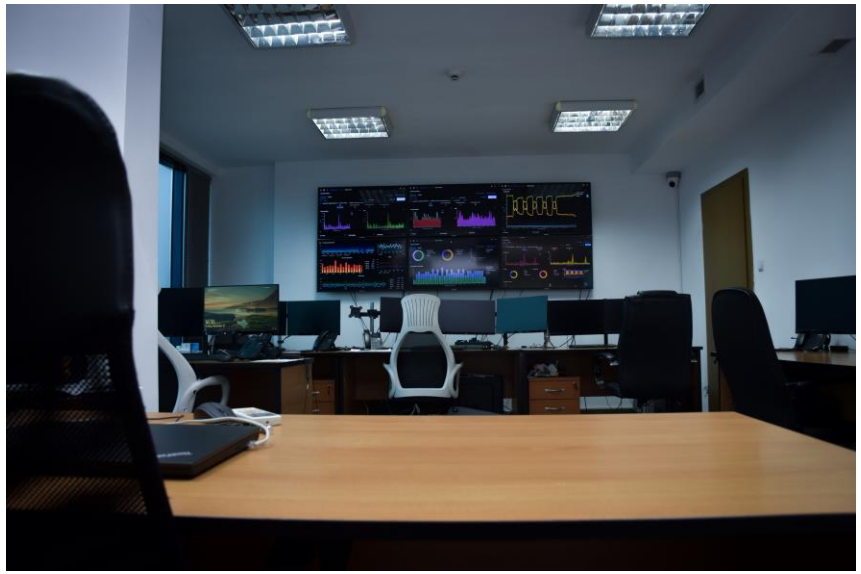
CYBER ONE

Cybersecurity Solutions

More information about us

CYBERONE is a company founded by Israeli and Bulgarian cybersecurity specialists in 2018. The company provide Israeli know-how and variety of technological solutions related to cybersecurity and information technology. The main priority of the company is the successful and effective provision of cybersecurity solutions to businesses in Europe.

Since 2019 the company established their own advanced Security Operation Center in Sofia, Bulgaria. Together with our partners we strive to provide quality cybersecurity and IT services. In addition, we provide complete software and hardware solutions for Cybersecurity and data protection.



How can we protect you?

CYBER ONE

Passive protection

Implementation of mechanisms for passive control and protection of IT infrastructure

Proactive protection

Providing regular penetration tests and vulnerabilities scan

Monitoring

Implementation of innovative solutions for monitoring servers, workstations and networks

Service overview

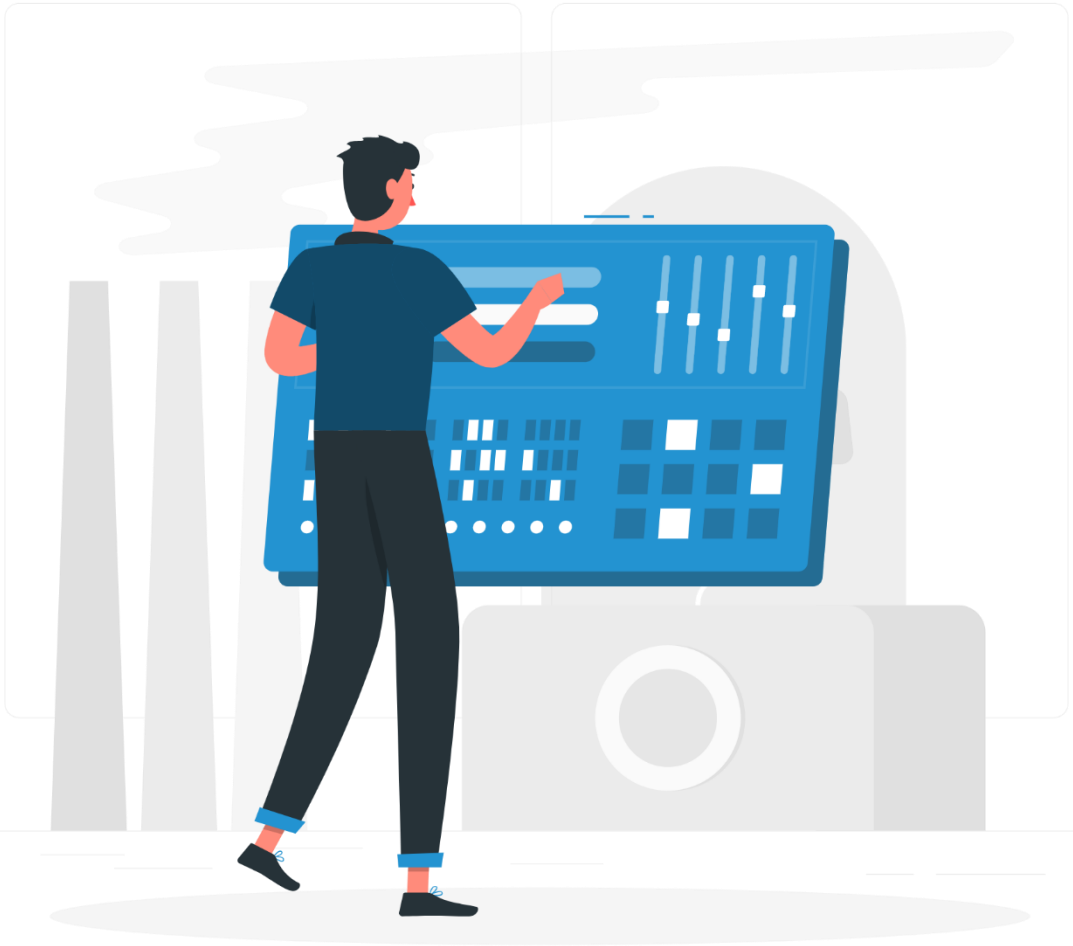
CYBERONE

Malwarebytes

For cybercriminals, corporate endpoints, where data, users and corporate systems all come together to generate and implement business processes, remain the primary target. To protect your corporate endpoints and prevent them being used as entry points into your infrastructure, your IT-security team should be reviewing ways to boost your existing security. Implementing the full endpoint protection cycle, from automatic common threat blocking to responding swiftly and appropriately to complex incidents, requires preventive technologies supplemented by advanced defense capabilities.

Malwarebytes Endpoint Protection provides powerful security with comprehensive visibility across all endpoints on the corporate network together, with superior defenses, enabling the automation of routine tasks to discover, prioritize, investigate and neutralize complex threats and APT-like attacks.

CYBERONE is an official partner of Malwarebytes and as such we can provide our customers with an access to both **Nebula®** and **Oneview®** platforms as part of the service. Whether you use Endpoint protection or Endpoint Protection and Response for your endpoints we will provide you with monitoring and support as well as 24/7 emergency hotline.



Endpoint Protection

CYBER ONE

Malwarebytes

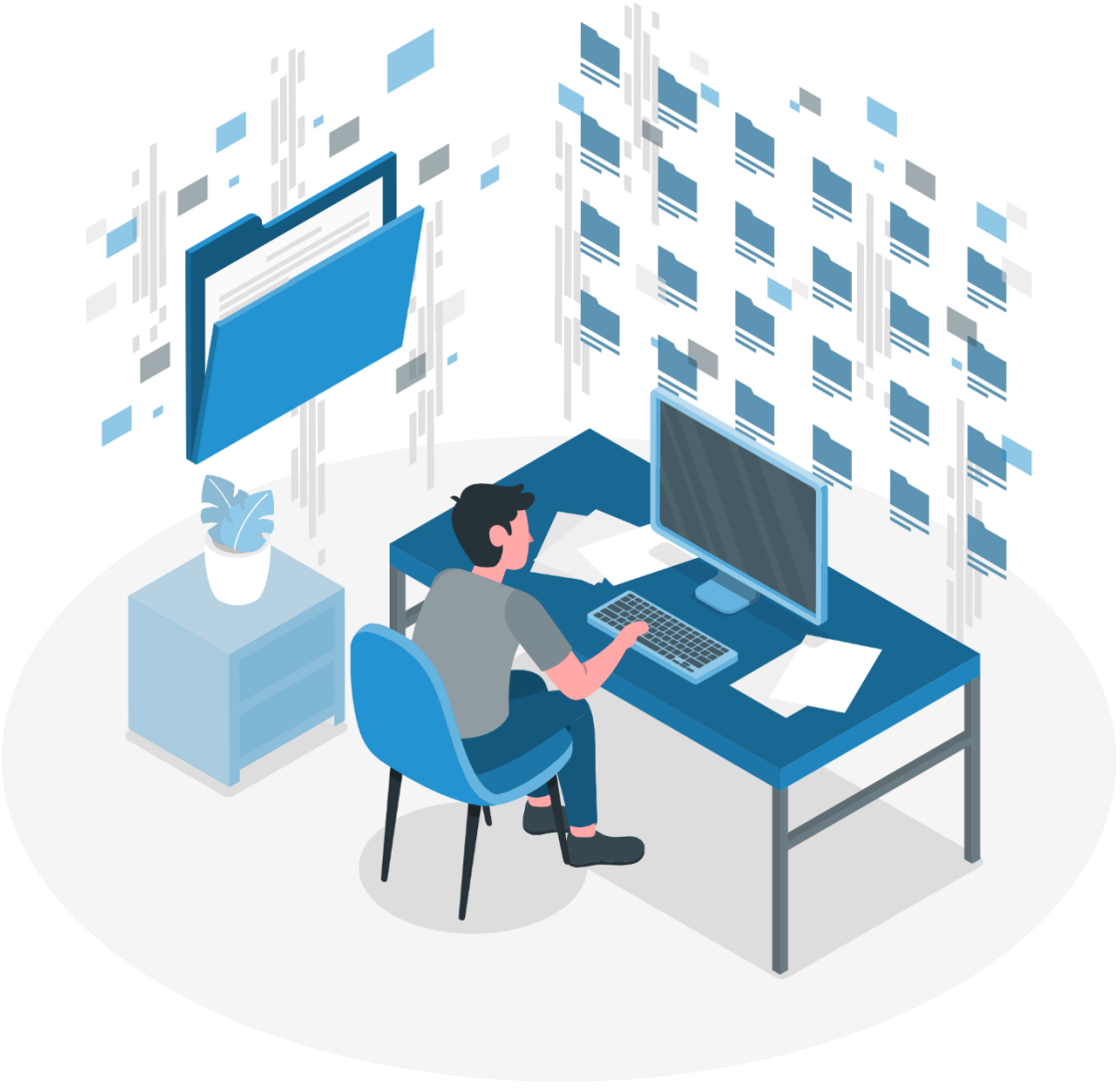
Malwarebytes Endpoint Detection (EP)

for Windows and Mac can easily replace or compliment other endpoint security solutions, including Microsoft Defender. The software is known for it being a non-disruptive, straightforward, and Economical solution to deploy via one endpoint agent, and offer robust integrations and compatibilities.

- Non-disruptive, deploy within minutes (even on AD networks)
- One endpoint agent, simple integration
- Intuitive cloud-native management console which is also used by our SOC.

Enter the world of Malwarebytes Endpoint Protection, a complete malware protection and remediation solution with predictive threat detection, proactive threat blocking, and integrated end-to-end protection. Driven from the cloud through a single pane of glass, Malwarebytes Endpoint Protection provides flexible management and speed for organizations of all sizes.

With our cloud-native solution, you can easily scale in order to meet future requirements. Our cyber intelligence expertise in remediation provides you with a solution that's powered by threat intelligence from millions of endpoints, both business and consumer. The REST API makes it simple to integrate with SIEM, SOAR, ITSM, etc. to further drive automation and compatibility.



Endpoint Protection advantages

CYBER ONE

Malwarebytes

Comprehensive protection and speed

Many endpoint security platforms stuff endpoints with an ever-increasing store of malware signatures and slow performance with brute-force scanning algorithms. In contrast, Malwarebytes uses a single, low footprint agent that quickly pinpoints and blocks malicious code from running without impacting device performance.

The right type of machine learning

Instead of training on malware, the Malwarebytes model is trained to recognize goodware—properly signed code from known vendors. The result is a predictive malware verdict that becomes increasingly faster to determine and incrementally more precise.

Comprehensive web protection

Our web protection technology proactively prevents users from accessing malicious sites, malvertising, scammer networks, and suspect URLs, as well as downloading potentially unwanted programs and potentially unwanted modifications. You can also add additional domains in blacklist or whitelist, depending on your organization's policies.

Fastest threat intelligence on the market

Benefit from Malwarebytes detection and remediation intelligence collected from millions of corporate and consumer-protected endpoints. Even brand-new, unidentified malware is typically eliminated before it can impact your endpoints.

Endpoint Protection advantages

CYBER ONE

Malwarebytes

Hardened devices and apps

Malwarebytes hardens your devices by blocking exploits, stopping remote code execution, and breaking communication with hostile malware servers to dramatically reduce your organization's attack surface.

Unified detection funnel catches more threats

Malwarebytes applies behavioral monitoring and machine learning to profile threats across web, memory, application, and files. Successive learnings along the detection funnel provide increasingly higher detection rates with increasingly lower false positives.

Behavioral-based blocking

Our behavior-based analysis provides near realtime identification of behavior that is undeniably hostile and automatically blocks the threat, delivering the most proactive protection on the market today.

Traces the infection, maps the removal

The Malwarebytes Linking Engine traces every installation, modification, and process instantiation—including in-memory executables that other antimalware packages miss—mapping a complete picture of the threat that enables full remediation.

Endpoint Protection advantages

CYBER ONE

Malwarebytes

Zero-day prevention

Malwarebytes applies signatureless payload analysis and anomaly detection to proactively identify and block malware attempting to exploit hidden vulnerabilities in your organization's operating systems and applications.

Lethal "one-and-done" remediation

Applying in-depth insights from the Linking Engine, Malwarebytes thoroughly and permanently removes both the infection and any artifacts, delivering lethal "one-and-done" remediation.

Fully Cloud managed

A full suite of endpoint security functionality and automation capabilities driven from the Malwarebytes Nebula cloud platform and accessed from an intuitive UI make fighting malware a matter of clicks, not scripts.

Analyzes the impact so you don't have to

Malwarebytes provides extensive threat analysis background along with assessment of its potential impact. Your IT Team can save time and effectively communicate potential impacts to executive management.

Deploy quickly and manage with ease

Deploy within minutes and manage with an intuitive cloud-native console

Detect, isolate, and remediate threats

Reduce risks and false positives; stop threats with multiple isolation modes

Threat hunt and rollback ransomware

Guided threat hunting and Windows ransomware rollback

Endpoint Protection and Response

CYBER ONE

Malwarebytes

Malwarebytes EDR includes integrated endpoint protection and automated adaptive detection techniques that learn along each stage of the threat detection funnel. Unlike more reactive signature-based solutions that allow malware to execute before working, our endpoint protection finds and blocks threats before devices are infected. Malwarebytes EDR proactively and accurately recognizes and prevents both hostile code and suspicious behavior.

The software uses unique Anomaly Detection machine learning to not only detect known threats, but also find unknown threats. Malwarebytes EDR boasts higher accuracy, which is why they have one of the industry's lowest false positive rates. The granular isolation capabilities prevent lateral movement of an attack by allowing you to contain individual machines, subnets, or groups, and continue active response activities.

- ✓ Detects "zero-day" threats with low false positives.
- ✓ Granular isolation for processes, networks, and Windows desktops.
- ✓ Removes executables, artifacts, and changes.

For Windows platforms, Malwarebytes EDR includes unique 72-hour ransomware rollback technology that can wind back the clock and rapidly return your firm to a healthy state. If an attack impacts user files, Malwarebytes can easily roll back these changes to restore files that were encrypted, deleted, or modified in a ransomware attack.

EDR vs Normal antivirus software

CYBER ONE

Malwarebytes

On one hand you have off the shelf anti-malware designed for the consumer looking to protect a few personal devices on their home network. Antivirus stops computer viruses, but it can also stop modern threats like some ransomware, adware, and Trojans as well.

On the other hand you have **EDR** for the business user, protecting hundreds, potentially thousands of endpoint devices. Devices can be a mixture of work-owned and employee-owned (BYOD). And employees may be connecting to the company network from any number of potentially unsecure public WiFi hotspots.

When it comes to threat analysis, the typical consumer only wants to know that their devices are protected. Reporting doesn't extend much beyond how many threats and what kinds of threats were blocked in a given span of time. That's not enough for a business user. Security admins need to know "What happened on my endpoints previously and what's happening on my endpoints right now?" Anti-malware isn't great at answering these questions, but this is where EDR excels. At any given moment EDR is a window into the day-to-day functions of an endpoint. When something happens outside the norm, admins are alerted, presented with the data and given a number of options; e.g., isolate the endpoint, quarantine the threat, or remediate.

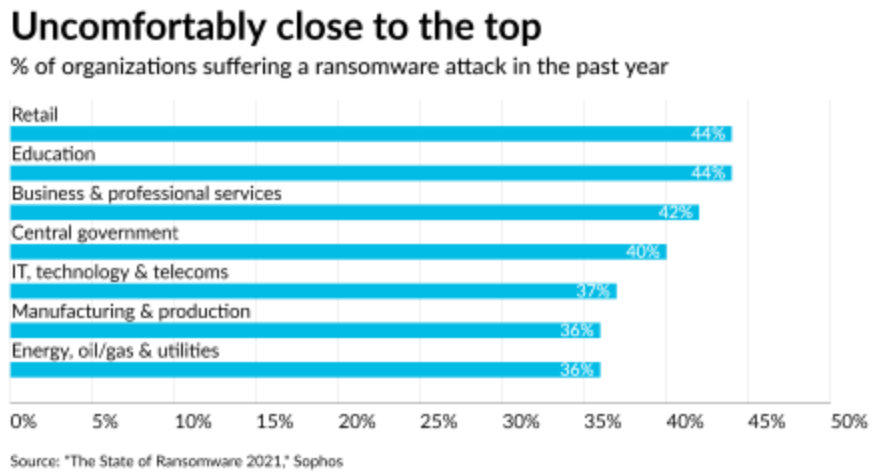
Why companies need EDR?

CYBER ONE

Malwarebytes

The biggest threat at the moment is ransomware. Ransomware detections on business networks are at an all-time high, due largely to the Ryuk, Phobos, GandCrab, and Sodinokibi ransomware strains. Not to mention Trojans like Emotet, which carry secondary ransomware payloads. And it's not just the big name, Fortune 500 companies getting hit.

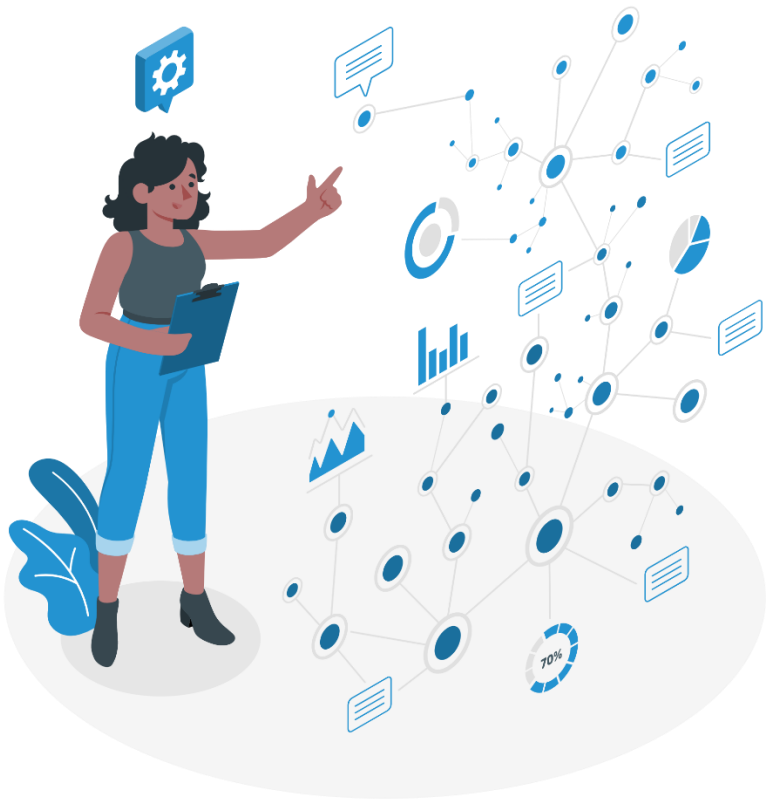
Organizations of all sizes are being targeted by cybercriminal gangs, lone wolf threat actors, hacktivists, and state-sponsored hackers looking for big scores from companies with caches of valuable data on their networks. Again, it's the value of the data, not the size of the company. Local governments, schools, hospitals, and managed service providers (MSPs) are just as likely to be the victim of a data breach or ransomware infection.



Full scale features and capabilities

CYBER ONE

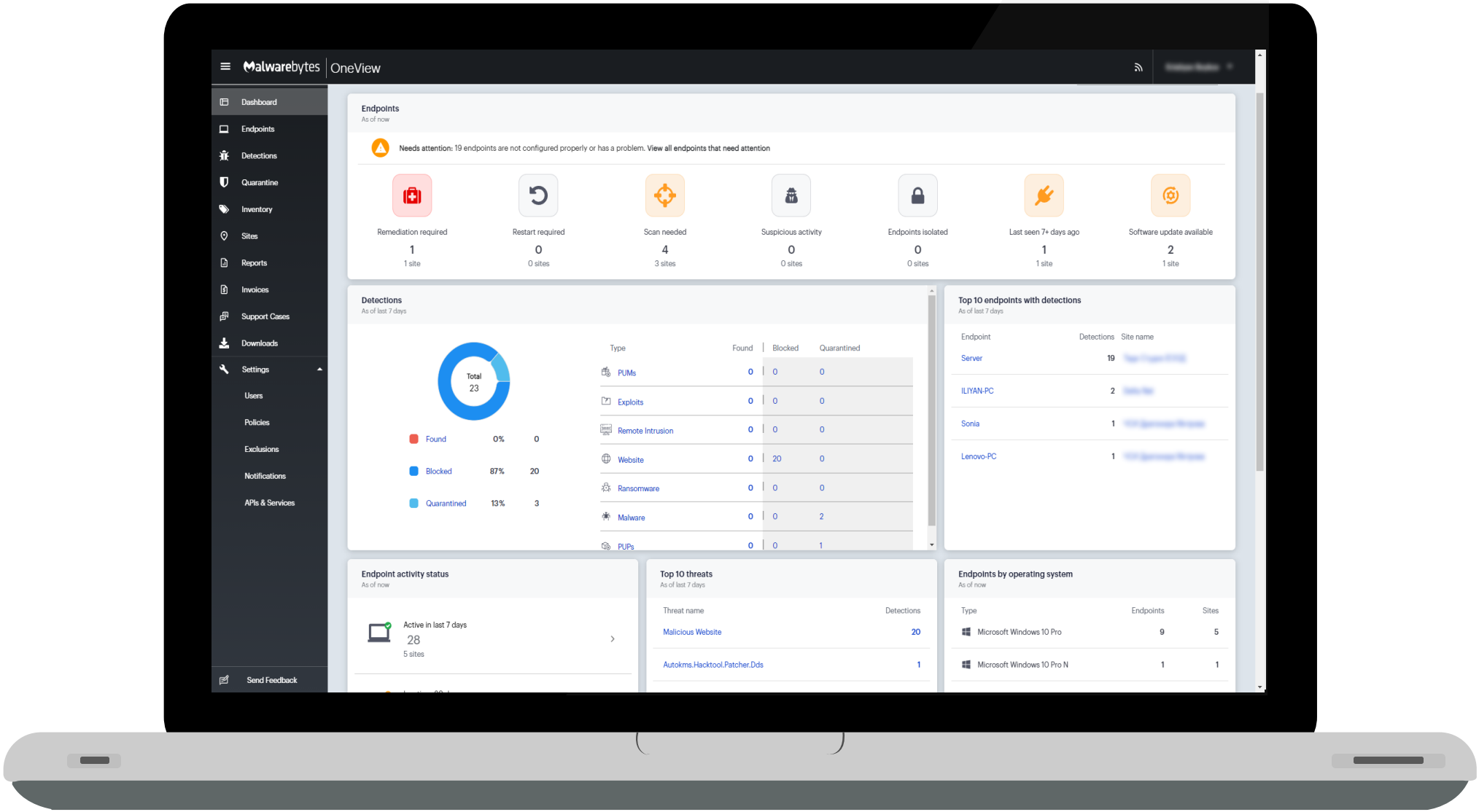
- Process monitoring and recording
- Windows ransomware rollback
- Guided threat hunting
- Cloud sandbox
- Desktop isolation
- Security updates monitoring
- Process and Network isolation
- Remote configuration and management



- Advanced filtering and search capabilities
- Automatic reports and insights by email
- Full inventory of software installed
- Custom blocklist or whitelist
- Granular policy management
- Advanced quarantine capabilities
- On demand malware scan remotely
- On scale system resource monitoring

OneView Cloud Platform

CYBER ONE



Benefits for your company

CYBER ONE

Detecting Incidents

An EP/EDR solution detects incidents that otherwise can go unnoticed. This technology proactively analyses everything happening on the PC to detect indicators of malicious activity. Moreover, since it gathers events from all sources across the network, the system can reconstruct the attack timeline to help determine its nature and impact. The platform communicates recommendations to security controls –for example, directing a firewall to block the malicious content.

Improved efficiency

An EP/EDR tools can significantly improve your efficiency when it comes to understanding and handling events in your IT environment. You can view the security log data from the many different hosts in your system from a single interface. This expedites the incident handling process in several ways. First, the ability to easily see log data from the hosts in your environment allows your IT team to quickly identify an attack's route through your business. Second, the centralized data lets you easily identify the hosts that were affected by an attack.

Compliance with Regulations

Companies use EP and EDR software to meet compliance requirements by generating reports that address all logged security events among these sources. Without such software, an organization need to manually manage all the antivirus software and report/scan on demand.

Incident Management

An EP or EDR improves incident management by allowing the security team to identify an attack's route across the network, identifying the compromised sources and providing the automated mechanisms to stop the attacks in progress.

CYBER ONE

Contact us:

www.cyberone.bg
office@cyberone.bg

+359 88 260 0493

51D “Cherni Vrah” blvd.
Sofia, Bulgaria