Current Threat Landscape, Q2 2018

Adam Gates, Senior Sales Engineer Malwarebytes

Who Am I?

Adam Gates, Sales Engineer

20+ years of industry experience as a consultant, engineer, and specialist

Focus on Office 365, Coffee, Security

Passion for thoughtful process and plan to achieve business goals

Contact me at agates@Malwarebytes.com or https://www.linkedin.com/in/ahgates/

Malwarebytes

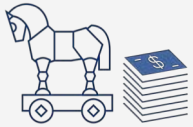
Top 2018 Attack Vectors

1

Cryptomining

Hardware Attacks

2



Banking Trojans

Phishing

3

Adware / Malvertising

Supply Chain Attacks

4

Backdoor

Hijackers

5

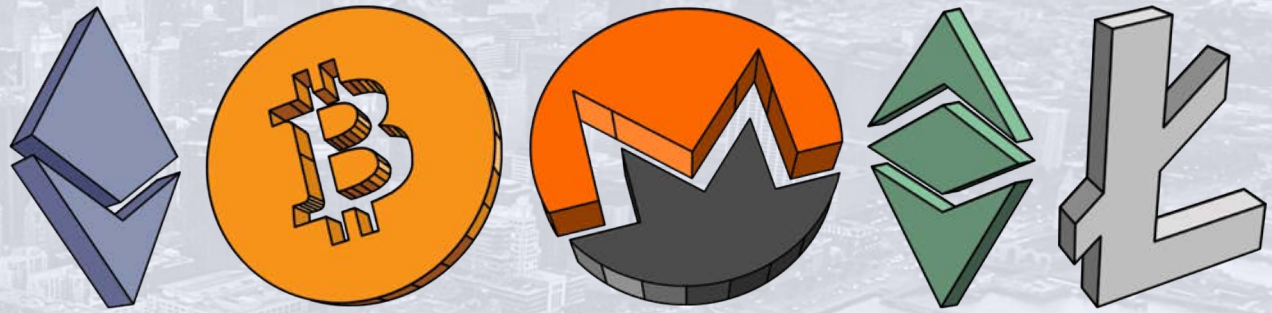
Spyware

Ransomware

Cryptomining/jacking Attacks (3.4 Million YTD)

Distribution Methods

- Drive-by
- Phishing campaigns
- Trojanized apps
- Supply chain attacks
- Bundled software



Concerns for Business

- Maxed out CPU cycles
- Degraded system hardware
- Higher utility expenses
- Future attack via backdoors to pivot from mining when ROI drops

Cryptojacking – Business Impacts

Increase in illegal coin-mining on **YouTube** via malware embedded ads

Numerous websites fall victim to illegal mining that went **un-detected for months**

Amount to date earned by attackers using **WordPress** servers to illegally mine Monero currency

Trojan Attacks (9.1 Million YTD)

DataBot Banking Trojan

- Credential/money theft
- Credential harvesting

Dorkbot Banking Trojan

- Steals credentials, spams, launches DDoS attack
- Affected 8% of all organizations worldwide

Emotet Trojan

- 57% of all banking Trojans
- Difficult to detect: polymorphic/sandbox evasion
- Major impact:
  - Allentown, PA - Entire city computer infrastructure
  - Cost - $1 Million (Additional $900k recovery phase)

Adware Attacks (5.2 Million YTD)

Cosiloon

- Obfuscated Code
- Pre-installed in Android firmware

Mobsuite

- Browser re-direct
- PII collection/spyware

FileTour

- Cryptojacking
- Software Crack/key generators

Adware – Business Impacts

Cosiloon

- Discovered across 100+ countries
- 18,000 Android devices infected

Mobsuite

- Theft of company intellectual property
- Company account credential theft

Predictions...

1. Expect big changes next quarter
2. Cryptocurrency miners will go out of style
3. PII will become even juicier target
4. Exploit kits will still be a threat
5. Ransomware will ramp up again

Get your copy at blog.malwarebytes.com

Malwarebytes:
Addressing Today’s Threat Landscape

Impact of Cybersecurity Threats

73%

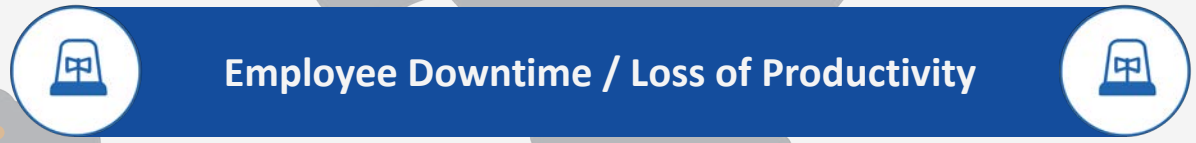
Organizations impacted by security event in past 12 months

$1.9M

Annual spend on cybersecurity-related costs

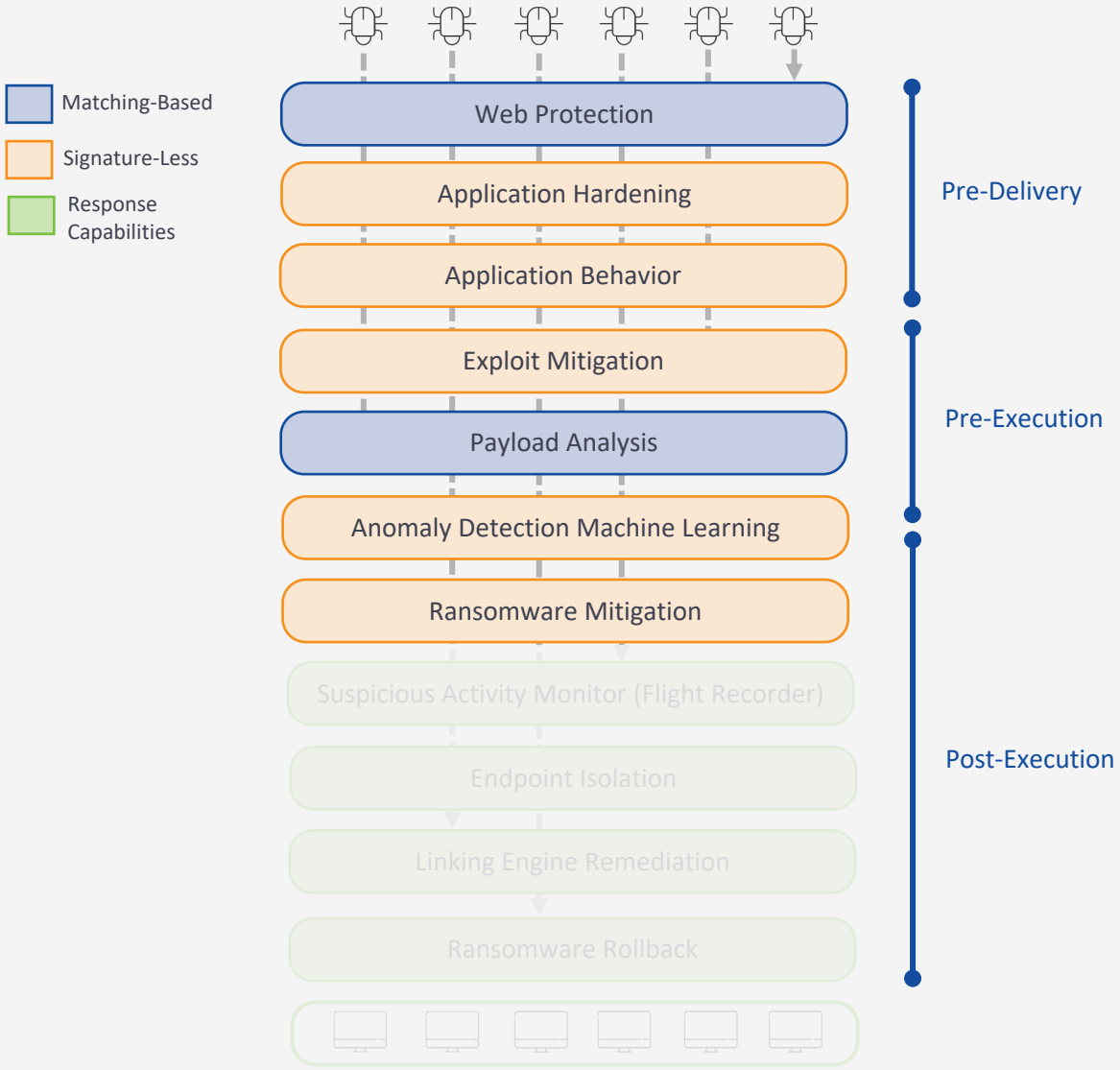
$430k

Cost to remediate a major security event

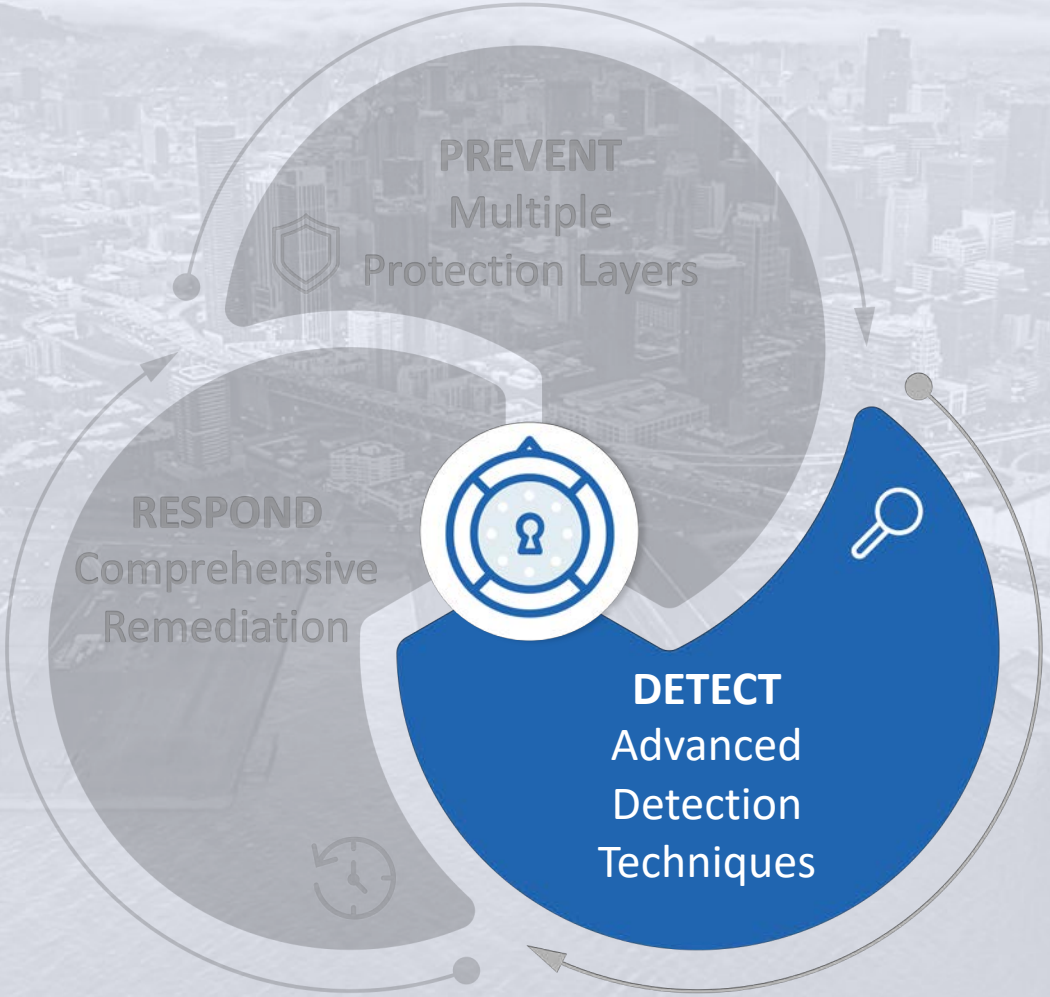


Effective Solution Components

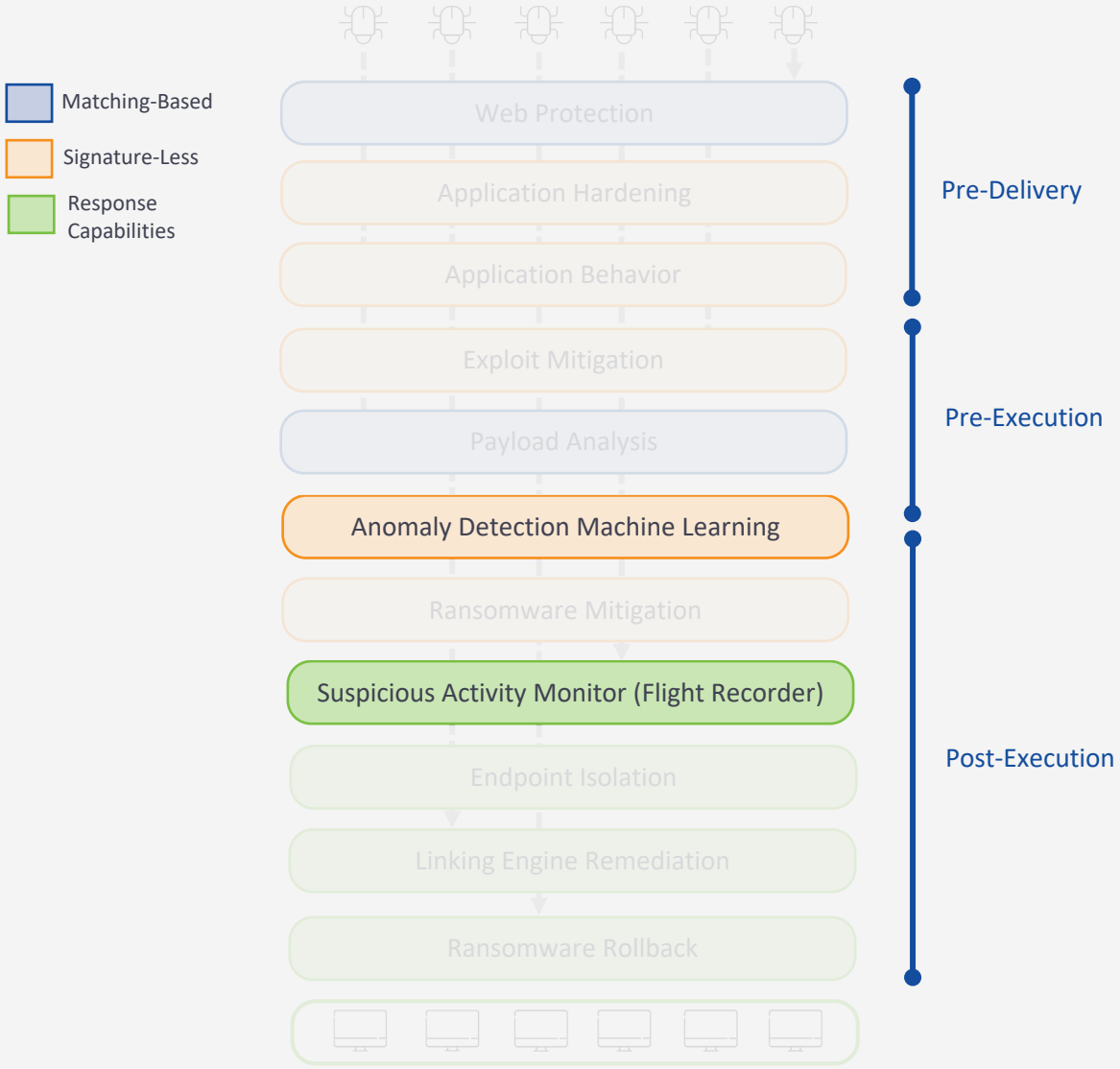
Protection, Detection, and Response Layers



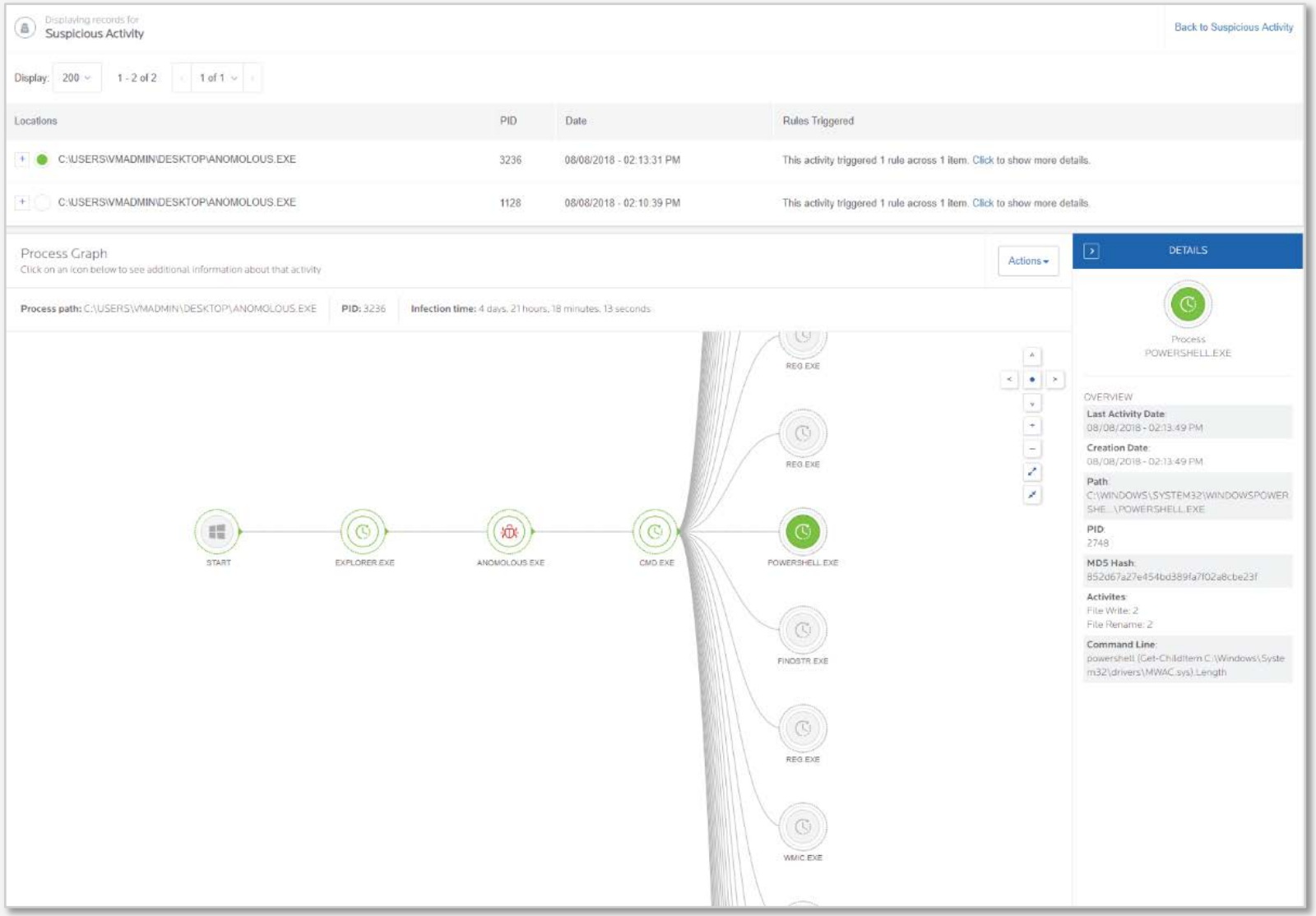
Effective Solution Components



Protection, Detection, and Response Layers

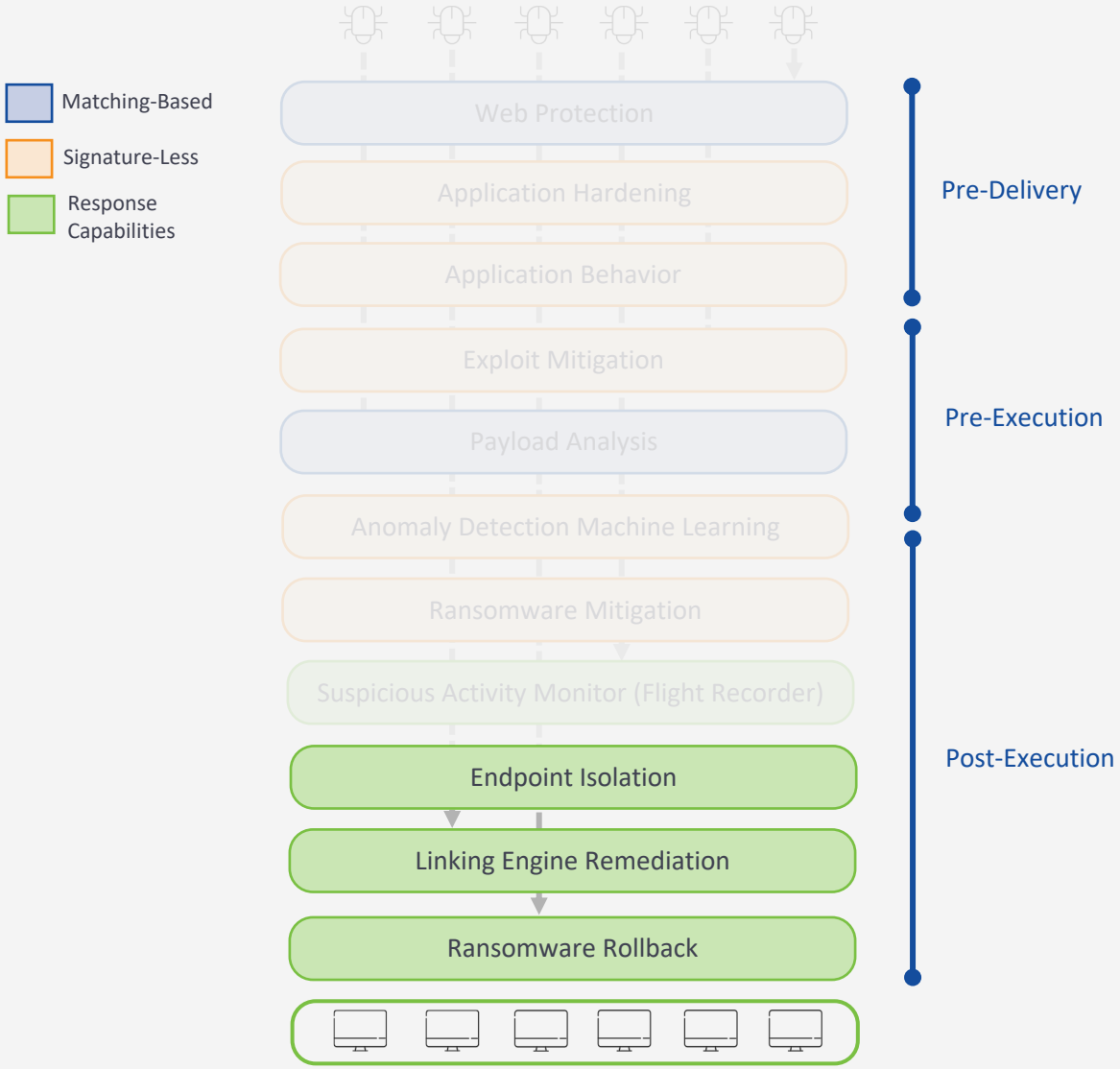


Protection, Detection, and Response Layers



Effective Solution Components

Protection, Detection, and Response Layers



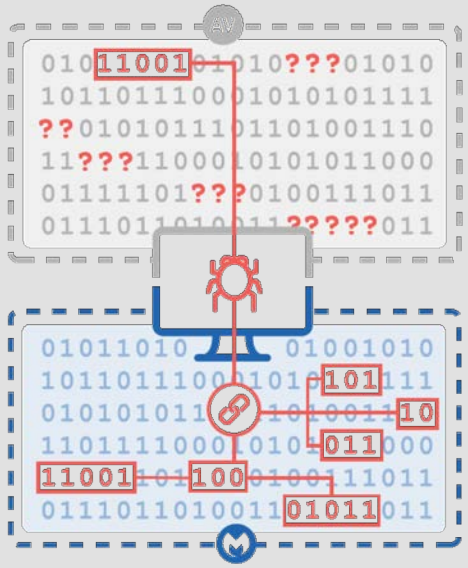
Protection, Detection, and Response Layers

Endpoint Isolation: 3 Modes

- Isolates endpoints to stop the bleeding
- Prevents malware from connecting to C&C
- Locks remote attackers out

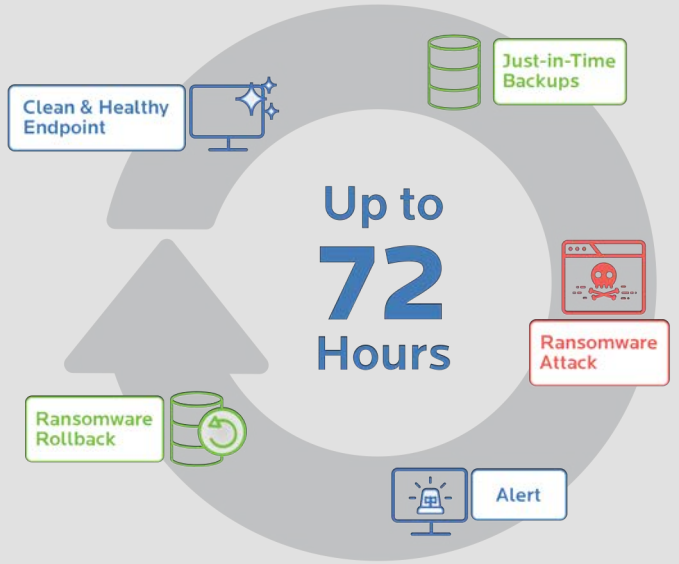
Thorough Remediation

- Cleans up primary payload
- Detects and removes all dynamic and related threat artifacts
- Minimizes end-user impact

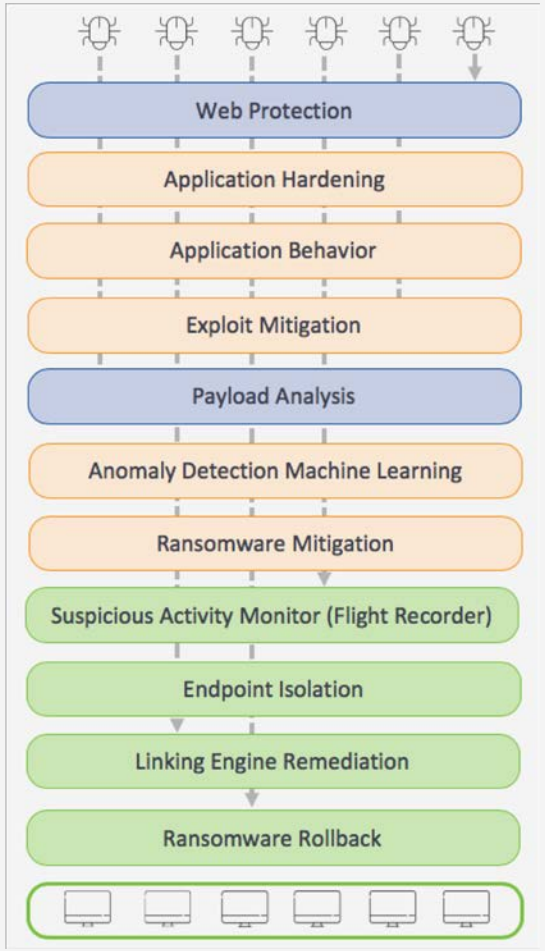


Ransomware Rollback

- Performs just-in-time backups of file changes
- Logs/associates changes with specific processes
- Rollback damage up to 72 hours



Malwarebytes Endpoint Protection and Response



We Don't Just Alert. We Fix It.

EDR WITHOUT COMPLEXITY

UNMATCHED THREAT VISIBILITY

COMPREHENSIVE ATTACK CHAIN PROTECTION

#1 TRUSTED NAME IN REMEDIATION

Thanks!