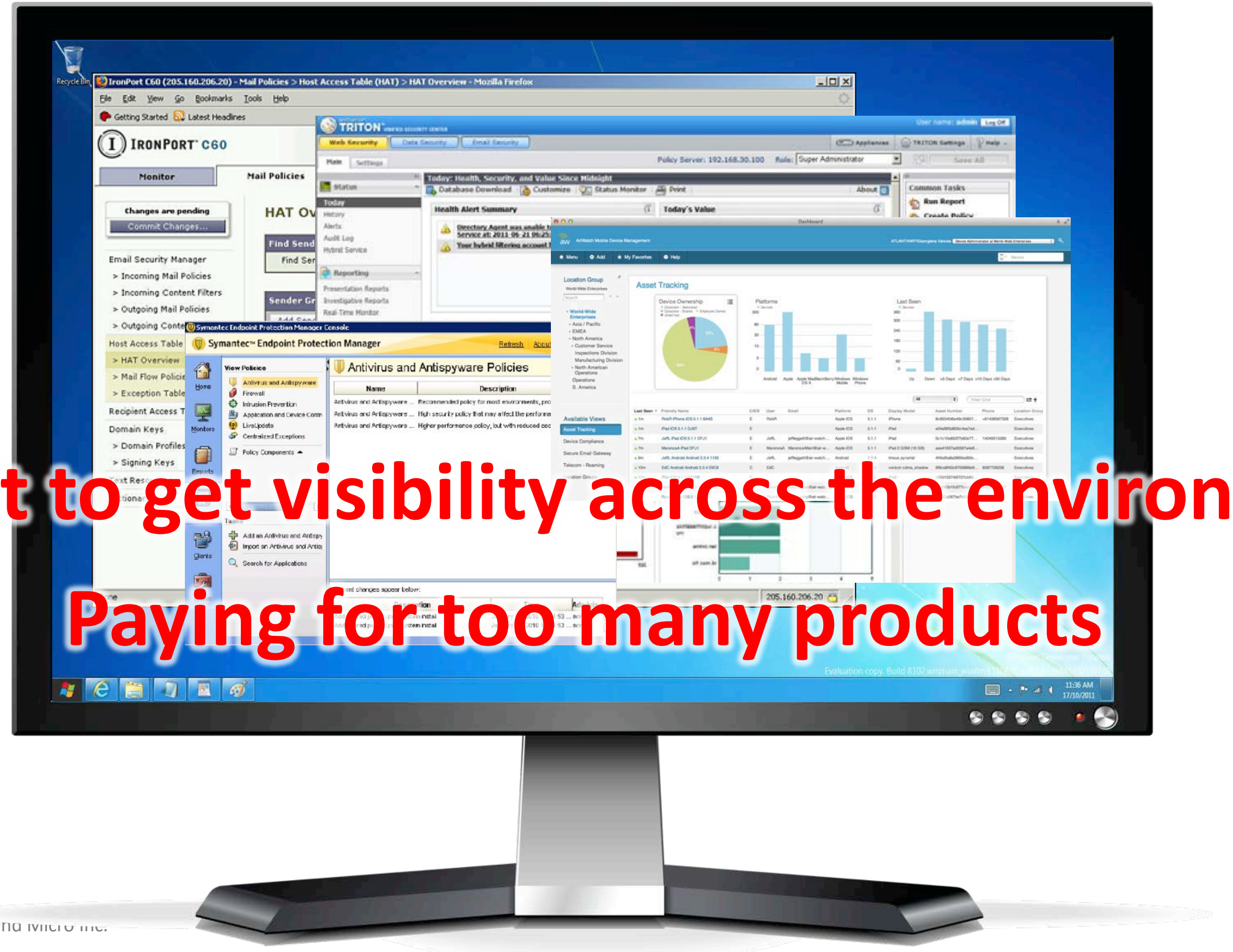


Decrypt Single File free

Make sure that decryption is possible, restore one file for free before you buy the decryption

Please select a file to decrypt, website will decrypt only one file

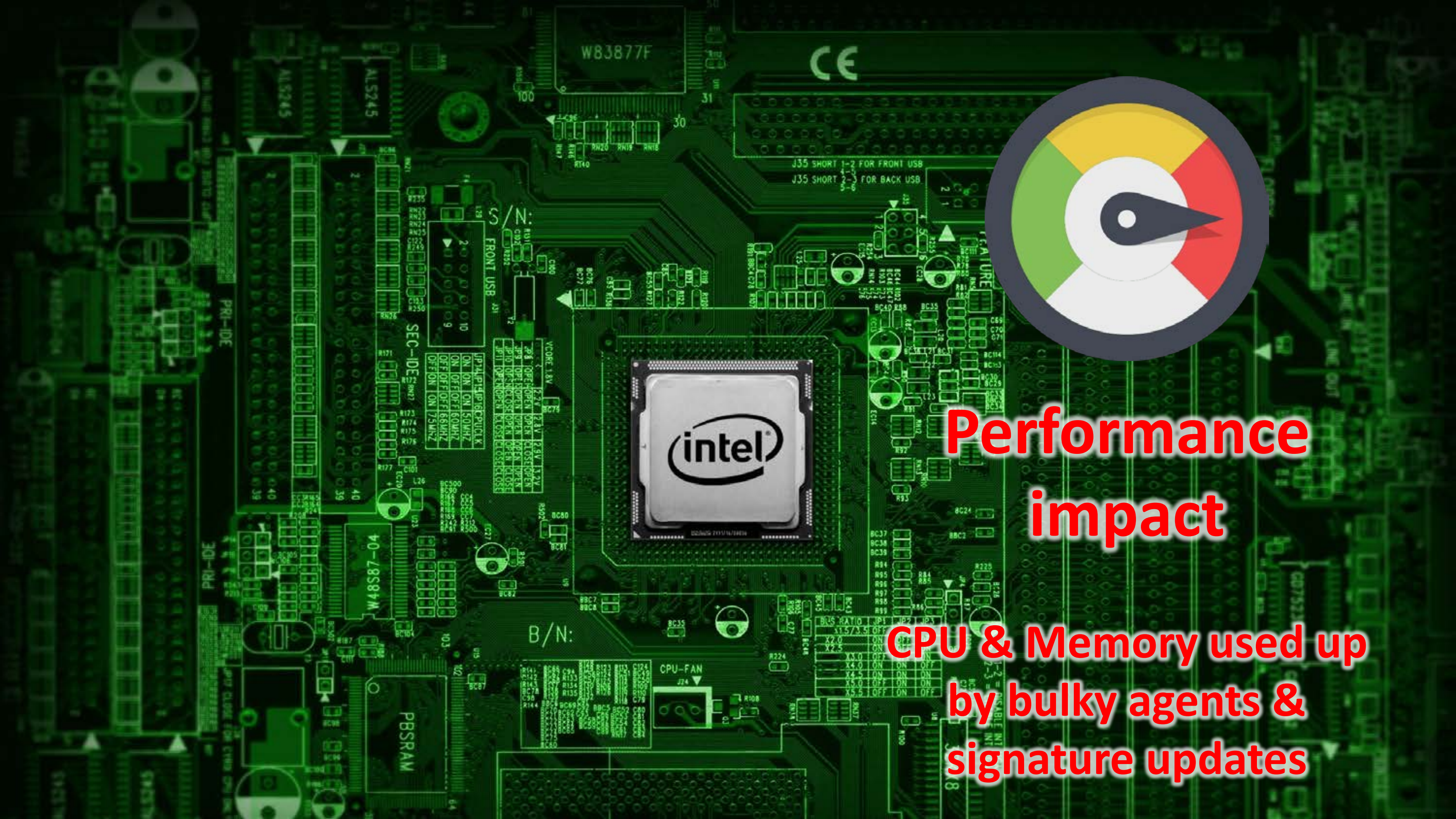
Note: file should not be more than 1 megabyte



Difficult to get visibility across the environment

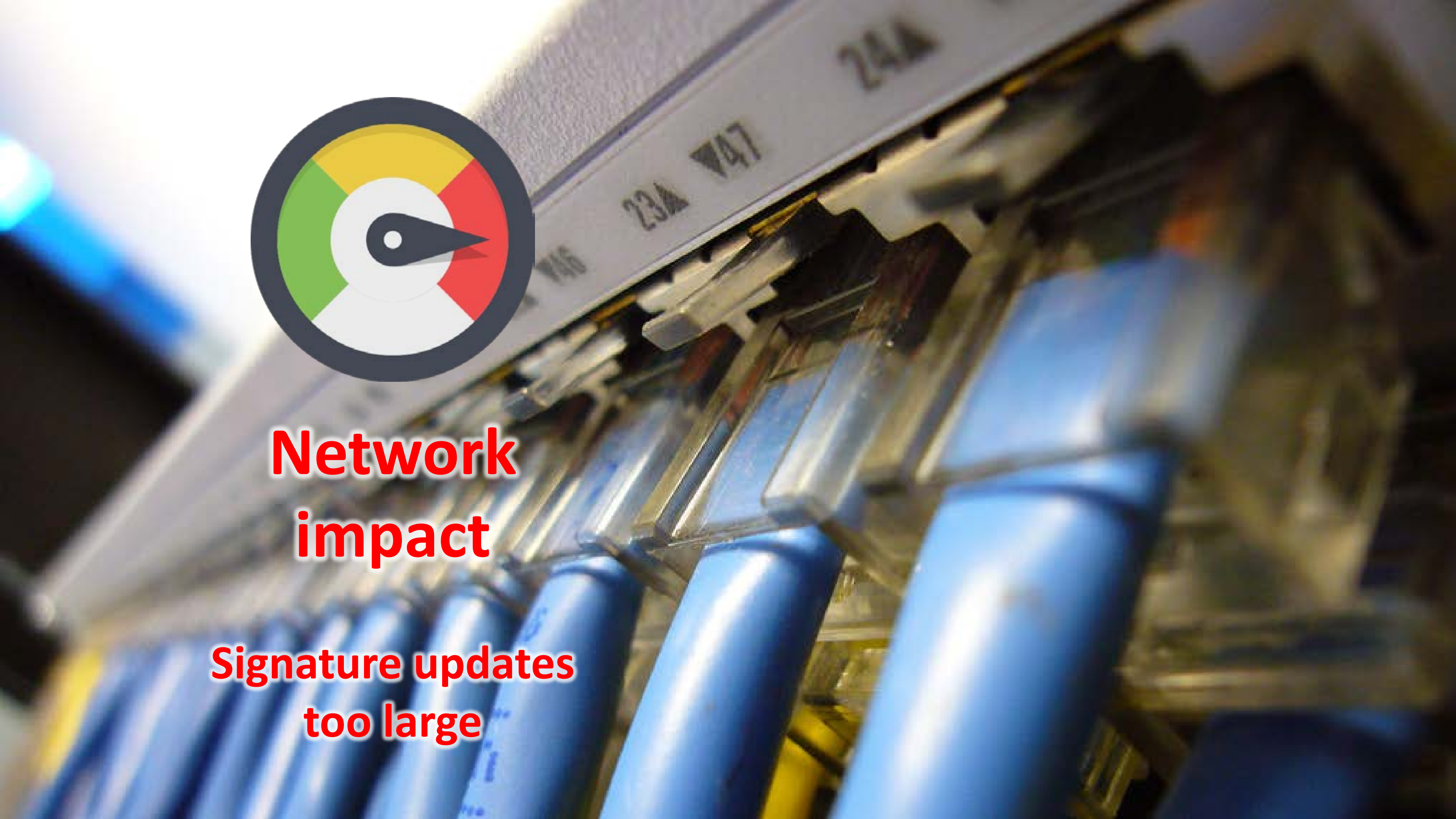
Paying for too many products

Copyright 2015 Trend Micro Inc.



Performance impact

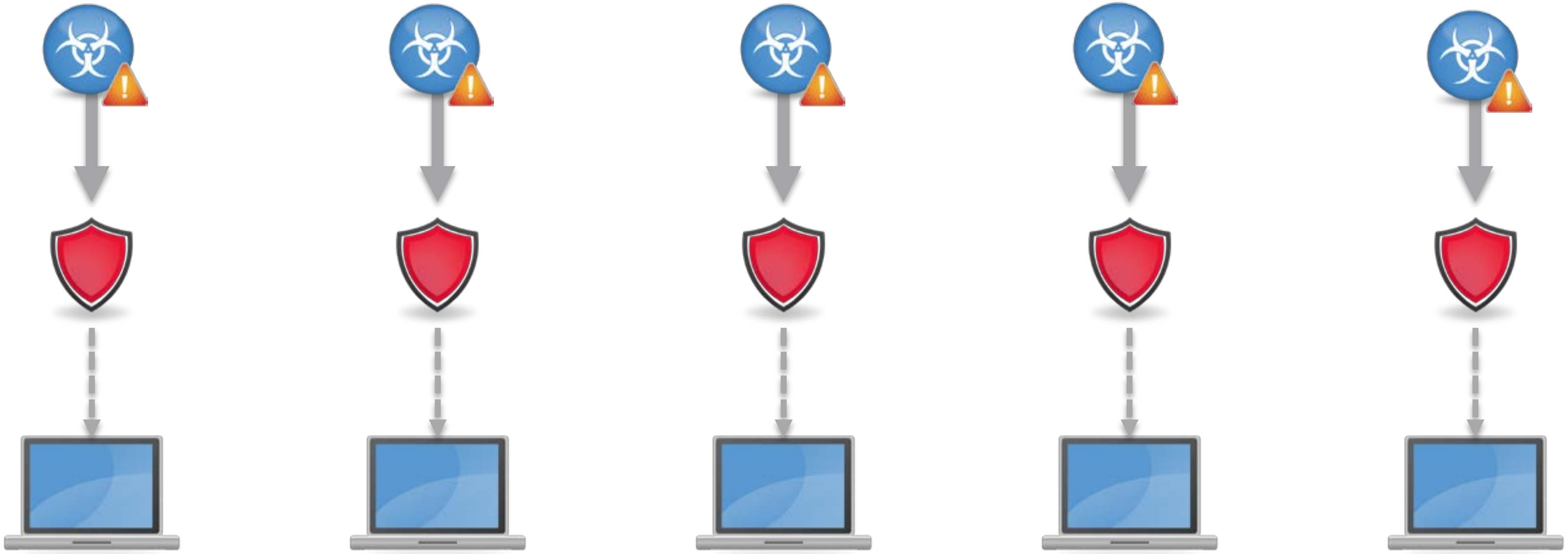
CPU & Memory used up by bulky agents & signature updates



Network impact

Signature updates too large

Beyond AV: Next Gen Techniques



Modern Anti-Malware

Application Whitelisting

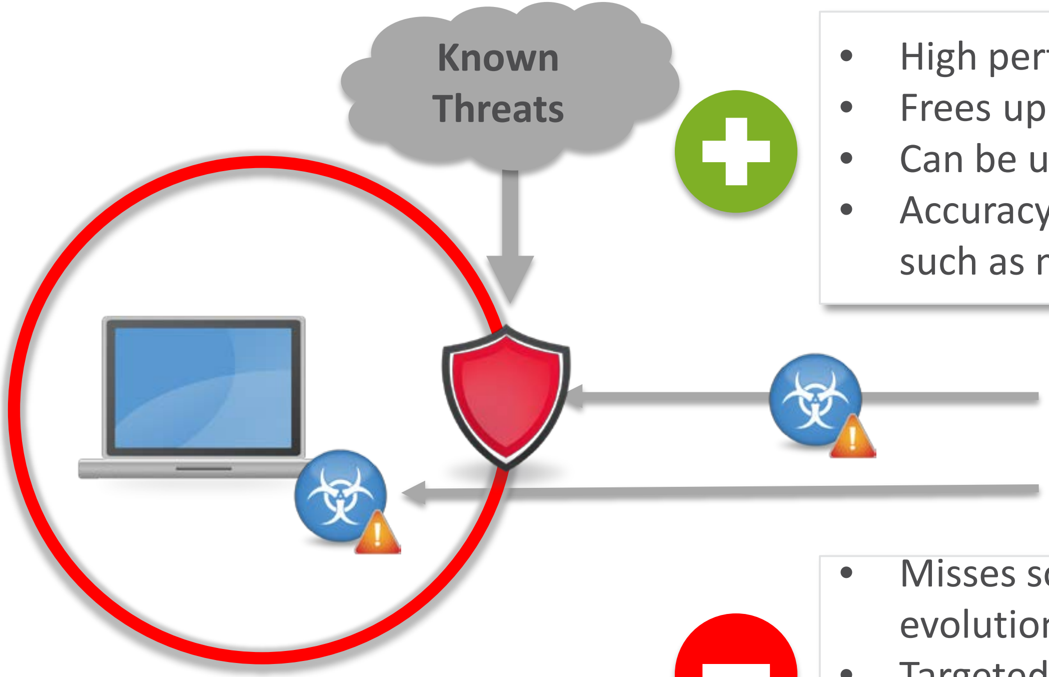
Behavioral / Sandboxing / Machine Learning

Vulnerability Shielding

Investigation / Forensics (EDR)

Copyright 2015 Trend Micro Inc.

Modern Anti-Malware



Known bad items, or those similar

Unrecognizable threats

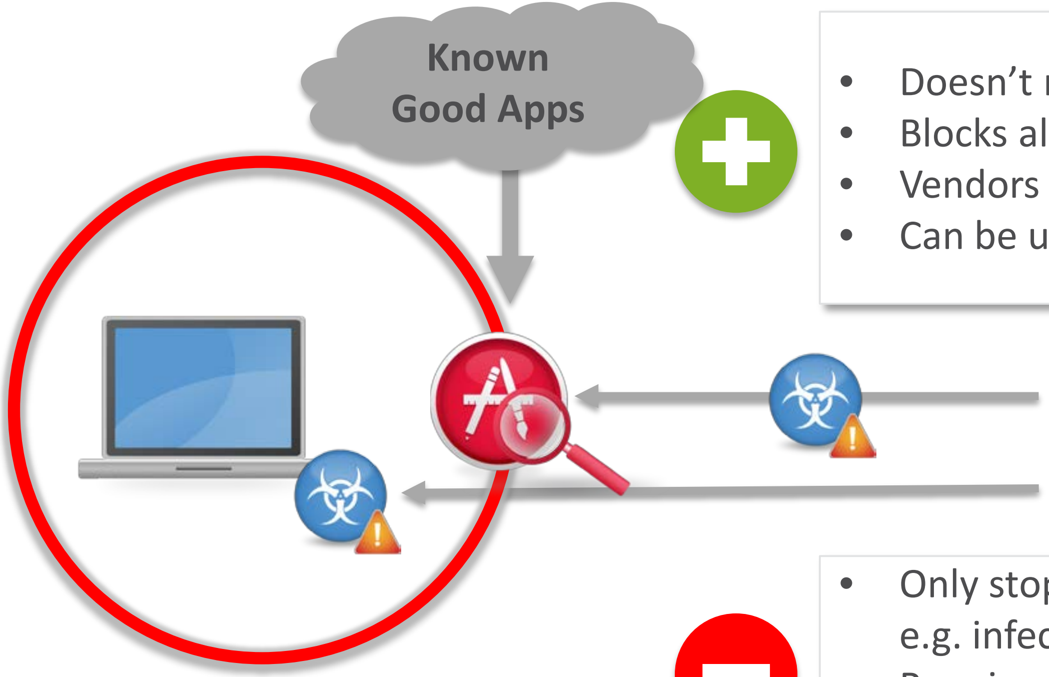
+

- High performance
- Frees up CPU for unknown-item investigation
- Can be updated locally or from the cloud
- Accuracy can be improved with enhancements such as memory inspection and prevalence

−

- Misses some unknown threats, malware evolution is rapid
- Targeted attacks can be crafted specially to avoid blacklists
- Web blacklists implemented at browser level

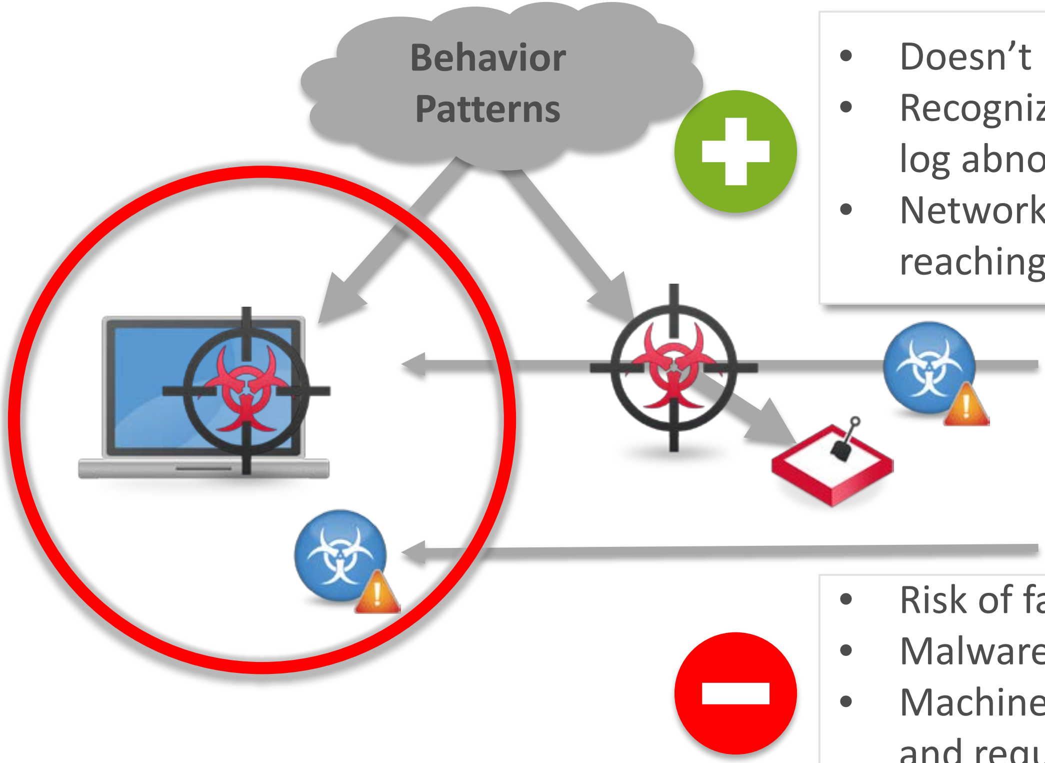
Application Whitelisting / Control



- Doesn’t need to identify malware
- Blocks all unknown apps
- Vendors can supply whitelist from the cloud
- Can be used for system lockdown

- Only stops EXE’s, misses other malicious items e.g. infected PDF, unless they launch an EXE
- Require configuration and management of the whitelist, with ongoing updates
- Can be vulnerable to code signing attacks

Behavioral / Sandboxing /Machine Learning



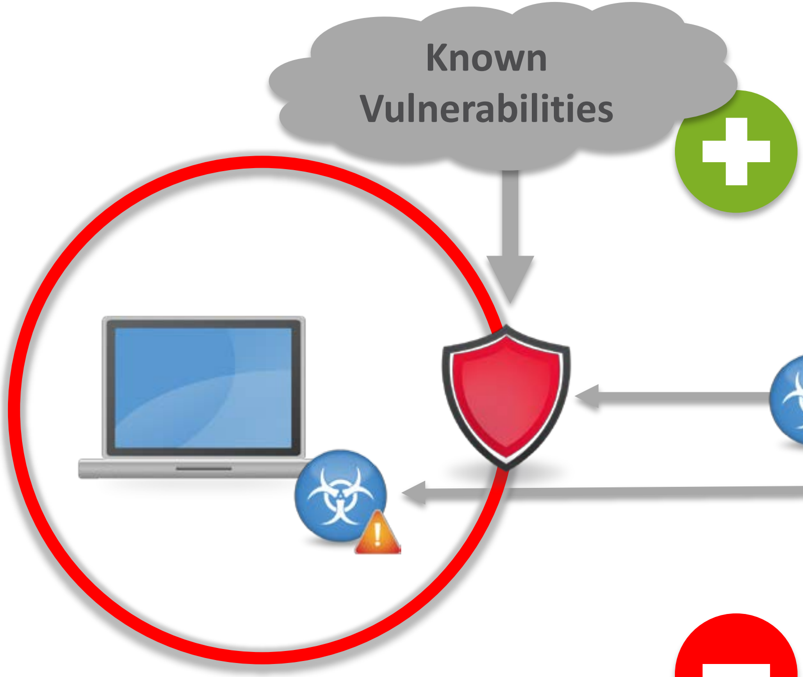
- Doesn’t need to recognize specific malware
- Recognizes many suspicious behaviors (actions, log abnormality, file integrity)
- Network sandbox may prevent malware from reaching the endpoint

Item behaving suspiciously eg. ransomware

Malware evading behavior detection

- Risk of false positive
- Malware can try to detect & evade analysis
- Machine Learning must be trained continuously and requires engine updates
- Can be more CPU intensive

Vulnerability Shielding



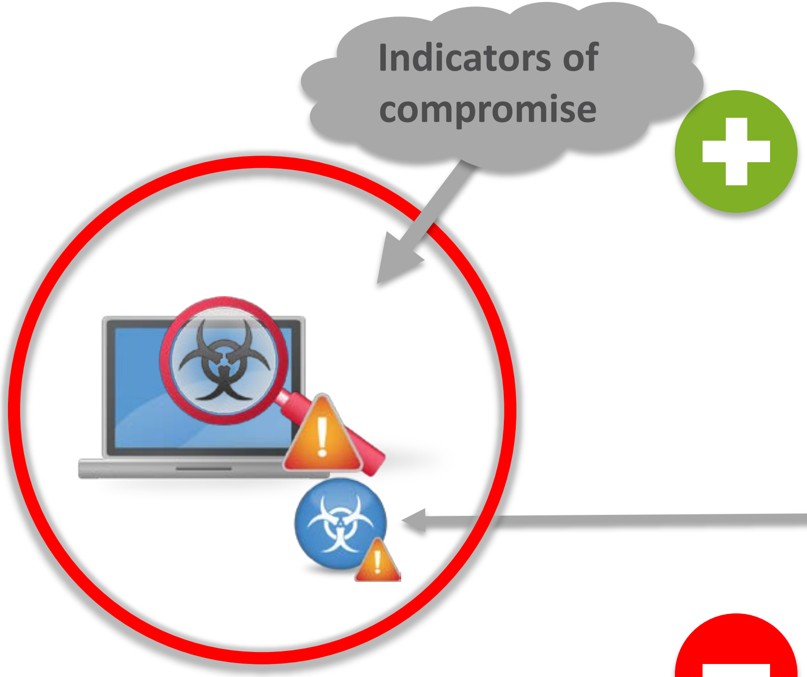
- Blocks unknown threats targeting known vulnerabilities
- Helps when OS or application patches not yet available or will never be available (i.e. legacy OS)

Vulnerability exploit

Malware downloads, USB items, etc.

- Can’t block malware that doesn’t exploit app / OS vulnerabilities
- Ineffective against zero-day exploits, until vulnerability rule update

Investigation / Forensics (EDR)



Any malware

➕

- Provides insight into history of malware infection
- Can help determine extent of data loss
- Can provide data to help block threat elsewhere

➖

- Doesn’t block malware or prevent spread on its own
- Requires sophisticated IT security staff

The Shiny Silver Bullet

"However, history has clearly shown that no single approach will be successful for thwarting all types of malware attacks. Organizations and solution providers have to use an adaptive and strategic approach to malware protection."

- Gartner Endpoint Protection Magic Quadrant, Feb. 2016

Investigation / Forensics

Modern Anti-Malware

Data Protection

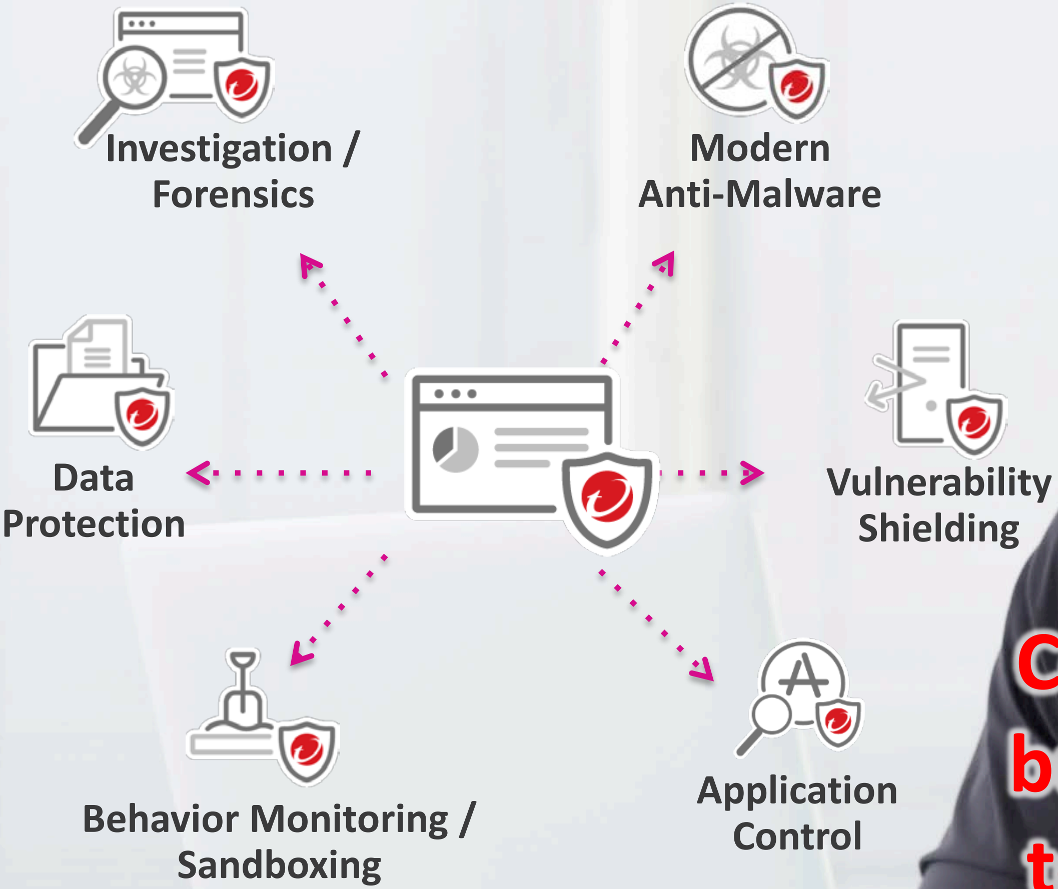
Vulnerability Shielding

Behavior Monitoring / Sandboxing

Application Control

Siloed protection:

Central Visibility Hard



Investigation / Forensics

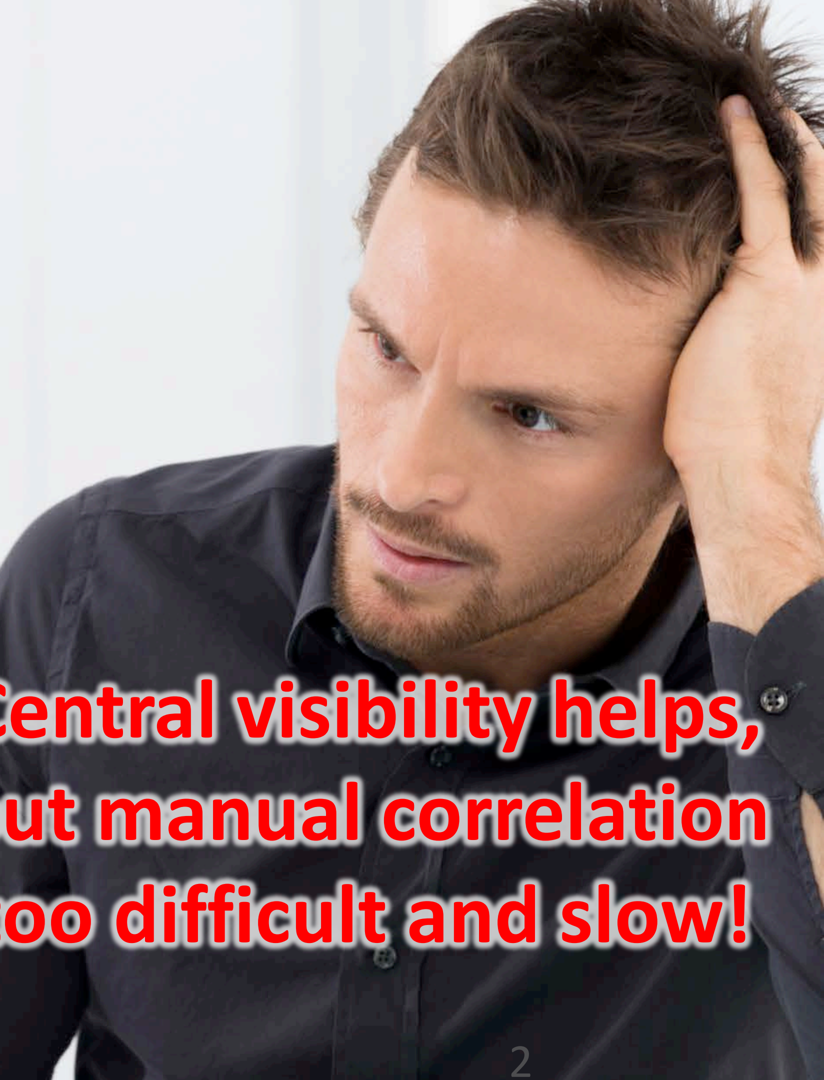
Modern Anti-Malware

Data Protection

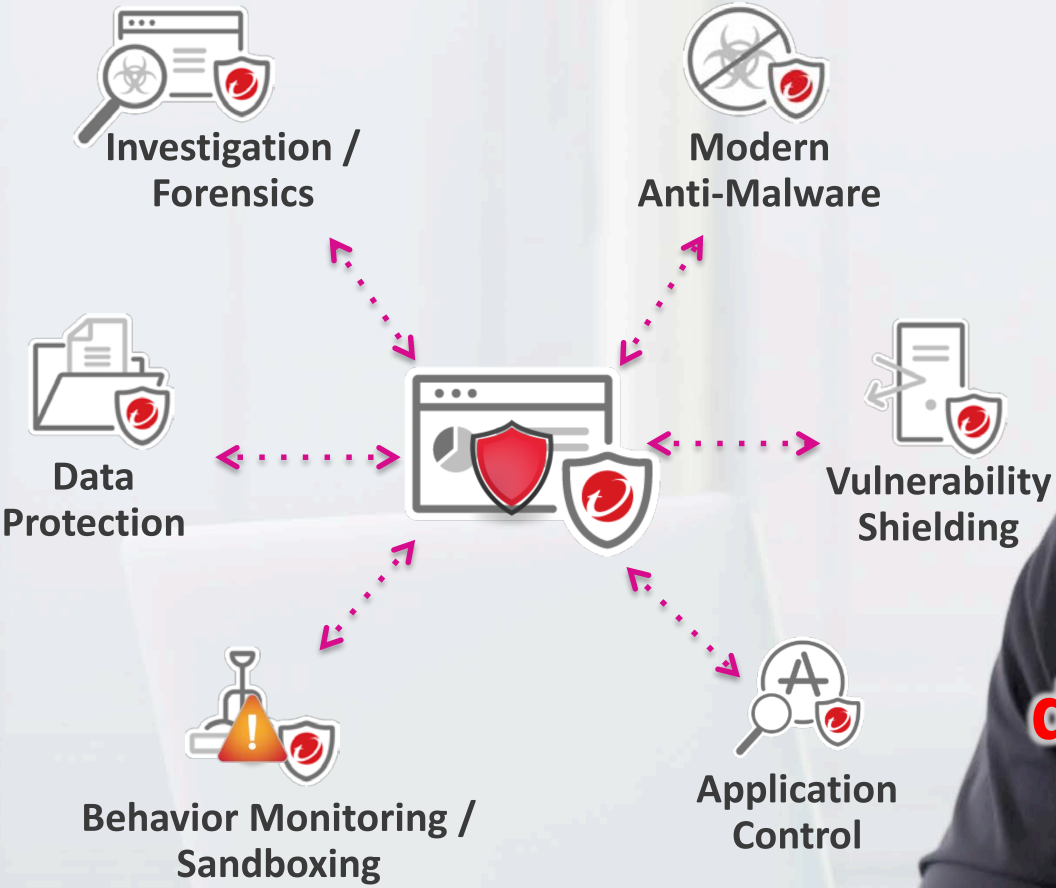
Vulnerability Shielding

Behavior Monitoring / Sandboxing

Application Control

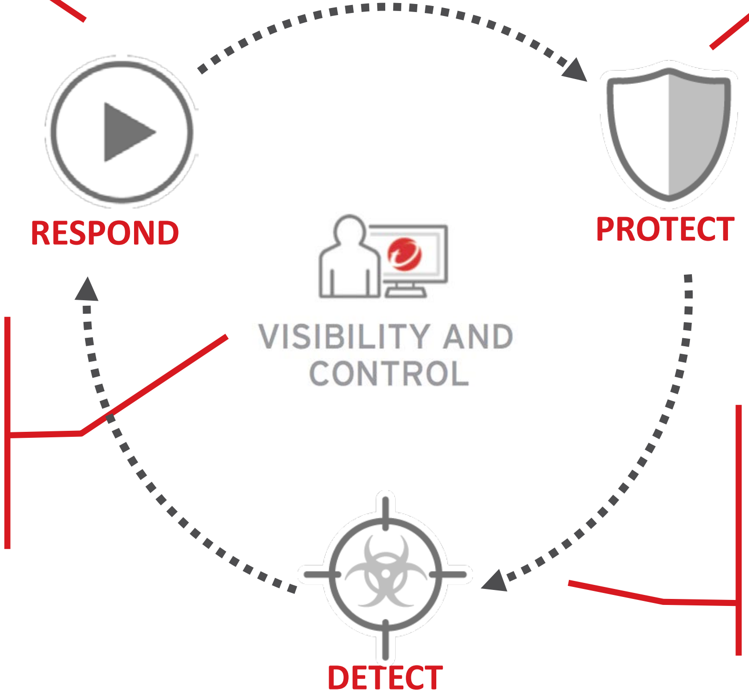


Central visibility helps, but manual correlation too difficult and slow!



A connected threat defense is required for timely, adaptive protection

Connected Threat Defense: Better, Faster Protection



Enable rapid response through shared threat intelligence and delivery of real-time security updates

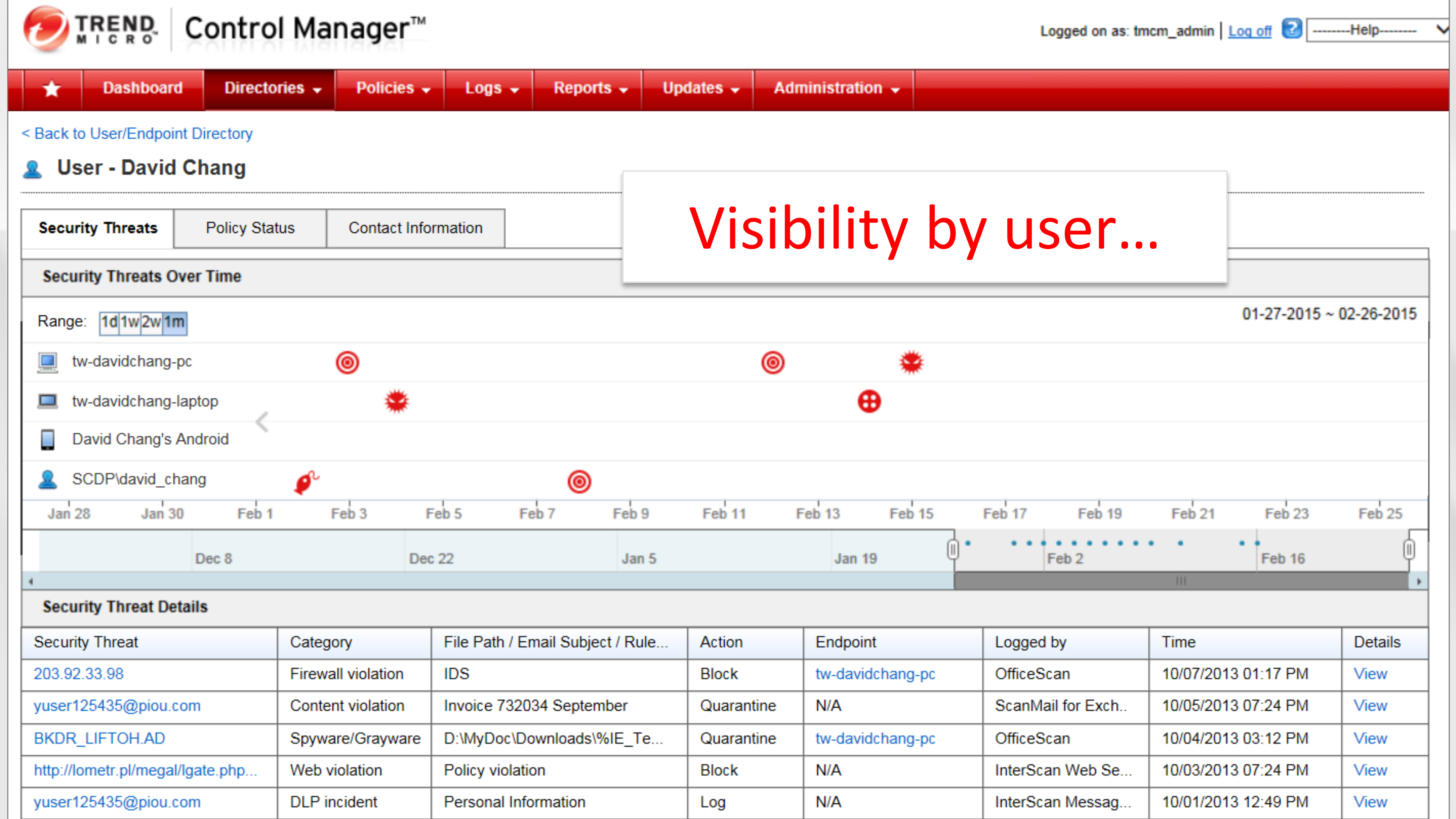
Assess potential vulnerabilities and proactively protect endpoints, servers and applications

Gain centralized visibility across the system, and analyze and assess impact of threats

Detect advanced malware, behavior and communications invisible to standard defenses

Copyright 2015 Trend Micro Inc.

Visibility by user…

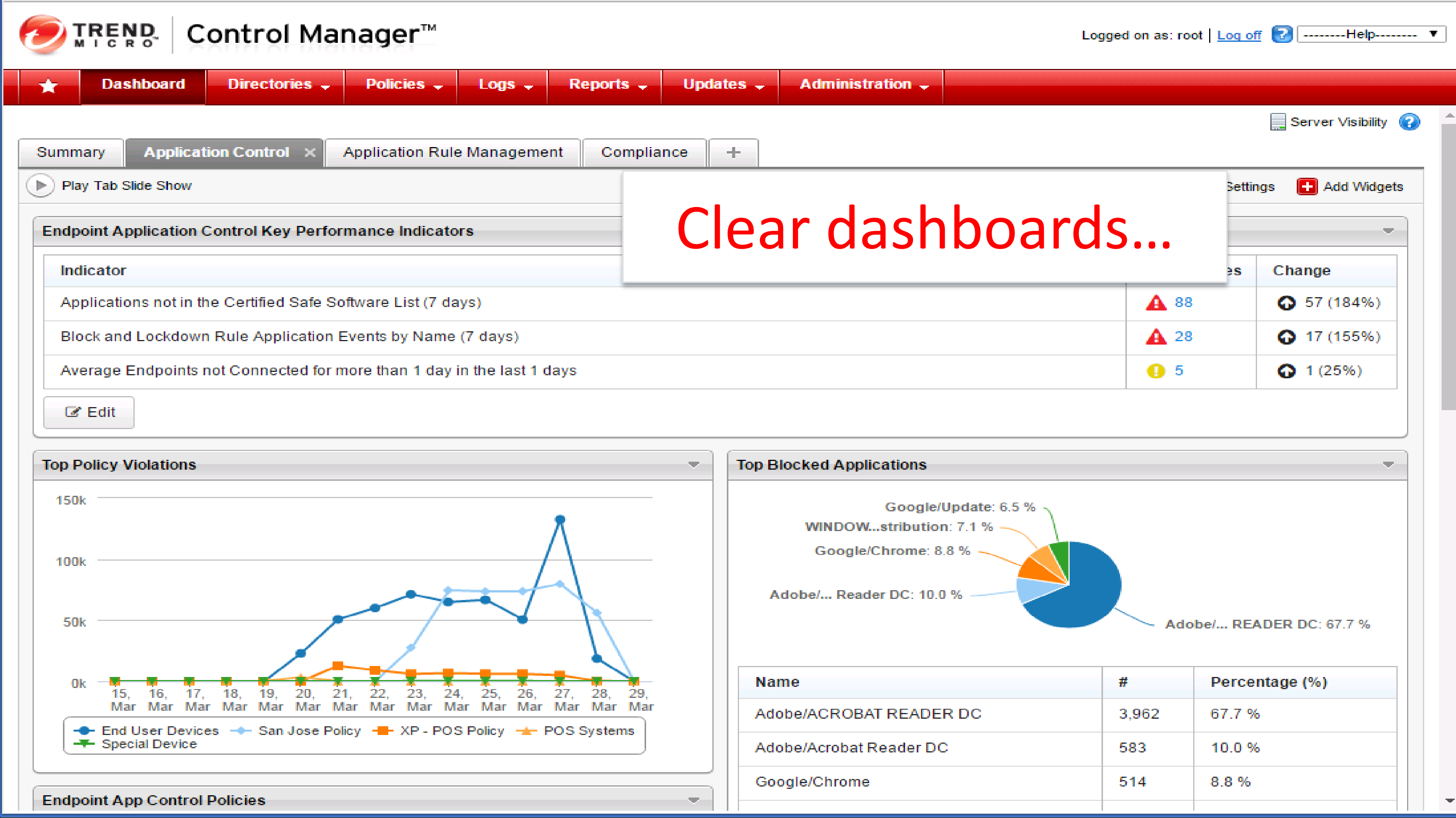


User - David Chang

Security Threats Over Time

Security Threat Details

Security Threat	Category	File Path / Email Subject / Rule...	Action	Endpoint	Logged by	Time	Details
203.92.33.98	Firewall violation	IDS	Block	tw-davidchang-pc	OfficeScan	10/07/2013 01:17 PM	View
yuser125435@piou.com	Content violation	Invoice 732034 September	Quarantine	N/A	ScanMail for Exch..	10/05/2013 07:24 PM	View
BKDR_LIFTOH.AD	Spyware/Grayware	D:\MyDoc\Downloads\%IE_Te...	Quarantine	tw-davidchang-pc	OfficeScan	10/04/2013 03:12 PM	View
http://lometr.pl/megal/lgate.php...	Web violation	Policy violation	Block	N/A	InterScan Web Se...	10/03/2013 07:24 PM	View
yuser125435@piou.com	DLP incident	Personal Information	Log	N/A	InterScan Messag...	10/01/2013 12:49 PM	View



Clear dashboards...

Endpoint Application Control Key Performance Indicators

Indicator	es	Change
Applications not in the Certified Safe Software List (7 days)	88	57 (184%)
Block and Lockdown Rule Application Events by Name (7 days)	28	17 (155%)
Average Endpoints not Connected for more than 1 day in the last 1 days	5	1 (25%)

Edit

Top Policy Violations

Top Blocked Applications

Google/Update: 6.5 %
WINDOW...stribution: 7.1 %
Google/Chrome: 8.8 %
Adobe/... Reader DC: 10.0 %
Adobe/... READER DC: 67.7 %

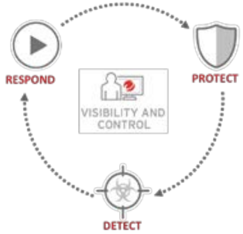
Name	#	Percentage (%)
Adobe/ACROBAT READER DC	3,962	67.7 %
Adobe/Acrobat Reader DC	583	10.0 %
Google/Chrome	514	8.8 %

Endpoint App Control Policies

Trend Micro Smart Protection Suites

Clear, all-inclusive suite packaging with Cloud flexibility

Comprehensive, proven & next gen protection techniques



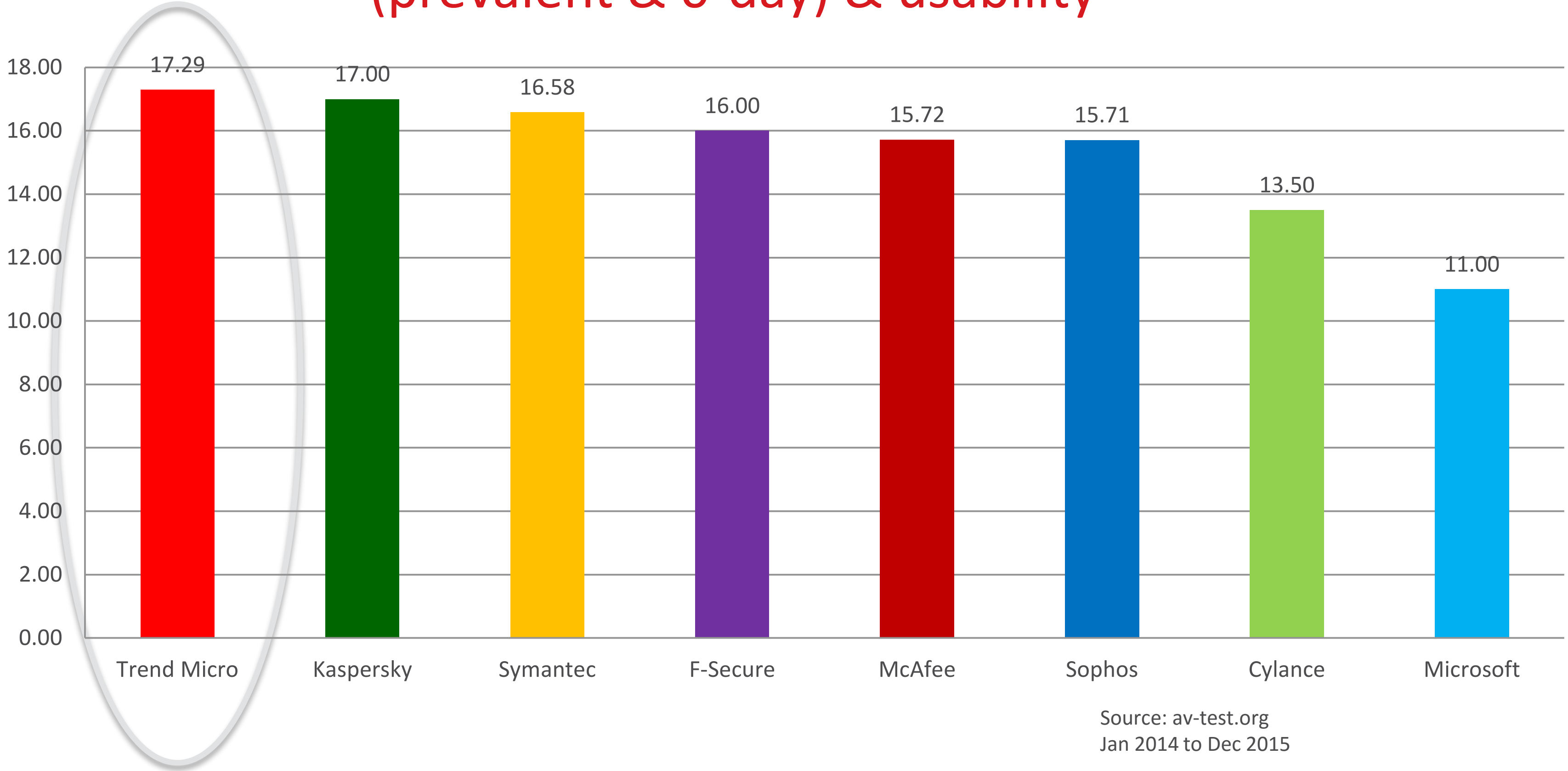
Connected Threat Defense

Low performance impact

Strong central visibility & control

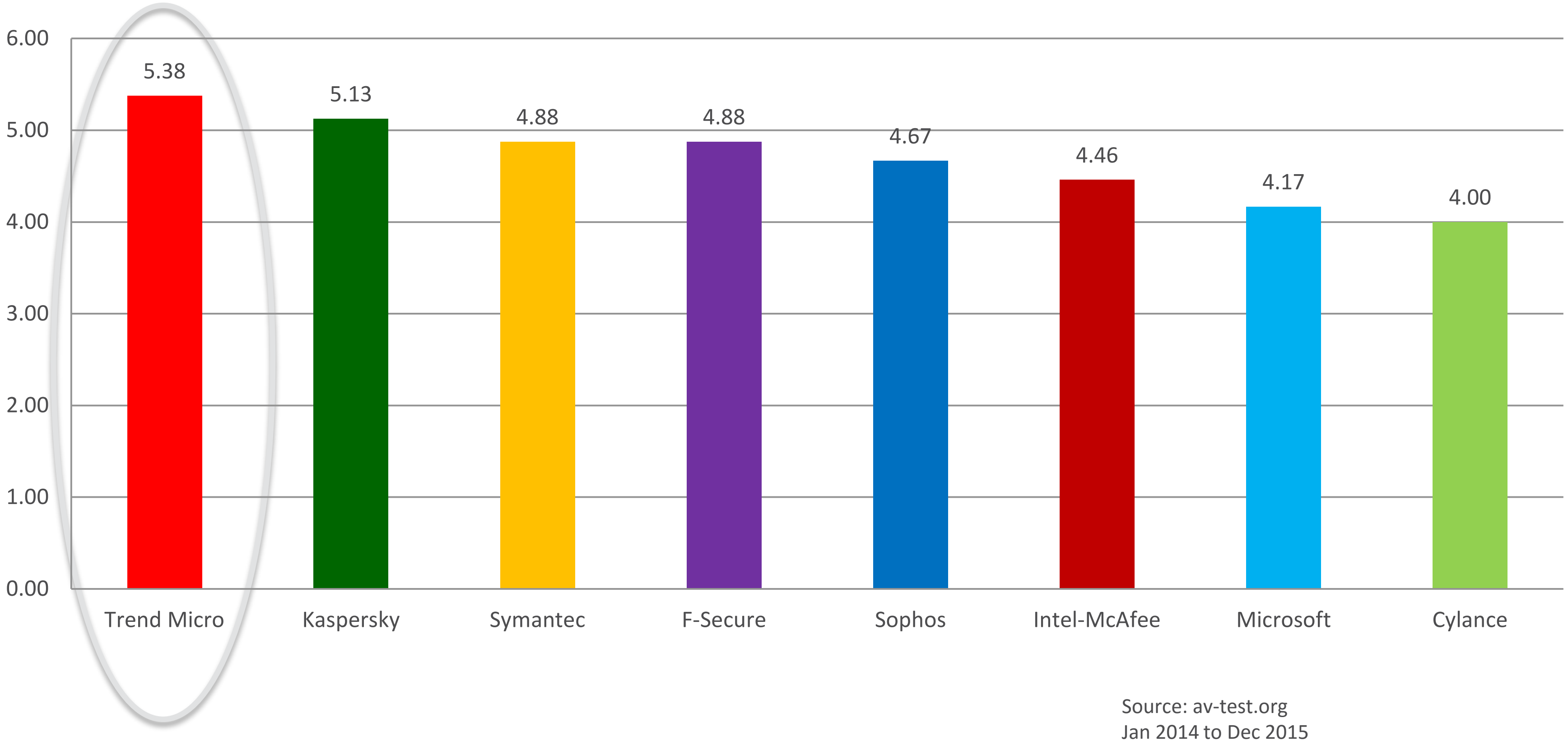
Best Overall Score

2014-2015: Includes performance, protection (prevalent & 0-day) & usability



Source: av-test.org
Jan 2014 to Dec 2015

Best Performance 2014-2015



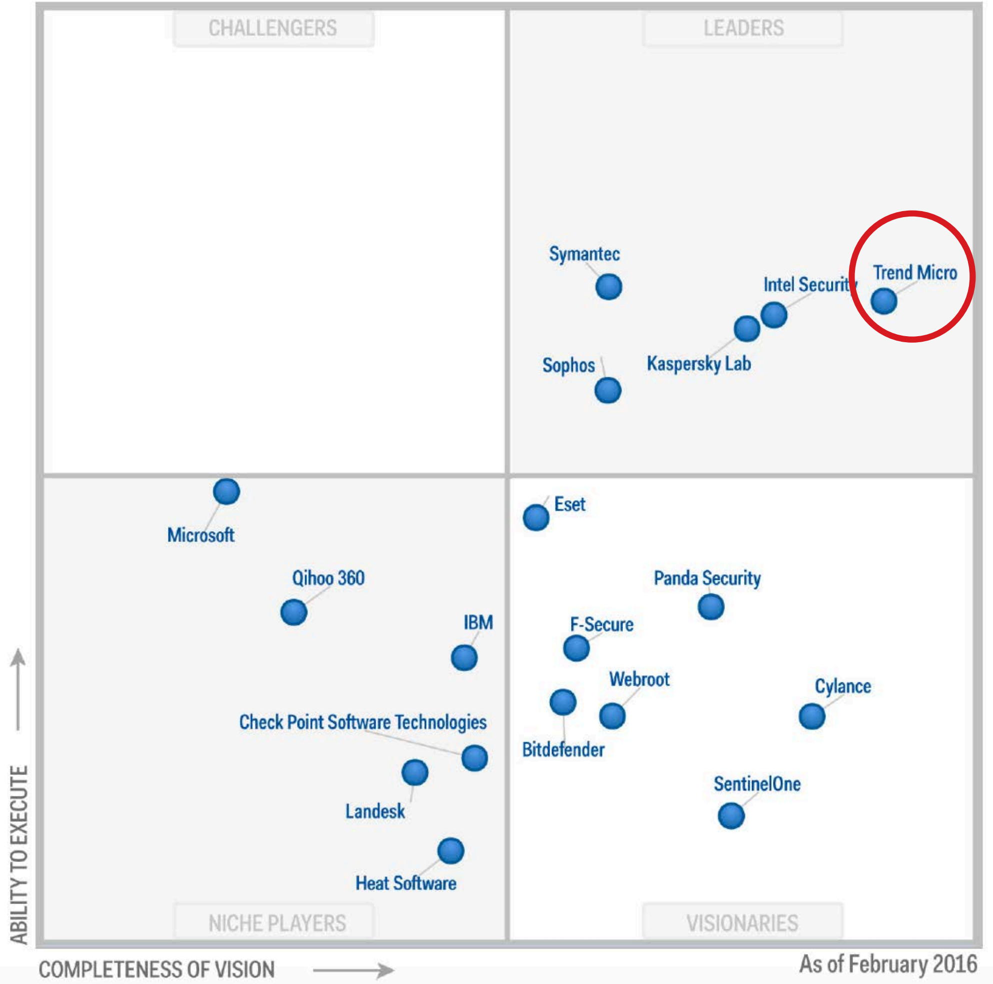
Source: av-test.org
Jan 2014 to Dec 2015

Gartner Magic Quadrant for Endpoint Protection Platforms

Feb 2016

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

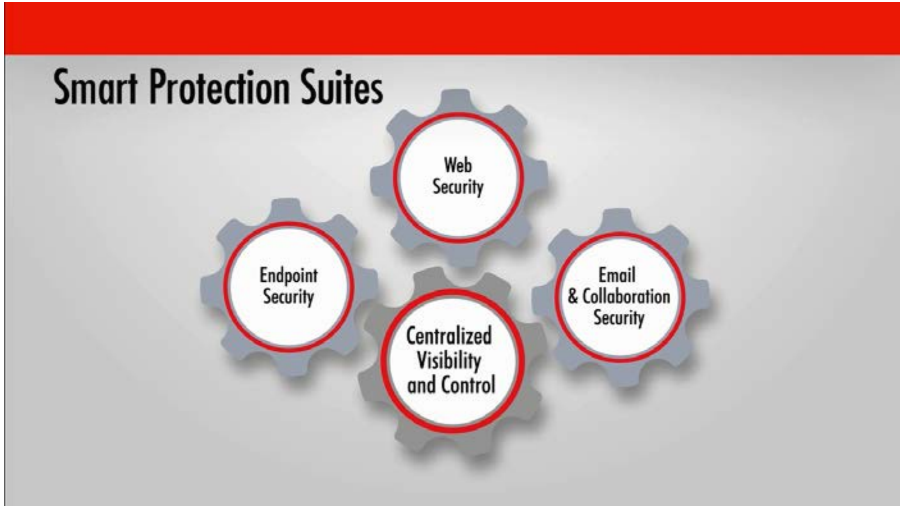
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



Source: Gartner (February 2016)

www.trendmicro.com/smartdemos

- Fully scripted for delivery with live audio or without
- Available now:
  - Endpoint Security
  - Web Security
  - Email & Collaboration Security
  - Cloud App Security



Smart Protection Suites

Web Security
Endpoint Security
Email & Collaboration Security
Centralized Visibility and Control

Copyright 2015 Trend Micro Inc.

SPCINTERNATIONAL

THE IT BUSINESS BUILDER ONLINE

Copyright 2015 Trend Micro Inc.