CROWDSTRIKE

THE FIVE CRITICAL ELEMENTS OF ENDPOINT SECURITY

SCOTT TASCHLER – DIRECTOR, PRODUCT MARKETING

CROWDSTRIKE

ENDPOINT THREATS – EARLY 2000s

MYDOOM
SLAMMER
MELISSA
NIMDA
CODE RED
ILOVEYOU
BLASTER
SASSER
NETSKY

Opportunistic
DoS
Vandalism

CROWDSTRIKE

6 20

CROWDSTRIKE

ENDPOINT PROTECTION – 2019

Gartner Magic Quadrant for Endpoint Protection Platforms, August 2019

2019 Gartner Magic Quadrant for Endpoint Protection Platforms

- 20 vendors listed (24 interviewed)

“This is a transformative period for the EPP market”

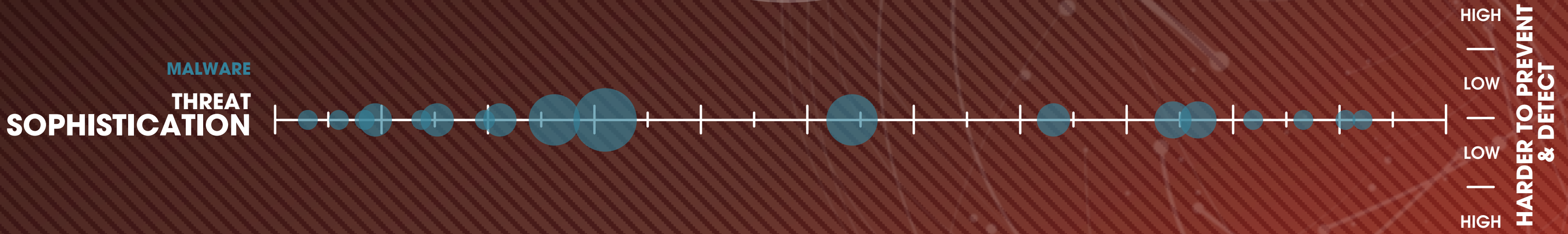
Targeted
Financial
Political

CROWDSTRIKE

OUTMODED DEFENSES

MALWARE

60%



CROWDSTRIKE

OUTMODED DEFENSES

MALWARE

60%

NON-MALWARE ATTACKS

40%

CROWDSTRIKE

SURVIVAL OF THE FASTEST

TO STAY AHEAD YOU MUST:

DETECT IN 1min

INVESTIGATE IN 10min

RESPOND IN 60min

1 Initial Access
2 Execution
3 Persistence
4 Privilege Escalation
5 Defense Evasion
6 Credential Access
7 Discovery
8 Lateral Movement
Collection
Exfiltration
Command & Control
Impact

MITRE ATT&CK PHASE

HOW?

5 CRITICAL ELEMENTS TO ENDPOINT PROTECTION

Prevention

Detection

Hunting

Anticipation

Readiness

PREVENTION – STOP BAD STUFF

- Known and zero-day malware
- Ransomware
- Fileless and malware-free threats
- Always on

PREVENTION-FOCUSED FEATURES

- Machine Learning
- Behavioral
- Exploit blocking
- Memory protection
- Custom whitelisting and blacklisting
- Integrated threat intelligence/IOCs
- Protects without daily updates
- Protects online and offline

CROWDSTRIKE

99%

DETECTION – ALERT FAST

- Detect attacks that prevention missed
- Fast
- Accelerate investigations and response
- Minimize false positives
- Collect data for forensics, investigations
- Develop and execute response

DETECTION-FOCUSED FEATURES

- Endpoint Detection and Response (EDR)
- ML, Behavioral, Threat Intelligence
- Kernel visibility eliminates blind spots
- Visualizations
- Deep forensic data even if endpoint is unavailable, inaccessible or destroyed
- Full context detections and alerts including threat intelligence data
- Response actions

MITRE | ATT&CK™ EVALUATIONS

CROWDSTRIKE

SEVERITY	High
OBJECTIVE	Gain Access
TACTIC & TECHNIQUE	Credential Access via Credential Dumping
SPECIFIC TO THIS DETECTION	A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script.

SEVERITY	High
OBJECTIVE	Follow Through
TACTIC & TECHNIQUE	Execution via Exploitation for Client Execution
SPECIFIC TO THIS DETECTION	Java executed with an unusual set of arguments. This might indicate a Java-based exploit. Review the command line.

SEVERITY	Critical
OBJECTIVE	Follow Through
TACTIC & TECHNIQUE	Exfiltration via Data Compressed
SPECIFIC TO THIS DETECTION	A RAR archive was written by a process with suspicious command line arguments.

MANAGED THREAT HUNTING – SEE AND STOP THE THE UNKNOWN

- Proactive hunt for stealthy, sophisticated threats
- Reduce attacker dwell time
- Prioritize the most urgent alerts and ensure critical incidents are not missed
- Guide response
- Augment current security team

MANAGED THREAT HUNTING-FOCUSED FEATURES

- In-house experienced and dedicated threat hunters
- 24/7 vigilance
- Access to deep pools of telemetry
- Immediate access to real-time threat intelligence
- Provides guidance during incidents
- Tightly integrated into endpoint platform

CROWDSTRIKE

THREAT HUNTING FINDS THE HARD STUFF

Large Financial

STOLEN CREDENTIALS
leveraged for remote RDP login

Mid-sized Telecom

COMMON MICROSOFT ADMIN TOOLS
used to download implants, bypassing detection

Small Academic

SPEARPHISHING
to deliver malicious Chrome extensions

ANTICIPATION – PREPARE FOR WHAT'S COMING

- Maximize defenses
- Prioritize activities and resources
- Proactively defend against future attacks
- Accelerate detections
- Expedite investigations and remediation

ANTICIPATION-FOCUSED FEATURES

- Automatically extract intelligence from local threats
- Provides additional context into alerts and detections for faster, deeper understanding investigation
- Automatic alerts on TI-related activity
- Ingest third-party IOCs
- Adversary profile reports
- Attack attribtion


Indicator Graph
Refine graph
Indicator info
Hash
Indicator intelligence
High
None
Targeted, Suspicious
Financial

READINESS – HARDEN THE BATTLEMENTS

- Find and eliminate risks
- Reduce exposure to attacks

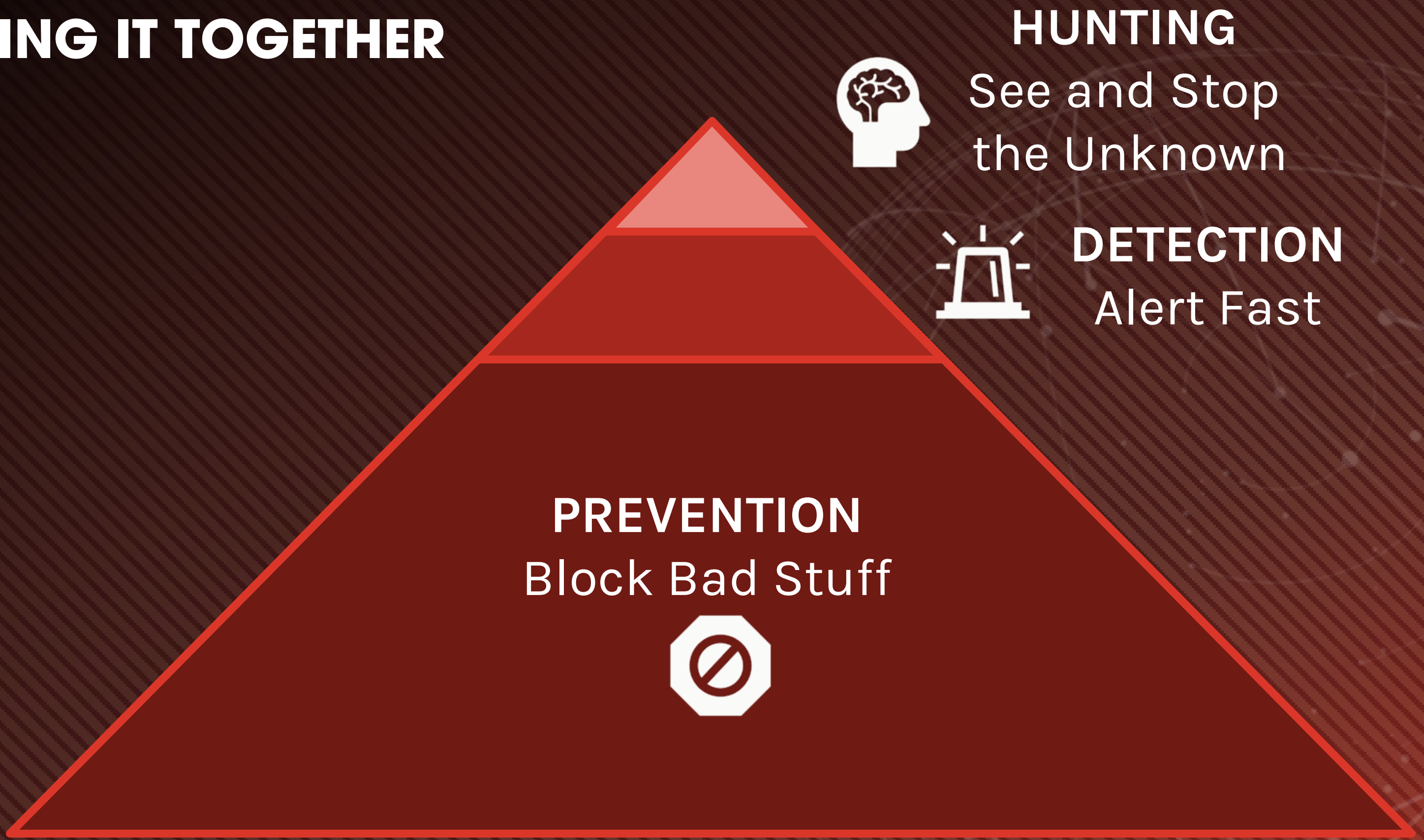
READINESS-FOCUSED FEATURES

- Vulnerabilities
- Account usage
- Provides a real-time view of assets in the environment
- Identifies rogue and unsupported systems
- Causes no impact on endpoints (no scanning)
- Does not require additional agents
- Application usage


Asset Inventory
451
38
289
485
315

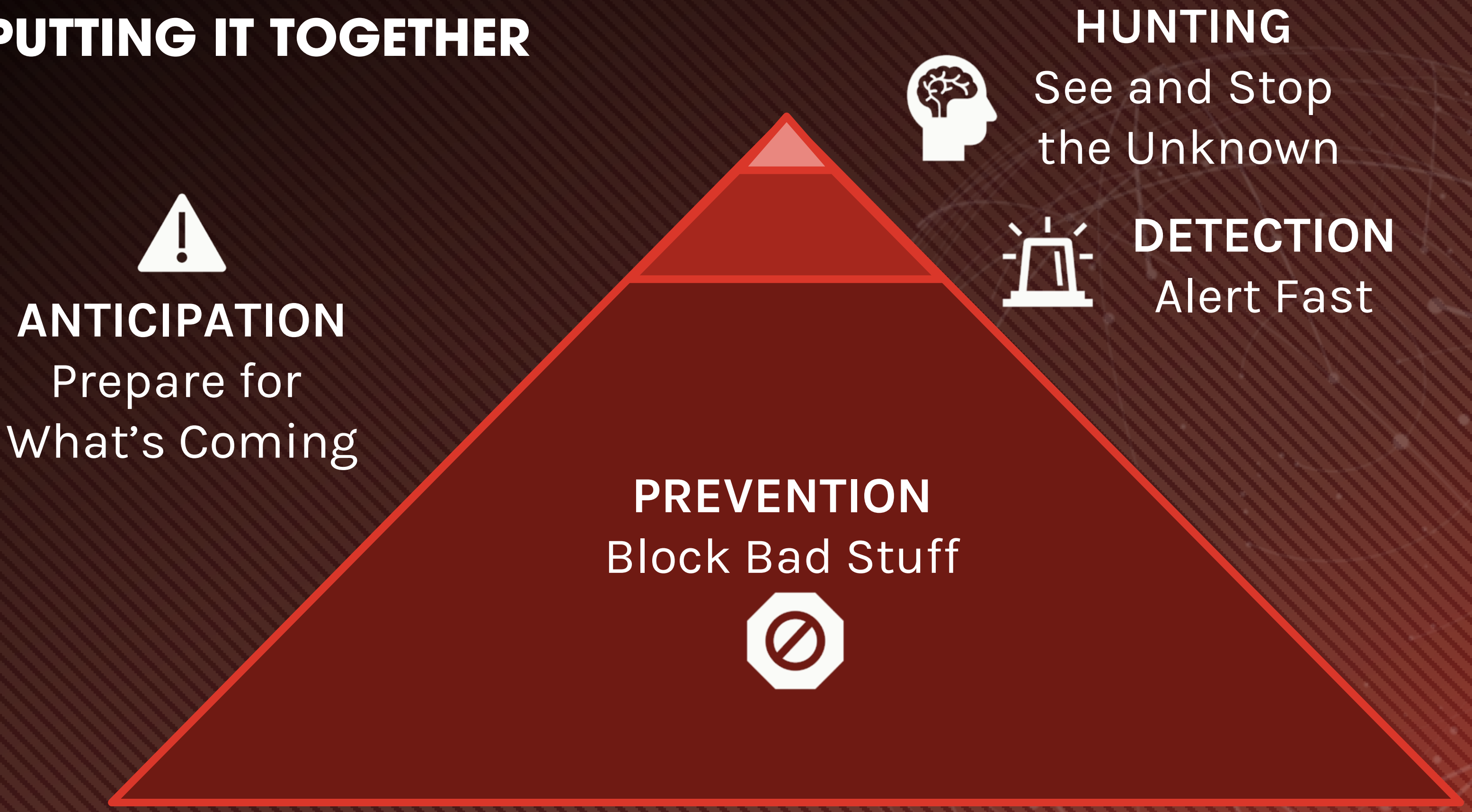
CROWDSTRIKE

PUTTING IT TOGETHER



CROWDSTRIKE

PUTTING IT TOGETHER



CROWDSTRIKE

PUTTING IT TOGETHER

HUNTING
See and Stop the Unknown

DETECTION
Alert Fast

ANTICIPATION
Prepare for What's Coming

PREVENTION
Block Bad Stuff

READINESS
Harden the Battlements

CrowdStrike Products

CROWDSTRIKE

ENDPOINT PROTECTION BUYERS GUIDE

How to select the best endpoint protection solution

THE 5 CRITICAL ELEMENTS OF ENDPOINT PROTECTION

PREVENTION	DETECTION	MANAGED THREAT HUNTING	ANTICIPATION	READINESS
NGAV (Next-generation Antivirus)	EDR (Endpoint Detection and Response)	MDR (Managed Detection and Response)	THREAT INTELLIGENCE	IT HYGIENE AND VULNERABILITY ASSESSMENT

CRITICAL ELEMENT ONE: PREVENTION

PROTECTING AGAINST MALWARE AND BEYOND WITH NGAV

Why you need next-gen AV

There are sound reasons why traditional, malware-centric endpoint protection products simply do not provide an adequate level of protection against today's threats and adversaries.

First, the 99 percent effectiveness rate achieved by malware-focused solutions still leaves a small gap. However, that tiny gap provides a huge window of opportunity for adversaries that can now quickly and easily procure or create zero-day malware. Second, malware-centric protection does not address the increasingly sophisticated fileless and malware-free tactics used by modern adversaries. In fact, studies show that 50 to 60 percent of today's breaches are not caused by malware at all, but rather carried out through techniques such as social engineering or credential theft from other sources.

A sound endpoint protection solution needs to solve those challenges by expanding beyond simply identifying and addressing known malware. First, it should protect against both known and unknown malware by using technologies such as machine learning (ML), that do not require daily updates to be efficient. It should also fully leverage behavioral analytics to automatically look for signs of attack and block them as they are occurring. In addition, the ideal endpoint protection solution should protect endpoints against all types of threats, from known and unknown malware to fileless and malware-free attacks, by combining all the necessary technologies for ultimate protection.

The table below outlines the key use cases and critical capabilities that the NGAV component of an efficient endpoint protection solution should provide.

There are sound reasons why traditional, malware-centric endpoint protection products simply do not provide an adequate level of protection against today's threats and adversaries.

CROWDSTRIKE
FALCON PLATFORM

DEFINING THE SECURITY CLOUD