Crowdstrike is an Endpoint Protection solution that is extremely effective in the cloud and endpoint security aspect of Securiy Operations. It is a single agent solution to stop breaches, ransomware, and cyber attacks- powered by world-class security expertise and deep industry experience. It is a **Cloud native, AI powered** solution.

Now, one of the products of Crowdstrike is Falcon which is built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks. It responds to any kind of malware attacks and zero day attacks as such by employing a powerful yet lightweight solution that unifies **next-generation antivirus**, **EDR**, and **threat hunting capabilities**. They all are nicely bounded in a tiny, single, lightweight sensor that is cloud-managed and delivered.

So the Falcon platform includes a wide range of solutions:

- ## ENDPOINT SECURITY SOLUTIONS:
  - **Falcon Prevent (NGAV)**: It is a AV providing comprehensive and proven protection to defend your organization against both malware and malware-free attacks. Incorporating identification of malware, ML and unknown malware, exploit blocking and advanced IOA(**Identifier Of Attack**) behavioral techniques.
  - **Falcon Insight(EDR)**: It allows for continuous and comprehensive visibility to tell you what's happening on your endpoints in real time. The extensive capabilities of Falcon Insight span across detection, response and forensics, to ensure nothing is missed, so potential breaches can be stopped before your operations are compromised.
  - **Falcon device Control (USB)**:
  - **Falcon Firewall Management (Firewall)**
  - **Falcon For Mobile**
  - **Falcon forensics**
- ## SECURITY & IT OPERATIONS:
  - **Falcon Overwatch (managed threat hunting)**
  - **Falcon Discover (security hygiene)**
  - **Falcon Spotlight (Vulnerability Management)**
- ## THREAT INTELLIGENCE:
  - **Falcon intelligence (threat intelligence)**
  - **Falcon Search Engine (Malware search engine)**
  - **Falcon Sandbox (automated malware analysis)**
- ## CLOUD SECURITY SOLUTIONS:
  - **CWPP For multi cloud**
  - **Falcon Horizon (CSPM)**

    - **Container Security**
- **IDENTITY PROTECTION SOLUTIONS:**
    - **Falcon ID threat protection**
    - **Falcon Zero trust**

Falcon also has a SOAR(Security Orchestration Automation and Response) solution. With this **Fusion** solution you can build automated workflows that enable data collection, enrichment, response actions and notifications by simply selecting a trigger, defining conditions and configuring actions. **Falcon Fusion** most of the modules listed above as it is a native solution its easier for it to be dependent on other native features.

Falcon Cloud Security

Let's take an attack/adversary that has occurred in your cloud environment. The single agent and unified solution introduces all the capabilities of an EDR solution into one. In Falcon you can visualize the breach and actively see details that show the attack path analysis and how the adversary gained access into your environment.

After reviewing and narrowing down your breach you can simply go to the Cloud security option in the blade and you can see what are the remediations that are to be followed. And as best practice you can configure an **Admission Control Policy** and other features such as: **IaC scanning**, **CI/CD integration** and **Registry Scanning**

Counter Adversary Operations

It is a unified threat intelligence and hunting team with integrated offering bringing together Falcon Intelligence and Falcon Overwatch. Today's adversaries are increasingly fast and elusive, with rapidly changing motives and tactics. The combination of threat intelligence and threat hunting is essential to detect, disrupt, and stop adversaries.

Threat intelligence informs security teams with the latest adversarial insights so they can proactively adjust protections. Security teams have a lot o errors and threats and remain slow to translate hence this provides adversaries an opportunity to bypass detections and infiltrate the network.

Many organizations do not have the resources or skills necessary to perform threat hunting, giving adversaries the chance to infiltrate, traverse laterally, and compromise confidential data without encountering any obstacles.

This combination of global threat intelligence and insights from local threat hunting benefits multiple teams inside the security organization.

- In-depth technical details on the latest attacks provide **security engineers** the necessary context to deploy comprehensive detection and prevention policies.
- Insights into the latest discovered adversary behaviors gives **threat hunters** new leads on what to hunt for, resulting in faster and more effective hunts.
- Real-time threat context **helps SOC analysts** prioritize alerts and accelerate investigations, resulting in faster and more efficient risk mitigation.
- Providing attribution and detailed threat actor profiles **enables responders** to effectively eliminate malicious activities by helping them understand all pertinent behaviors and vulnerabilities being exploited.
- **Security planners and decision-makers** get trusted strategic insights into threats along with trends and industry-specific reports. This knowledge enables them to assess their risk posture and formulate security strategies, resulting in an enhanced return on investment.

CAO Features:

- CrowdStrike Falcon Adversary OverWatch: Around-the-clock protection across endpoint, identity, and cloud workloads is delivered by AI-powered threat hunting experts, and built-in threat intelligence exposes adversary tactics, vulnerabilities, and stolen credentials.
- CrowdStrike Falcon Adversary Intelligence: End-to-end intelligence automation cuts response time across the security stack and empowers security teams to instantly submit potential threats to an AI-powered sandbox, extract indicators of compromise, and deploy countermeasures — all while continuously monitoring for fraud and protecting your brand, employees, and sensitive data.
- CrowdStrike Falcon Adversary Hunter: World-class intelligence reporting, technical analysis, and threat hunting and detection libraries enable organizations to lower the time and cost required to understand and defend against sophisticated nation-state, eCrime, and hacktivist adversaries.
- CrowdStrike Falcon Counter Adversary Operations Elite: The industry’s first and only white-glove service created to rapidly disrupt sophisticated adversaries with the fusion of industry-leading intelligence and threat hunting. CrowdStrike’s Counter Adversary Operations assigned analysts will use advanced investigative and threat hunting tools to identify and disrupt adversaries across the customer IT environment and beyond.

MICROSOFT EDR VS CROWDSTRIKE:

MDE:

Microsoft's biggest advantage is the unique endpoint protection space, as it is the only vendor to provide built-in endpoint protection capabilities tightly integrated with the OS. Windows defender AV is now a Core component in all Windows OS's and provides cloud-assisted attack protection.

MDE was previously called as Advanced Threat Protection providing EDR, monitoring and response, on AV and Exploit Guard, vulnerability and configuration manager.

It has also released Endpoint Protection for Mac while Linus is supported through platforms. Overall, microsoft has the edge on the various features and native integration.

Since the Company itself is a financially sound tech giant they have the direct incentive to build the most competitive platform possible without pressure of driving growth and appeasing venture capitalists.

Hence, the result is an elegant solution that does more than its competitors, some features like the 'undo' button for the remediation page are unique to Microsoft and make the usability much more satisfying. Although to leverage the features you need to purchase a license and here comes a slight crunch. The licenses of microsoft are far too vast and diverse to carefully choose which would be suitable.

For Example, the bundling of price into the E5 Licensing makes clients unsure if they are paying more or less for the solution and lack of clarity in its licensing for non-windows ecosystems.

The point is that being Microsoft should be able to deliver the same product at a lower price point than competitors that have to pass infrastructure costs on to the end user, this confusion should be lessened as security buyers will look for a shift to a more transparent licensing model as a signal to buy.

All in all this is the best solution and choice for organizations primarily running Windows due to ease of deployment, integration and management provided by the cloud native approach of Microsoft.

MDE Features:

Defender provides malware protection using a range of techniques including behavioral, emulation, script analysis, memory and file scanning, network monitoring and hardening. MDE can also work alongside some other vendors' EPP or EDR agents or will step up to protect clients automatically if a third-party EPP engine fails, is out of date or is disabled, this is called passive and active deployment of EDR.

Microsoft also has a one of the better SOAR Capabilities to integrate with Microsoft partner products and to automate repetitive tasks. Conditional access rules enable a continuous adaptive risk and trust assessment architecture It also stores 6 months of data at no extra charge.

MDE also adds threat and vulnerability management attack surface reduction features: AAC, Network protection, Hardware isolation, FIM

The secure score and vulnerability management and configuration information provide enough context and remediation steps to improve the security posture and endpoint hardening. This score also helps admins and CISO(Chief information Security Officer) an insight and overall understanding into the security posture of the environment along with improvements.

They have also launched a new service known as Microsoft threat experts to support customer incident response and alert analysis.

CONS:

Defender AV and EG are included with all versions of Windows 10. However, most enterprise buyers will want ATP to provide a competitive experience in EDR functions, such as attack visibility, reporting and threat hunting, as well as vulnerability management.

Another limitation would be its limited support to legacy XP and older and the requirement of a license with complex inclusions and higher cost comparatively.

CROWDSTRIKE:

Crowdstrike provides an extensive cloud native platform that enables additional security services like iT hygiene, VA and threat intelligence. It's app store allows customers to acquire additional security functions such as user and entity behavior analytics and FIM through partners that exploit the same client and cloud management console.

It's Falcon Overwatch service which provides managed threat hunting, alerting, response and investigation assistance. Falcon Complete on the other hand provides fully managed detection and response, engagement consulting for incident response and a 1 million dollar breach prevention warranty.

Organizations looking for a modern, cloud native EDR focused EPP solution with a range of managed services will find Crowdstrike extremely suitable. It is also purchased as a standalone product since it's features itself are benchmarks that other companies wish were available in their selected products.

The threat intelligence capability of Crowdstrike is nothing short of a miracle since it is designed to collect and enrich it by feeding the data into their own product and Overwatch service to ensure they are detecting even the most- advanced attacks.

Features:

Crowdstrike has a very huge client base competitively against Microsoft. It is utmost popular in part due to its cloud architecture and its lightweight, single agent supprts all environments physical, virtual and cloud. the cloud architecture comes forth when the Crowdstrike records

most of the endpoint events and sends all recorded data to its cloud for analysis and detection. Some prevention is done locally on the agent via a Machine learning AV.

The agent and management console also takes care of Falcon Prevent protection and Falcon Insight EDR. Recent improvements include vulnerability detection, discovery for AWS and Asset inventory: and security config for cloud assets.

This includes Real time response and Real Time Query to enable remote commands on infected or suspected machines, custom blacklisting and indicators of IOAs for DR.

Falcon is designed to defend against all kinds of malware and their blocking. Crowdstrike has also introduced Falcon for Mobile to isolate corporate apps from unmanaged devices. Thereby reducing any kind of attack surface and securing the environment from almost all kinds of attacks or vulnerabilities that can be exploited.

CrowdStrike is also the first Endpoint Protection vendor to provide Firmware visibility and Vulnerability Detection to reduce the risk of hardware based attacks, it offers agents for a broad range of endpoints and supports new Linux kernels in less than a week. It also extends support for Oracle and Amazon Linux.

CONS:

Unlike MDE Crowdstrike does not have an integrated solution but it works with third party tools. But, the full product is more expensive than other EPP solutions.

Overwatch service covers the cost of cloud data storage for EDR which is used for full hunting and investigation is comparatively very less than what MDE offers which is 7 days as opposed to 6 months.

How Falcon processes data:

- A TLS-encrypted tunnel is used by the CrowdStrike to send between the sensor and the cloud.
- CrowdStrike uses certificate pinning on sensor side. The sensor only communicates with the endpoints that have a known certificate.
- You can allow endpoints in firewall that Falcon sensors only communicate with CrowdStrike.
- CrowdStrike tags the customer data with unique Customer ID, the queries and exchange of data is limited to the scope of specific customer ID, which further secures the data.
- All data in CrowdStrike cloud, including backups are encrypted with Industry standard AES256 encryption.

- Direct access to the endpoints is limited to engineers with business need. Access is protected by VPN and multi-factor authentication.

Falcon is a leading EDR solution due to its single-package lightweight agent process. It supports all the OS's (WML). The sensor continuously monitors process events like process creation, drivers being loaded, disk access, memory access, network connections and registry modifications.

You can go to the hosts and management in the options blade and download the sensor which requires no configuration, no reboot and can be done completely silently.

It occupies very less space (3mb) and uses very less bandwidth (1-5mbps), less RAM (10mb) and practically no CPU overhead. It provides real time detection and prevention of malicious activities(IOC and ML) using different parameters (IOA) thereby maintaining a continuous monitoring, rapid access and hunting capabilities in your data. Real time means it preserves the original state as long as possible.