Companies today are turning to Cynet and newer Extended Detection and Response (XDR) solutions that provide expanded visibility across their environment, preventing and detecting endpoint, network, user and cloud-based threats on a single platform. Cynet also provides extended automated response capabilities to greatly reduce the burden on your security team and ensure threats are quickly and properly addressed before damage can be done.

While activating Microsoft Defender for Endpoint is easy on machines running the Windows 10 OS, it’s far more onerous to install in Apple environments. With mediocre detection capabilities, dangerous delays in alerting and a disjointed set of management consoles, Defender for Endpoints is not optimized for lean security teams. Perhaps more importantly, does it make sense to use a company that continuously fails to prevent attacks that exploit flaws in its own platforms and software?

Further, Microsoft licensing is complex and confusing. Upgrading to Microsoft E3/E5 plans provides more capabilities, but the platform becomes prohibitively expensive and difficult to operate. Upgrading to E5, for example, requires several additional required modules such as:

- Microsoft O365 E5 License
- Microsoft MCAS (free with E5, but you need to pay for storage) – to enhance investigation capabilities
- Microsoft Enterprise Mobility – required for enhanced visibility
- Microsoft Intune – required for DLP
- Microsoft Azure AD premium tier – required for user protection
- Microsoft Azure Sentinel – to extend analytics to networks and users

Cynet has many advantages over Microsoft Defender for Endpoint, especially for lean security teams that can’t afford the time and cost required to leverage solutions that cater to large corporations.

**Top reasons to choose Cynet 360 over Microsoft Defender for Endpoints**

**Elite protection against today’s threats**
Cynet detected 107 of the 109 MITRE ATT&CK techniques (98.5%), 3rd highest across all vendors.

**Visibility across multiple layers**
Cynet provides intuitive visibility into entities, not just events, allowing users to analyze endpoints, user and network-based threats.

**Optimized and automated**
Cynet 360 delivers broad automation capabilities that minimize manual intervention and optimize the power of lean teams.

**Defender against what, exactly?**
Microsoft Defender detected only 98 of 109 ATT&CK techniques (90%), leaving customers exposed.

**You can’t protect what you can’t see**
Microsoft Defender does not provide visibility into network-based threats, while visibility into user-based threats requires a separate license.

**Sprawling and complex**
The Microsoft Defender for Endpoint suite consists of multiple, loosely integrated products that use separate consoles. Extensive and complicated settings, automation is limited to basic endpoint remediation actions.
Visibility is Key to Threat Protection

You can’t protect what you can’t see. Effective protection requires visibility beyond the endpoint.

**We’re Expansive**
As an XDR, we have visibility into endpoint, user and network-based threats. And we leverage deception technology.

**They’re Narrow**
Microsoft Defender for Endpoint only sees endpoint threats, while visibility into user and network-based threats comes with added costs.

**We’re A Solution**
If you want a solution that provides defense in depth out of the box, protecting against endpoint, user and network-based threats along with deception technology, Cynet’s best of suite platform is for you.

**They’re a Component**
If you can afford all the additional tools required for a full threat protection stack, you can use Microsoft Defender as one of your stack components.

It’s All About Protection

The most important feature of any security tool is protection. Speed of detecting, blocking and alerting on malicious activities is critical for stopping threats before they do damage and propagate.

**We Protect in Real Time**
Cynet detects and blocks malicious activities in real time, instantly alerting the security team to ensure attacks are immediately contained and eliminated.

**They’re Protection Is Slooooow**
Microsoft Defender for Endpoints suspicious file analysis can take several minutes, delaying the time for malicious files alerts to show up in the security console. Attackers only need seconds to do damage.

Simplicity Is Complexity Resolved

Many security tools require a steep learning curve and significant ongoing support. Tools that are “overly configurable” often mire users in unnecessary yet time consuming details. Security tools should be easy to learn, intuitive to set up and operate, and accessible by anyone on the security team.

**We’re Intuitive**
If you have a lean security team that wants to focus on what’s important, Cynet 360 requires a very short learning curve to learn, configure and operate. You’ll be up and going in days.

**They’re Confusing**
Microsoft Defender for Endpoints utilizes multiple user interfaces that must be searched to find the settings you want. You’ll be confused for months.
Streamline Operations and Improve Security with Automation

Not every company has a large bench of security experts. Automated cybersecurity solutions allow your team focus on important strategic initiatives.

We’re Automated

Cynet provides a wide array of automated remediation actions across files, hosts, users and networks, including pre-built and customizable remediation playbooks to fully resolve attacks without the need of human intervention.

They’re Manual

Anything but basic host remediation actions require a considerable manual effort that results in very limited automated response capabilities using Microsoft Defender for Endpoints.

We Provide the Whole Attack Story

Cynet’s Incident Engine provides automated attack investigation and reconstruction including root cause analysis and attack scope determination.

They Provide an Attack Snippet

Microsoft’s investigation function provides minimal context on individual endpoints. You’ll need the expensive E5 to see the bigger picture.

Cynet’s Incident Engine automatically launches an investigation following certain high-risk alerts.

- First it traces back to understand how the discovered activity was generated to uncover the root cause of the attack.
- Then it searches to see if the same underlying malicious presence exists anywhere across your environment to uncover the full impact of the attack.
- Finally, it can automatically remove all components of the attack across your environment using built-in remediation workflows or custom remediation playbooks.
Independent Testing Is More Trustworthy Than Vendor Claims

The MITRE ATT&CK evaluation provides open, unbiased testing of leading EDR solutions against simulated attack scenarios. Results can be used to get a sense of vendors’ capabilities.

We Detect More and Better
For the second year in a row, Cynet 360 detected more attack techniques than Microsoft, 98.2% vs. 89.9% in the 2022 evaluation.

Their Detection was Subpar
In its third year participating in the MITRE ATT&CK Evaluation, Microsoft, a top 20 Fortune 500 company could not outperform Cynet in detecting attack substeps. And we’re quite proud.

We Detect Fileless Attacks
Cynet was consistently more successful than Microsoft at detection and telemetry for fileless attacks, including registry and persistence attacks.

They Let Stealthy Attacks Get By
With advanced attacks shifting to stealthier fileless attacks, Microsoft fileless detection performance just doesn’t cut it.

We Are Leaders in Visibility
Cynet leveraged 15 different data sources for detecting threats, the highest number achieved in the 2022 MITRE ATT&CK evaluation. The more data sources, the broader the visibility and the more accurate the detection.

Their Visibility was Just OK
Microsoft leveraged 36% fewer data sources than Cynet (11 vs. 15), meaning less visibility when detecting common attack vectors and less context to help analysts investigate alerts.

No Nickel and Diming
Many security platform providers offer a highly complex pricing structure that aims to reap revenue from a variety of platform and service configurations and add-ons. Most clients, understandably, prefer simplicity and openness.

Our MDR is a Help Center
Cynet Elite and Ultimate packages include a full 24x7 MDR service that continuously monitors all client environments, providing best-of-breed detection and response services.

Their MDR is a Profit Center
Microsoft partners with several vendors (listed in the Azure Marketplace) to provide MDR services. Even the price of a modestly sized deployment is well out of reach for most mid-sized enterprises.

We Provide A Comprehensive Solution
Most companies prefer solutions like Cynet that are intuitive, easy to use and highly automated to reduce the burden on the company’s limited resources at a cost-effective price point.

They’re Very Basic, Unless You Pay
Microsoft Defender for Endpoints provides very basic and limited EDR capabilities. You’ll need the expensive E5 upgrade plus a full SOC to work with the complex platform.
Business Differentiators

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Automate Investigation | Automating the manual process of pivoting against and remediating threats | Simple, light, intuitive management tool bar, harden security settings. Easy platform with multiple integrated investigative settings widgets.

**Features**

**Feature Differentiators**

**Threat Detection and Detection**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Deep Packet Inspection and Allow | Multi-layer malware protection in and detection, including endpoint and behavioral detection, to identify malicious恶意的 ended devices and threats. | Full set of features.

**Investigation and Response**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Incident Engine | Automatically determine root cause and remediate root cause of an attack across environment and related environment remediation actions. | Cynet’s Incident Engine includes automated remediation. Cynet’s Incidence Engine provides automated restore of specific files.

**Backup and Recovery**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Forensics | Forensic database for investigation, threat hunting, and integrated threat intelligence. | Significantly limited to basic EDR forensics.

**Managed Detection and Response (MDR) Service**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Summary view | Simple graphical view of artifacts related to an alert in “Investigation and Response” | Top-down additional details from partner integrations with customized views for different MDR service levels.

**Architecture**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Endpoints | Windows, Mac, Linux | Windows, Mac, Linux

**Deployment**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Cloud, On Prem, Hybrid | Deploy on-premises, cloud or hybrid environments. | Deploy on-premises, cloud or hybrid environments.

**Agent**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---

**Agent malware**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Leverage Cynet’s breadth of malware coverage when host is offline. | Leverage Cynet’s breadth of malware coverage when host is offline.

**Multi-tenancy**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Multi-tenant architecture | Multi-tenant architecture. | Multi-tenant architecture.

**Cloud E2K**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Multi-layer threat detection | Simple graphical view of artifacts related to an alert in “Investigation and Response” | Top-down additional details from partner integrations with customized views for different MDR service levels.

**Agent Protection**

**Capabilities**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Support EDR in cloud on-prem | Agent EDR Protection on-premise & SaaS. | Agent EDR Protection on-premise & SaaS.

**Endpoint Protection**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Full RBAC | Full RBAC | Full RBAC

**Support and Contact**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Accurately send an alert to multiple adders or alerting teams. | Accurately send alerts to multiple teams or alerting teams.

**Automation**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Automated capability that reduces false positives and false negatives. | Automated limitation to basic remediation actions.

**Validation**

**Capability** | **Explanation** | **Microsoft Defender**
--- | --- | ---
Detect new threats, critical vulnerabilities, common attacks, and threats. | Detect new threats, critical vulnerabilities, common attacks, and threats.
Cynet enables any organization to put its cybersecurity on autopilotstreamlining and automating their entire security operations while providing enhanced levels of visibility and protection, regardless of the security team’s size, skill or resources and without the need for a multi-product security stack.

It does so by:

Natively consolidating the essential security technologies (including EPP, EDR, Deception, Network Analytics and more) needed to provide organizations with comprehensive threat protection into a single easy-to-use XDR platform.

Automating the manual process of investigation and remediation across the environment.

Providing Cynet Elite and Ultimate customers a 24/7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting.

**CYNET KEY DIFFERENTIATORS**

**XDR - 360 attack prevention and detection**
Cynet provides attack prevention, detection and remediation against endpoint, network, and user-based attacks.

**Response Automation**
Automated investigation to unveil an attack’s root cause and impact, coupled by automated remediation to eradicate all malicious presence and activity.

**24x7 MDR services included**
Cynet Elite and Ultimate packages include access to a top skilled analyst team that provides alert monitoring, threat hunting, attack investigation and assistance with incident response.

**Deception Security Built-in**
Cynet is the only XDR vendor to include deception technology to lure attackers into revealing their presence.

**Lightspeed deployment and immediate value**
Seamless distribution across thousands of agents within a single hour with immediate security benefits.

**Operational simplicity**
Single lightweight agent delivers all prevention, detection, and response automation capabilities, thereby reducing operational costs and efforts.