



CROWDSTRIKE

THE FIVE CRITICAL ELEMENTS OF ENDPOINT SECURITY

SCOTT TASCHLER - DIRECTOR, PRODUCT MARKETING

ENDPOINT THREATS – EARLY 2000s

Opportunistic
DoS
Vandalism

SLAMMERS MYDOOM
MELISSA
CODE RED ILOVEYOU
NETSKY BLASTER SASSER





CROWDSTRIKE

620



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”

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 CrowdStrike. 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. GARTNER is a registered trademark and the Gartner Peer Insights Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual users based on their own experiences, and do not represent the views of Gartner or its affiliates. All reviews and ratings are current as of August 26, 2019.



Targeted Financial Political



OUTMODED DEFENSES

MALWARE
60%

STOPPING
MALWARE
**IS NOT
ENOUGH**

MALWARE
THREAT
SOPHISTICATION



HIGH
—
LOW
—
LOW
—
HIGH
**HARDER TO PREVENT
& DETECT**



OUTMODED DEFENSES

MALWARE
60%

YOU NEED COMPLETE
BREACH
PREVENTION

NON-MALWARE
ATTACKS
40%

MALWARE
THREAT
SOPHISTICATION

NON-MALWARE
ATTACKS

TERRORISTS

HACKTIVISTS/
VIGILANTES

CYBER-
CRIMINALS

ORGANIZED
CRIMINAL GANGS

NATION-
STATES

HIGH
—
LOW
—
LOW
—
HIGH

HARDER TO PREVENT
& DETECT



SURVIVAL OF THE FASTEST

TO STAY AHEAD
YOU MUST:

DETECT IN
1min

INVESTIGATE IN
10min

RESPOND IN
60min



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

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

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

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 attribution

Indicator Graph

Refine graph

99010bc0fa1c0ee22dfc7b69b2b5e3a75895b1bc13d7d06...

Indicator info

TYPE	Hash
FIRST SEEN	May 31, 2018 15:11:24
ALL HOSTS	1
AVAILABLE HOSTS	0

Indicator intelligence

CONFIDENCE	High
WALKING HAZARD	None
THREAT TYPE	Targeted, Suspicious
TARGETS	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

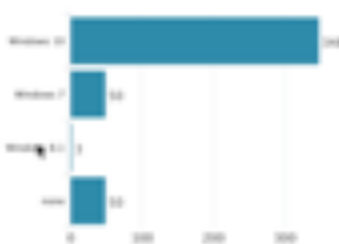
NOTE: Input filters ONLY apply to Unmanaged and Unsupported Assets

Include Subnet (CIDR): Exclude Subnet (CIDR): Exclude WAC Prefix: Exclude Manufacturer(O): Company: Submit [Hide Filters](#)

451

Active Windows Workstations (Last 7 days)

Managed Workstations by OS



38

Active Macs (Last 7 days)

Managed Macs by OS



289

Active Servers (Last 7 days)

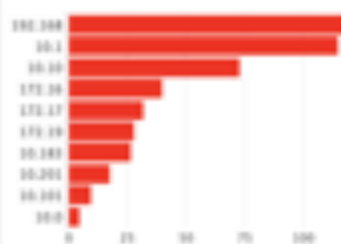
Managed Servers by OS



485

Unmanaged Corporate Assets

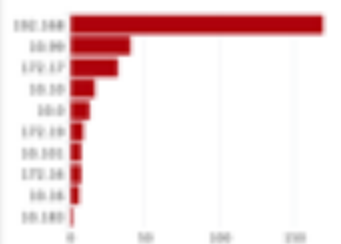
Unmanaged Assets by Subnet (Top 10)



315

Unsupported Assets

Unsupported Assets by Subnet (Top 10)



Managed Workstations by Model (Top 10)



Managed Macs by Model (Top 10)



Managed Servers by Model (Top 10)



Unmanaged Assets by Manufacturer (Top 10)



Unsupported Assets by Manufacturer (Top 10)



PUTTING IT TOGETHER



PUTTING IT TOGETHER



ANTICIPATION

Prepare for
What's Coming



HUNTING

See and Stop
the Unknown



DETECTION

Alert Fast

PREVENTION
Block Bad Stuff



PUTTING IT TOGETHER



ANTICIPATION

Prepare for
What's Coming



READINESS

Harden the
Battlements



PREVENTION
Block Bad Stuff



HUNTING



See and Stop
the Unknown



DETECTION

Alert Fast



ENDPOINT PROTECTION BUYERS GUIDE

How to select the best endpoint protection solution

ENDPOINT PROTECTION BUYERS GUIDE

THE 5 CRITICAL ELEMENTS OF ENDPOINT PROTECTION

PREVENTION	DETECTION	MANAGED THREAT SURFING	MITIGATION	RECOVERY
NGAV (Next-generation Antivirus)	EDR (Endpoint Detection and Response)	MDR (Managed Detection and Response)	THREATINTELLIGENCE	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 move 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 90 to 95 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 second endpoint protection solution needs to solve these 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 analysis 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.

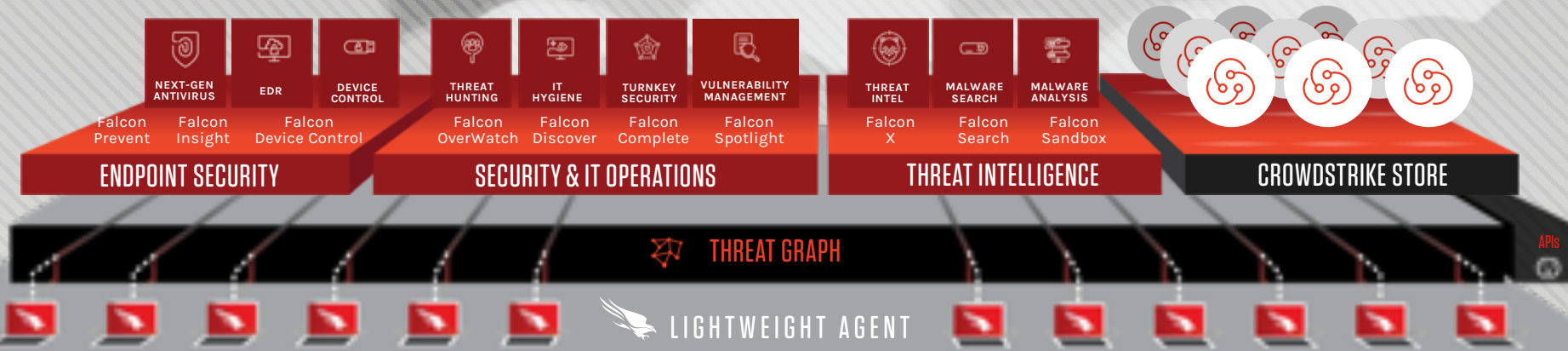
The table below outlines the key processes and critical capabilities that the NGAV component of an efficient endpoint protection solution should provide.

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





START YOUR FREE TRIAL

crowdstrike.com/freetrial

