Please stand by. Webinar will start momentarily.

# Prevent Cyber Attacks at Government Agencies

BlackBerry | CYLANCE

BlackBerry | CYLANCE

# Prevent Cyber Attacks at Government Agencies

**Brian Winkler**
Sr. Federal Solutions Engineer

**John Wood**
Director, Incident Response

# Brian Winkler

- Bachelor of Science
- 20+ years in IT, Telecom and Cybersecurity
- 10+ years working on Federal Programs including DHS Einstein 2 & 3, Census Decennial 2010, HHS, TSA and others.
- 3+ years on BlackBerry Cylance's Federal Sales Engineering Team

BlackBerry | CYLANCE

# John Wood

- Retired from the FBI after 23 years focusing on Cyber Intrusion Investigations
- Bachelor of Science in Criminal Justice/Chemistry
- Master of Science in Computer Forensics
- A+, Net+, Security+, GCIH, GREM, GCFA, GWAPT
- Forensic examiner on several high profile cases: Snowden, Petraeus, 911 attacks, Ardit Ferizi ISIS case, Russian Voter intrusion case, Michael Kadar, etc.
- Conducted IR on national security cases at the White House, State Department and both houses of Congress.

# AGENDA

- Cybersecurity Reality
- What Government Agencies are Facing?
- Interview with John Wood
- Rethink Your Cybersecurity Strategy

# CYBERSECURITY REALITY

- 40,000 new malicious binaries created every hour, 5 malware events per second
- >90% of all cyber attacks utilize malware
- Adversaries create huge numbers of malware variants and mutations to avoid detection… or they design one just for you
- Unique malware is the norm rendering traditional AV completely useless.

BlackBerry | CYLANCE.

# WHAT GOVERNMENT AGENCIES ARE FACING

Mission Impact

Excessive Alerts

Tool Consolidation and Operationalization

# Interview with John Wood

# Rethink your Cybersecurity Strategy

# PREVENTION IS POSSIBLE

Continuous prevention is an intelligent endpoint security solution that combines AI-driven, prevention focused software with specialized security services designed to eradicate active threats and safeguard against future ones.

## THINK BEYOND TRADITIONAL INCIDENT RESPONSE

BlackBerry | CYLANCE

# AI AND THE EVOLUTION TO PREVENTION

## LEGACY

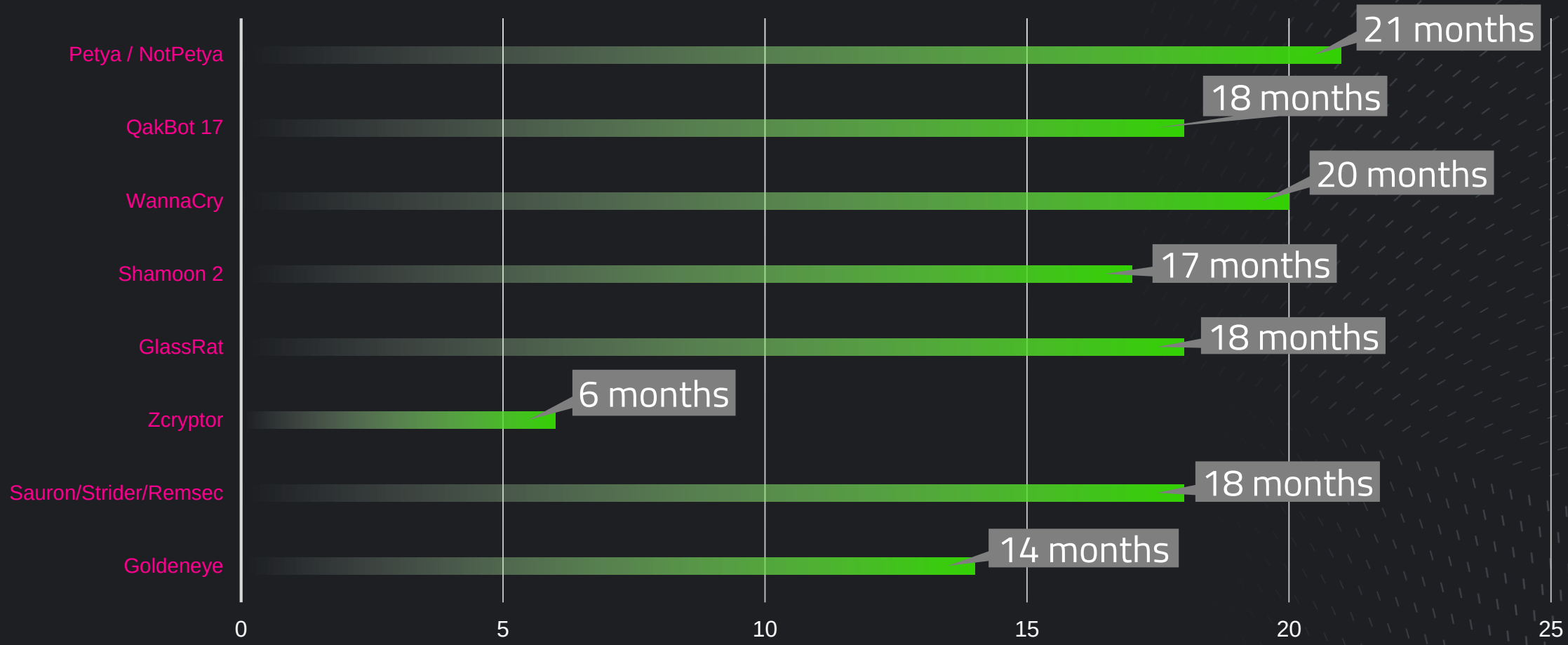
- One of the tools detects “something”
- Reactive
- Image the entire disk and/or memory
  - Time consuming
  - Large amount of data
- Requires hardware/appliances in environment for additional visibility
- Increase in capital costs
- “Seize all, find all”

## PREVENTION-BASED INCIDENT CONTAINMENT

- No network taps or monitoring of egress points
- Assesses every endpoint
- Leverage your software deployment to push out dissolvable scripts and/or through the agent
- Principle of least data
- Speed in analysis – we’re TWICE as fast!
- Use AI for detection of malware, PUPs and compromised credentials
- Containment with a single mouse click

# PREDICTIVE ADVANTAGE

BlackBerry Cylance provides a solution that is proven able to block emerging threats months before they are first detected in the wild. We've stopped tens of millions of potential attacks with a system that is continually learning and continually getting better.




*SE Labs Report

BlackBerry | CYLANCE

# BENEFITS OF BLACKBERRY CYLANCE

## Effectiveness

Prevents over 99% of malware before it can execute, including system and memory-based attacks, scripting, spear phishing, zero-day malware, privilege escalations, and malicious and potentially unwanted programs.

## Simplicity

Simple to deploy and manage – no daily endpoint management and signature updates required, our intuitive cloud-based management console simplifies deployment and management and reduces operational overhead.

## Performance

Lightweight agent uses only 1-3% of PC processing power - 10 times fewer system resources than traditional endpoint security solutions - to provide superior, preventive protection.

# BLACKBERRY CYLANCE SOLUTIONS


## AI-Driven Threat Prevention

CylancePROTECT® delivers industry-leading threat prevention powered by AI, combined with application and script control, memory protection, and device policy enforcement to identify and block threats before they can cause harm.


## Immediate and Intelligent Response Solution

CylanceOPTICS™ is an endpoint detection and response solution that extends the threat prevention delivered by CylancePROTECT by providing incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities.


## Proactive Managed Response and Detection Solution

Subscription-based managed detection and response offering that leverages our award-winning native AI platform and the 24x7 support of a world-class team of BlackBerry Cylance incident responders and prevention experts.

BlackBerry | CYLANCE

# ARCHITECTURE DEPLOYMENT OPTIONS

## Cloud Deployment
### for Connected Environments

Streamline management from the cloud. A single lightweight agent supporting Windows, Mac and Linux. Deploy in minutes – no reboots, no signatures, with zero hardware and maintenance cost – for immediate effective prevention.

FedRAMP

## Hybrid Deployment
### for Unique Environments

Choose a single-point connectivity solution. Download once, redistribute locally. Hybrid deployment facilitates security-related communication between the cloud and local infrastructure without exposing your network.

FedRAMP

## On-Premises Deployment
### for Closed Environments

On-premises deployment architecture represents a common environment, deployed exclusively within your local network infrastructure. You can choose to host CylancePROTECT on a physical server or from a compatible virtual server.

BlackBerry | CYLANCE

# Resources and Next Steps

# THE NEXT-GEN OF CYBERSECURITY IS HERE

## Connect with BlackBerry Cylance at dlfederalsales@cylance.com

Chat with our experts today and see how BlackBerry® Cylance® solutions can prevent advanced threats that traditional AV cannot. We're certified to deploy CylancePROTECT's revolutionary AI based agent through cloud-managed architecture for the U.S. government.


**Brian Winkler**
Sr. Federal Sales Engineer
bwinkler@cylance.com
(703) 969-5873

**Dan Sweeney**
Federal Enterprise Sales Manager
dsweeney@cylance.com
(703) 297-6799

**Robert Greenfield**
Federal Enterprise Sales Manager
rgreenfield@cylance.com
(410) 703-8596

**John Wood**
Director, Incident Response
jwood@cylance.com
(314) 792-4123

**James Zembriski**
Federal Business Dev Rep
jzembriski@cylance.com
(201) 961-4904


BlackBerry | CYLANCE

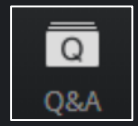
# RESOURCES

- See the next generation in endpoint security solution, get a demo
- Spotlight on Government Security: case studies, white papers and podcasts
- BlackBerry Cylance Deployment Architecture Options
    - Cloud Deployment for Connected Environments
    - Hybrid Deployment for Unique Environments
    - On-Premises Deployment for Closed Environments
- Incident Containment: 888-808-3119 or request for a consultant
- Learn more about Consulting Services
- Research and Intelligence
    - Operation Shaheen Threat Intelligence Report
    - OPM Breach Report

# Questions

+

# Answers



"Not only does Cylance replace traditional endpoint antivirus and anti-malware products, it also precludes the need for other detection, forensic recording, and host intrusion prevention technologies. It does this while reducing the need for experienced threat response teams to investigate, deconstruct, and remediate attacks."

**Government Agency**


©2019 Cylance Inc. All Rights Reserved.