Orange
Cyberdefense

Managed Endpoint Security

Next generation endpoint security plays a major part in the protection against modern and advanced threats.

Managed Endpoint Security is a 24/7 Managed Service, protecting your endpoints against advanced threats.

New and advanced technology is necessary in order to protect your endpoints such as servers, workstations, and VDI-clients from the latest threats.

Managed Endpoint Security utilizes the latest in Next Generation Endpoint Security and provides the best protection against the latest advanced and unknown threats such as ransomware, zero-day malware, exploits and other undesirable software.

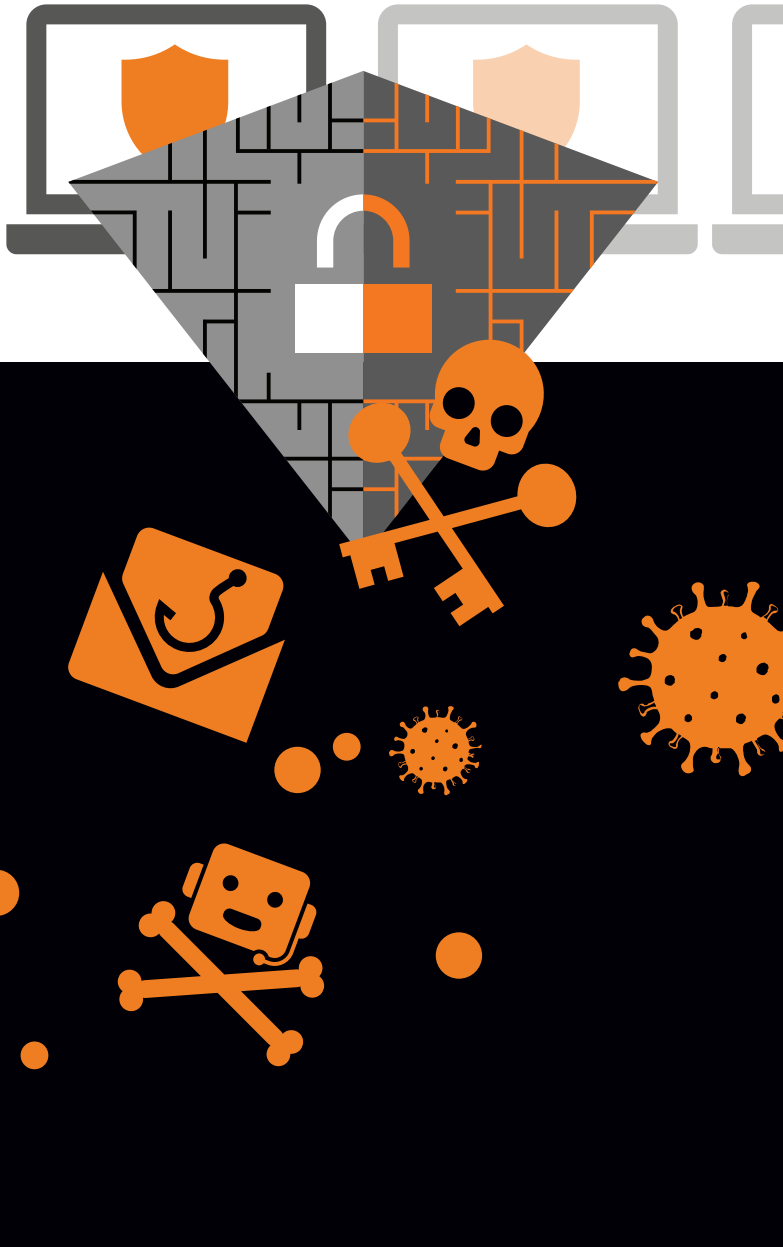
In addition the service also includes standard endpoint control features such as the ability to enforce a policy on device usage like USB mass storage control, helping to enforce policies around usage of removable media and decrease the risk of data exfiltration.

Threats are detected and prevented using multiple methods so that damage can be prevented with world class efficacy. Letting our experts manage the solution also secures that you get the best possible prevention at any given time.

Onboarding with the Threat Clean Service

Our experience shows that when using the Managed Endpoint Security solution for the first time, many (potentially) compromised Endpoints are found with malware or other Potentially Unwanted Programs. Some existing legitimate software might also trigger some detections, which will need to be whitelisted to avoid blocking them from running.

Threat clean onboarding delivers a clear configuration for the Managed Endpoint Security service matching your environment.



Managed Endpoint Security Service includes:

- Third-party vendor subscribtions
- Threat Clean onboarding
- 24*7 support
- On demand changes
- Management console upgrades
- Agent upgrades
- Centrally controlled agent updates
- Monthly reporting

Find out more on how to protect your endpoints on:
orangecyberdefense.com/global/endpoint/

Enhances endpoint security: Malware detection based on profiling malicious behavior. Intercepting and blocking previously unknown malware prevents breaches and avoids regulatory compliance violation.

Quick time-to-value: Recognize the full value of next-generation endpoint protection and advanced feature sets, as well as strong proven processes and reporting. All within short deployment timeframes.

Complete management: Identifitaction and notificationof issues related to device availability. Proactive checks of key device metrics and trends. Full deployment of patches, updates and upgrades to the device specific software.

Automated prevention: Threat Clean deployment services ensures proper deployment and tuning within customer environment. Agent automated prevention actions on machines regardless of their location (in or outside the network).

Challenges

- Management and continuous improvement of endpoint security deployment
- Not enough skilled security engineers to handle the additional workload of advanced endpoint protection.

When should you consider it?

- If you require engineers to help deploy and manage endpoint security
- If you have limited Security engineer resources and want to have analysts, skilled in Delivering change & software Management

What do we do?

- Deploy the EPP platform
- Platform management of console and agents
- Change Management and Software Upgrades
- Incident Management
- License Lifecycle management for the EPP platformIntegration of Orange Cyberdefense unique Threat Intelligence Datalake and custom EDR rules (Premium)

What will you get?

- A deployment according to best practices that looks to make full use of the technology
- Monthly report detailing key operational and security metrics
- Pro-active operations activities

Learn more

If you would like to know more about how our Managed Endpoint Security service, simply Contact us to arrange a free, no obligation consultation, or visit orangecyberdefense.com.