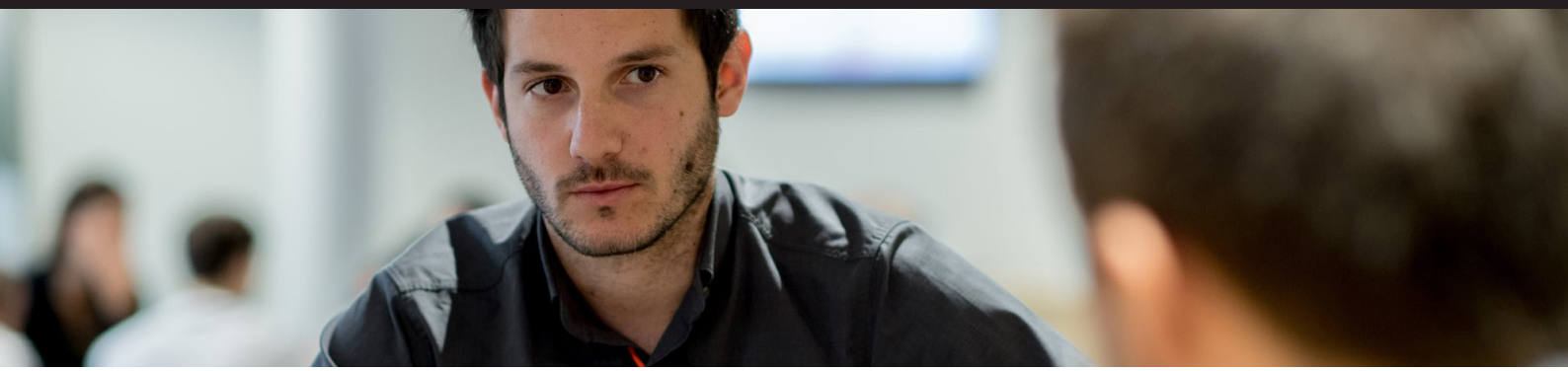
Orange
Cyberdefense



Service overview

Managed Next-Generation Endpoint Security

Key benefits

Enhanced endpoint security
Non-signature based malware detection profiles malicious behaviour without relying on lists of white-listed or blacklisted executables.

Reduced risk
Intercepting and blocking previously unknown malware prevents breaches and avoids regulatory compliance violation.

Incident alert
Identification and notification of issues related to device availability.

Proactive monitoring
Subject to contract, 24x7x365 proactive monitoring of key device metrics.

Service-desk support
Subject to contract, 24x7x365 support to remediate issues in normal operation of scoped appliances.

Patching, updates and upgrades
Where performed remotely, full deployment of patches, updates and upgrades to the device specific software.

Change assessment
Assessment of risk to business-as-usual by requested changes.

Change management
a) In coordination with change processes and change windows specific to the customer business and, b) Assistance with the creation and implementation of changes.

Business continuity
Weekly backups of device policies and hardware configuration.

Service description

With the latest cybersecurity attacks and breaches it has become evident that the endpoint has become the latest battleground. Desktops and mobile devices face increasingly complex and numerous attacks by malicious software (malware) authors attempting to gain an entry point into the network to exfiltrate data or, through ransomware, for financial benefit.

Attackers are not only attacking vulnerabilities in endpoints but are exploiting features within well-known applications. Recent research from SensePost has shown that exploiting features within common Microsoft Office applications have a close to 100% success rate.

Legacy antivirus products, though having evolved through the addition of host intrusion detection and/or behavioural heuristic analysis, still rely heavily on detecting malicious files by matching the file against a database of known bad signatures which leaves a considerable window of opportunity for 'zero-day' malware to take hold and proliferate across the network if there is no signature for it.

Next-Generation anti-malware defences have entered the marketplace to work in tandem with, or replace, signature-based detection. Known variously as sandboxing, containerisation, threat emulation and threat extraction these products seek to fill in the gap between known-bad and known-good by intercepting the execution of the file, profiling the file's metrics and intended actions and then preventing the file's execution based on the probability that it will perform malicious actions.

Our fully managed Next Generation Endpoint Security service removes the complexity of continuous rule-base management allowing in-house IT teams to focus on the tasks the business needs.

By monitoring and managing the endpoint-management server or appliance, Orange Cyberdefense's service offers businesses peace of mind that their endpoints are under constant supervision and have fully updated malware detection mechanisms in place. The service also increases visibility into user behaviour and extends protection against email attachment and web-based attacks to reduce the risk of infection by zero-day.

Why Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Key service components

- Initial application of 'detect-only' policies to the endpoint management server or appliance followed by finer tuning for a period of 30 days working with the customer to configure policies according to required actions and severity
- Creation of initial whitelists and blacklists to allow or deny execution of files
- Ongoing fine-tuning of endpoint- or user-based policies and signatures on a monthly basis
- Creation of additional policies or amending existing policies as part of the business's change control process
- Signature updates deployed according to agreed customer schedule. (Due to updates being automated the agreed schedule should include customer resource allocation to test critical applications)
- Reports detailing the top 50 events detected, along with key related metrics including, for example: Top malware blocked, Top malware detected, Top infected endpoints