CYBERARK®

CyberArk and CrowdStrike "Better Together"

Increase Your Endpoint Security by Eliminating the Blind Spots

KEY BENEFITS

- Detect and prevent ransomware attacks through continuous monitoring and in-depth analysis.
- Accelerate response and mitigation through comprehensive threat intelligence and visibility.
- Maintain user productivity with strong security through the removal of standing admin rights, application controls and credential rotation and theft protection on the endpoint.
- Simplify deployment and operations, and experience immediate time to value through SaaS-based solutions.

Privileged endpoint accounts like Microsoft Windows or macOS administrator accounts represent one of the most significant security vulnerabilities an organization faces today.

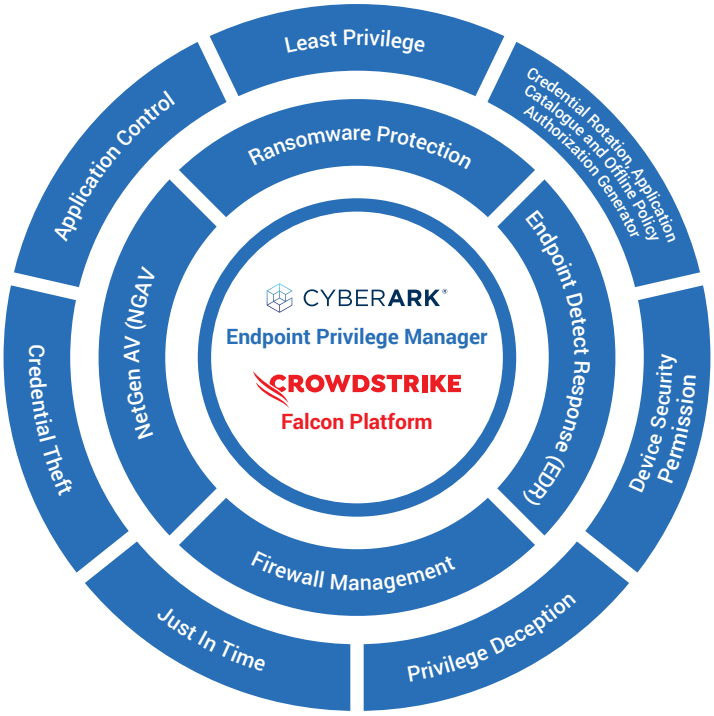
Attackers gain access to privileged account credentials and traverse a network, taking over workstations, VM's, servers, and other critical infrastructure to wreak havoc or steal data. Bad actors also exploit privileged endpoint accounts to disable threat detection and other security programs, install malware and launch damaging cyberattacks.

While most security solutions have the "we can stop breaches" mindset, CyberArk Endpoint Privilege Manager operates with an "assume breach" approach. With both philosophies combined, a better security posture is accomplished.

A "better together" story between CyberArk and CrowdStrike provides customers with the ability to increase security across the organization, secure and respond to security events happening within their environments from Day 1.

- **CyberArk Endpoint Privilege Manager** combines least privilege, privilege defense, credential theft protection, ransomware and application control protection to drastically reduce the attack surface and mitigate the risk of a severe data breach in a transparent way to end users and without impacting productivity. All of this is done with proactive zero trust approach to the organization assets.
- **CrowdStrike Falcon Platform** protects endpoints that access the enterprise, providing advanced threat hunting, next-generation antivirus (NGAV) protection, endpoint detection and response (EDR). Further, CrowdStrike Falcon Identity Protection enables frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics.

FEATURES OF CYBERARK AND CROWDSTRIKE



CyberArk EPM Review of Features:

- **Least Privilege/Privilege Management**
  - Prevent attacks that start at the endpoint by removing local admin rights on Windows workstations, servers, and Macs. Once local admin rights are removed privilege elevation occurs automatically and seamlessly, based on policy, as required by trusted applications to enforce least privilege. Least privilege is an essential part of Zero Trust. Zero Trust models demand that organizations verify anything and everything trying to connect to systems before granting access.
  - Create privilege elevation policies based on Users, Groups, commands, tasks, Trusted Sources such as SCCM, software distributors, updaters, URL and more.
- **Application Control**
  - Application Control allows IT operations and security teams to allow approved applications to run while restrict the unapproved ones. Unknown applications run in 'Restricted Mode' which prevents them from accessing corporate resources, sensitive data or the Internet.
- **Credential Theft Protection**
  - Credential theft plays a major part in any attack. Advanced protection helps an organization detect and block attempted theft of Windows credentials and those stored by popular web browsers (currently 45 credential store protections). Protect OS, browser and file cache credential stores with the Credential Theft Blocking feature.

- **Just in Time Elevation & Access**
  - Add users to a local privilege group for a limited time, provide an audit trail on the endpoint throughout the temporary period the user had privilege rights, revoke and terminate access at the end of the session or before if required.
- **Privilege Deception**
  - Allows defenders to set deception credentials on endpoints that look like privileged credentials. This enables defenders to quickly detect and proactively shut down in-progress attacks when attackers try to leverage these credentials.
- **Ransomware Protection**
  - Malware solved - stop ransomware with Endpoint Privilege Manager, in addition detect and stop suspected credential theft attempts on Windows workstations and servers. OOTB policy definition for protection against ransomware including comprehensive least privilege controls readily tested on hundreds of thousands of malware samples.
- **Device Security Permission**
  - Allows customers to manage access to local resources such as files, folders and registry keys, Windows Service and removable storage devices and determine who has the ability to manage or access which resource.
  - Mitigate risks associated with access control.
- **Services**
  - **Credential Rotation**
    - Protected credentials from CyberArk Enterprise Password Vault are managed locally on endpoints, on or off the network.
  - **Offline Policy Authorization Generator Tool (OPAG)**
    - Enables EPM admins to provide authorization tokens to end users who request use of an application that is currently unavailable to them. This is useful for end users who temporarily do not have EPM server connectivity and are unable to get policy updates pushed to them until they are connected again. In addition, the Offline Policy Authorization Generator tool allows administrators to proactively generate authorization tokens for end users, without waiting for requests from them. These tokens are generated by running the tool in CLI mode.
  - **Application Catalog**
    - Enables quick discovery of new applications in the system, regardless of whether they generated events or are monitored by any EPM Policy.
- **Other Integrations**
  - CyberArk Endpoint Privilege Manager integrates with other technologies to create unified, integrated experiences across diverse disciplines. These examples are threat intelligence, identity providers, SIEM solutions, helpdesk systems, software distributors, configuration management and more.

- **Current vendors can be found under our Marketplace.**

CrowdStrike Review of Features:

- **NextGen AV Replacement**
  - Machine learning and artificial intelligence detect known and unknown malware and ransomware
  - Behavior-based indicators of attack (IOAs) prevent sophisticated fileless and malware-free attacks
  - Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
  - Threat intelligence prevention blocks activities known to be malicious
- **Device Control**
  - Enables clients to determine precisely what devices are allowed or restricted, and the granular level of access granted to each device
  - Mitigate risks associated with USB devices
  - Gain automatic visibility of USB device usage
- **Firewall Management**
  - Create, manage, and enforce policies with a simple centralized approach
  - Defend against network threats, and gain instant visibility to enhance protection and inform action
  - Delivered via the same lightweight agent, management console and cloud-native architecture, it deploys and is operational in minutes
- **EDR**
  - Continuous monitoring captures endpoint activity so clients know exactly what's happening
  - Delivers visibility and in-depth analysis to automatically detect suspicious activity and ensure stealthy attacks – and breaches – are stopped
  - Accelerates security operations, allowing users to minimize efforts spent handling alerts and quickly investigate and respond to attacks
- **Ransomware Protection**
  - Detects and blocks known ransomware
  - Exploit blocking to stop execution and spread of ransomware via unpatched vulnerabilities
  - Machine learning for detection of previously unknown "zero-day" ransomware attacks
  - Indicators of Attacks (IOAs) to identify and block additional unknown ransomware, and protect against new categories of ransomware that do not use files to encrypt victim systems
- **Falcon Identity Protection:**
  - Automatically segments identities (for example, service accounts, privileged and regular user accounts)

- Adds the context of "who" to network attack discovery and investigation, with behavioral analysis for every credential
- Provides unified visibility and control of access to applications, resources and identity stores in hybrid environments
- Improves alert fidelity and reduces noise by recognizing and auto-resolving genuine access incidents through identity verification
- Enforces consistent risk-based policies across cloud and legacy systems to enable Zero Trust architecture with zero friction — actions include block, allow, audit and step-up using MFA

SUMMARY

A defense-in-depth strategy with identity controls and endpoint security technologies working together is critical to combating advanced cyber attacks. CyberArk EPM is designed to substantially reduce the attack surface presented by distributed endpoints by combining least privilege, privilege defense, credential theft protection, ransomware and application control protection. CrowdStrike Falcon is the next-generation enterprise endpoint protection platform spanning across endpoints, workloads, identities and applications, from the network edge to the cloud. CyberArk complements the real-time continuous monitoring and automated response and analysis capabilities provided by CrowdStrike to detect and mitigate advanced threats. Leverage a multi-layered endpoint security solution today to enable your modern enterprise to stop breaches faster.

Visit the **CyberArk Marketplace** or contact your local account team to take advantage of the CyberArk and CrowdStrike joint solution.

About CyberArk
CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. To learn more, visit **www.cyberark.com**.

About CrowdStrike® Inc.
CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security. To learn more, visit **www.crowdstrike.com**.

CYBERARK®