CROWDSTRIKE

PREVENTING MALWARE AND BEYOND

The Power of **Falcon Host**

Why Prevention **Matters?**

As the security industry and its customers have learned the hard way, prevention is not 100 percent effective. Still, prevention adds tremendous value in weeding out the obvious, allowing security teams to focus their efforts and resources on what truly requires their attention. This is why Falcon Host includes the most powerful prevention features designed to stop malware, and in a much broader scope, to stop breaches.

What Prevention Capabilities Does **Falcon Host** Provide?

Falcon Host offers prevention against malware. But it expands beyond just malware protection by also offering prevention against advanced targeted attacks and attacks that do not use malware, filling the wide gap left by solutions that primarily focus on malware. Faclon Host uses the right detection and prevention feature at the right time to prevent breaches across the entire attack continuum.

Attack Continuum	File Based Detection Signature/Traditional AV File Whitelisting File Reputation	Behavioral Detection Exploit Blocking Host Intrusion Prevent Appliance Sandbox	Other Detections IOC detection Forensics SIEM correlation	Falcon Host Machine Learning Exploit Blocking Whitelisting Indicators of Attack
ATTACK STARTS				
DELIVERY	●	●	●	●
INITIAL BEACH HEAD	●	●		●
ATTACK UNFOLDS				
ESTABLISH PERSISTENCE	○	○	●	●
CREDENTIAL THEFT/PRIVELEDGE ESCALATION			●	●
LATERAL MOVEMENT/EXPLORATION			○	●
FINAL OBJECTIVES				
E.G. DATA EXFILTRATION			○	●

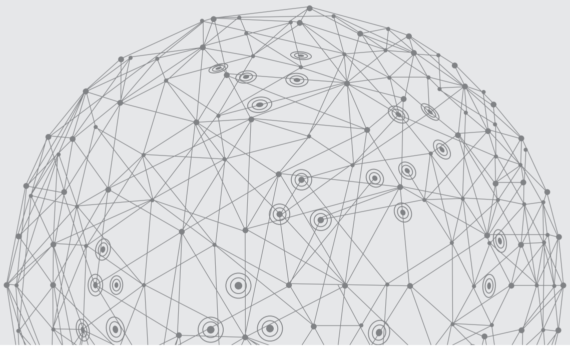
Prevention of **Known and Unknown Malware**

Machine Learning

Machine learning (ML) is used for pre-execution prevention. Falcon Host employs sophisticated machine learning algorithms that can analyze millions of file characteristics to determine if a file is malicious. This signature-less technology enables Falcon Host to detect and block both known and unknown malware. CrowdStrike ML technology has been independently tested and furthermore, it was provided to VirusTotal to contribute to the security community for the benefit of all. For more information about CrowdStrike ML, read the blog, "CrowdStrike Machine Learning and VirusTotal."

Blacklisting and Whitelisting

This feature gives users the ability to upload custom hashes from their own whitelists or blacklists to set either an "always block" or "always allow" policy for known malware and machine learning, allowing other methods such as behavioral indicators of attack (IOAs) to still see and prevent whitelisted processes from performing malicious activities



Prevention of **Malware-Free Attacks**

Exploit Mitigation

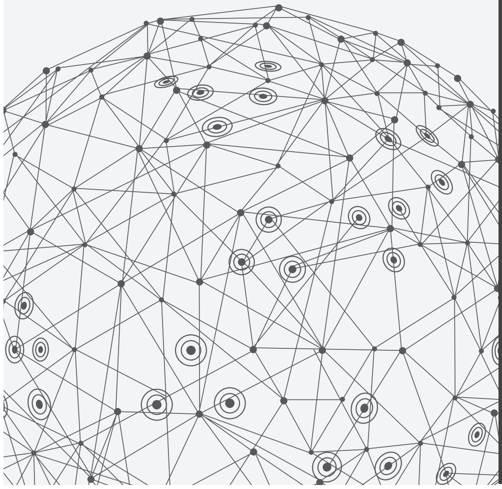
When a malicious actor leverages an exploit as part of either malware-based or malware-free attacks, Falcon Host provides extensive exploit mitigation protection. Exploit mitigation consists of stopping vulnerability exploit attempts andpreventing hosts from being compromised. Falcon Host looks at the pre-execution technique that is being used, rather than the exploit itself, to prevent both known and zero-day exploits.

Indicators of Attack (IOAs)

Sophisticated attackers will not limit their tactics to the use of malware and exploits. For example, they can access tools that are part of the operating system and use them for malicious purposes. Since those executables are legitimate, preventing the malicious activity can be difficult for most endpoint security solutions. In contrast, Falcon Host excels at blocking those types of techniques by using IOAs, which are focused on detecting intent -- what an attacker is trying to accomplish -- regardless of the tools used in the attack. IOA-based prevention capabilities allow customers to prevent threats that bypass traditional technologies such as signatures, whitelisting, or sandboxing. For more information about IOAs, read the white paper, "Indicators of Attack vs. Indicators of Compromise."

Offline and Online Prevention

The **Falcon Host** intelligent sensor offers prevention both offline and online. The sensor supports data processing and decision making on the endpoint. This not only enables highly accurate detection and prevention, but also keeps the endpoint protected everywhere -- in the office or on the road, online or off. Offline protection includes blacklisting, whitelisting, exploit mitigation and indicators of attack. In addition, machine learning at the sensor level is on the roadmap for the end of 2016.



Prevention of Ransomware

To combat the escalating level of sophistication used in ransomware, CrowdStrike uniquely combines all of the methods previously discussed into an integrated approach that protects endpoints more effectively against this threat

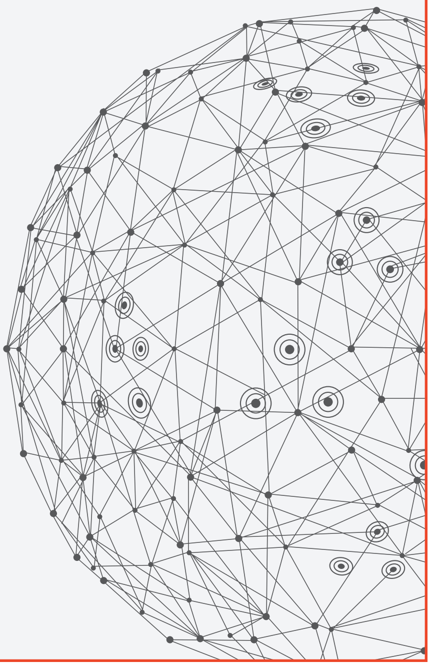
- Blocking known ransomware to eliminate common ransomware variants with minimum effort
- Exploit blocking to stop the execution and spread of ransomware via unpatched vulnerabilities.
- Machine learning for detection of previously unknown, or zero-day ransomware
- Ransomware specific IOAs to identify and block additional unknown ransomware and protect against new categories of ransomware that do not use malicious files, or that rely on legitimate tools such as PowerShell.

To learn more about CrowdStrike's ransomware prevention capabilities, visit www.crowdstrike.com/products/ransomware

> “CrowdStrike solves our prevention, detection and visibility challenges by unifying next-generation AV and endpoint detection and response (EDR) via a cloud-delivered model. Their solution provides us with an advanced level of threat protection and visibility into what is happening in our environment via a single agent.”
>
> **David Giambruno,**
> Chief Information Officer,
> Shutterstock.

Conclusion
Going Beyond Prevention

Falcon Host is unique in combining an array of powerful methods to provide prevention against the tactics, techniques and procedures used by an adversary -- including commodity malware, zero-day malware and even malware-free attacks – to breach organizations. But CrowdStrike knows that however powerful it may be, no prevention is perfect. Thus, customers need the ability to find out and respond if it fails. This is why Falcon Host also includes EDR (Endpoint Detection and Response), to detect the early stages of an attack as soon as possible. This means that with Falcon Host, customers don't have to choose whether to shift their budget from prevention to detection, or ask for a budget increase. They get both prevention and detection in one unified solution.



CROWDSTRIKE

crowdstrike.com | 1.888.512.8906
15440 Laguna Canyon Road, Suite
250, Irvine, California 92618