

BLACKBERRY SECURITY SOLUTIONS



Presented by Christian Buschfort, Principal Sales Engineer



BlackBerry AI leverages the power of machines, not humans, to dissect malware or to notice anomalies and prevent threats from compromising an organization.

PREVENTING THREATS BEFORE THEY EXIST

Predictive Advantage: How far in the future can your security products detect a threat?



Ryuk
-44Mo.



WastedLocker
-52Mo.



Maze
-48Mo.



Petya-Like
-25Mo.



GlassRat
-18Mo.



Emotet
-20Mo.



Zeppelin
-49Mo.

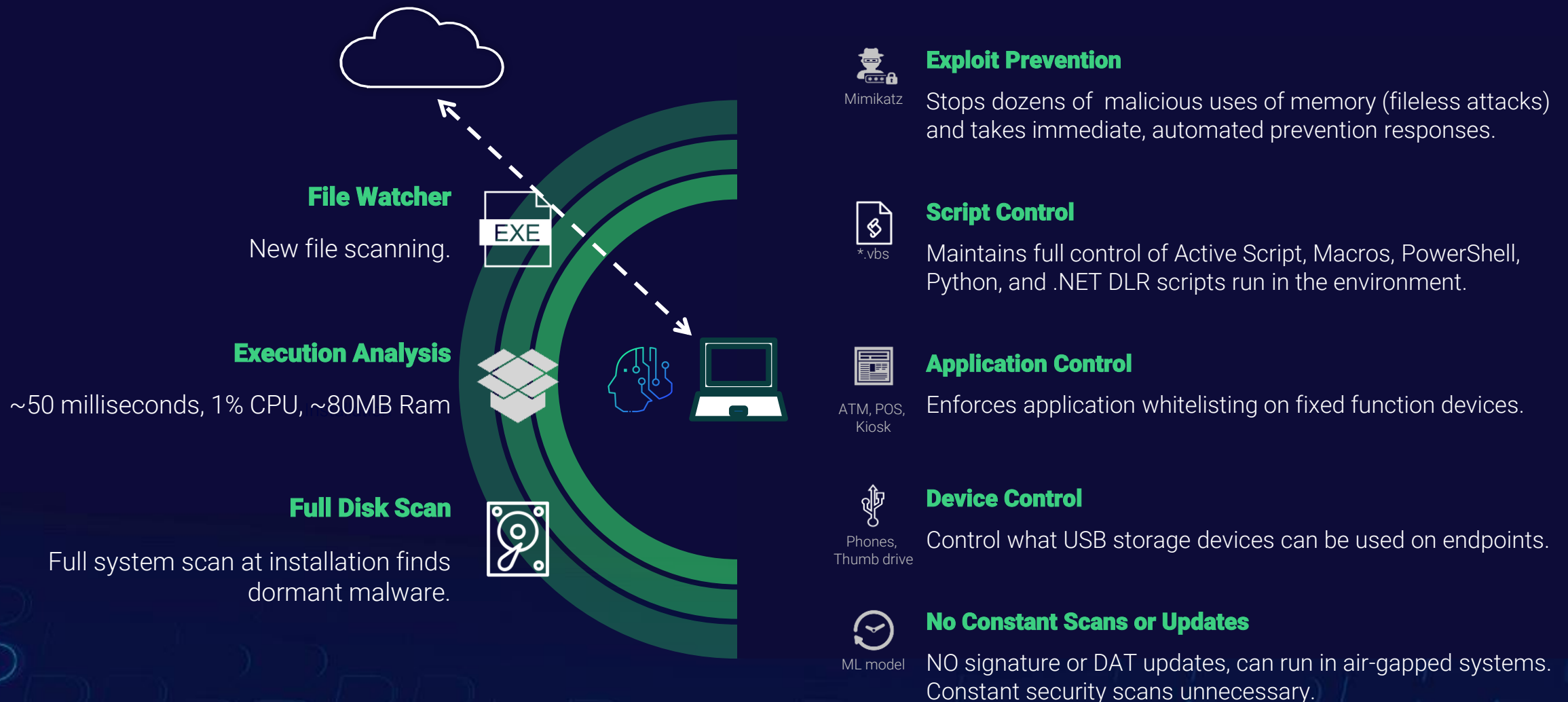


WannaCry
-24Mo.



PRODUCTS OVERVIEW

PROTECT – MACHINE LEARNING EPP





BLACKBERRY PROTECT MOBILE



EDGE AI PROTECTION

Cylance AI identifies and block mobile malware, protects against side loading, and identifies security vulnerabilities and compromises with the OS



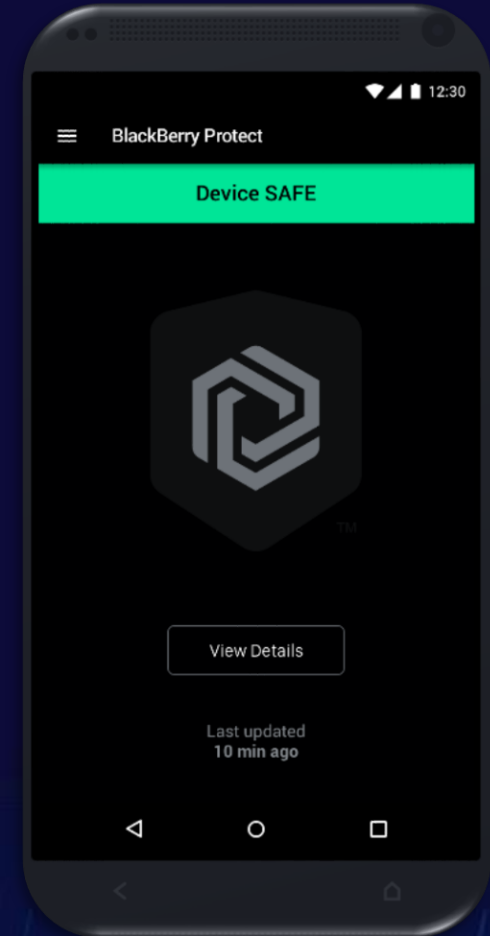
REMEDIAION

Once a threat is identified, Protect can inform and allow the user to self remediate the issue by removing the threat or automatically enable options like safe browsing



BLOCK SOCIAL ENGINEERING

Neutralizes the threat of social engineering attempts via malicious SMS/MMS messages; URL scanning/anti-smishing.



OPTICS FEATURES

Proactive, Local Action

Not dependent on the cloud for protective actions.

Threat Hunting & Root Cause Analysis

Use the power of Elastic Search and Event Query Language to perform in-depth threat hunting and display results in an easy-to-understand timeline.

Built-In & Custom Rules Drive Detections

Fit our product to your environment by using our curated or custom-built JSON rules.

Large List of Sensors Track Activity

File, Process, Network, Registry, DNS, Windows Security Events, WMI, PowerShell and other forms of activity are monitored and recorded.



24 / 7 Forensic Data Storage Options

30-day storage of data by default. 90 and 365-day storage options available.

Remote Response

Connect to systems with a remote shell and perform investigation, troubleshooting, and remediation.

Manual or Automated Custom Scripts

Use Python scripts to gather information or perform corrective action.



BLACKBERRY PERSONA

BlackBerry Persona uses machine learning and predictive AI to dynamically adapt a security policy based on user and device conduct. By improving the user experience, it protects against human mistakes and well-intentioned workarounds



ADAPTIVE PROTECTION

Adaptive Endpoint Protection with Predictive AI and Machine Learning



CONTINUOUS AUTHENTICATION

Passive biometrics and usage-based patterns continuously verifies a user's identity



REAL TIME RISK SCORE

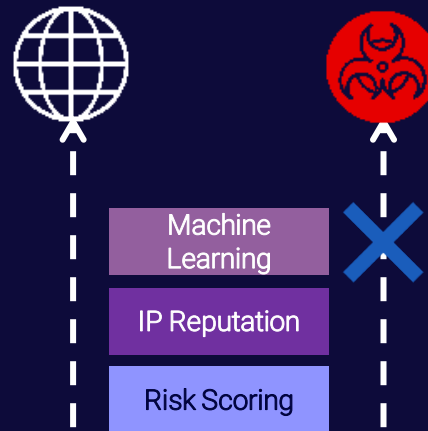
Dynamically Adapts Security Policies Based on Situational Risk

BLACKBERRY GATEWAY - ZERO TRUST NETWORK CLIENT



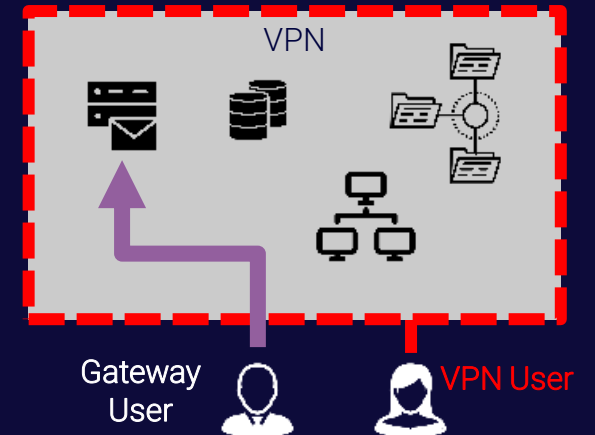
Continuous identity risk analysis

Machine learning evaluates user behavior and anomalies are detected when a Gateway user's network usage pattern is not consistent with past behavior.



Evaluation of Internet destinations

Maintains an ever-evolving list of malicious Internet destinations and can block access automatically.



Segmented private network access

Connectors provide remote access without changing the network topology. Access through Gateway offers strong isolation; only the parts of the network you choose are exposed to endpoints.

PROFESSIONAL SERVICES

World-class cyber security and product implementation services.



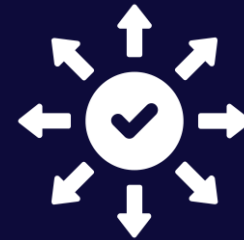
COMPROMISE ASSESSMENTS

Run a health check to evaluate your environment.



INCIDENT RESPONSE

Stop threats with the number one SOC team in the world.



THREATZERO

Work with our team of experienced deployment professionals to operationalize our products and tune them for your specific needs.



GUARD

Let us monitor your security environment with our 24/7 managed detection and response.

Q & A