Orange
Cyberdefense

SecurePrevent Endpoint

Next generation endpoint security is a major part of modern multilayer security models

SecurePrevent Endpoint is a 24/7 Managed Service, protecting your endpoints through artificial intelligence.

New and advanced technology is necessary in order to protect your endpoints from the latest threats.

Endpoints such as servers, workstations and VDI-clients. Traditional signature based solutions can no longer offer satisfactory protection and have a negative impact on the systems overall performance.

SecurePrevent Endpoint relies on the “Next Generation Endpoint Security” approach. This monthly pay-per-point-service provides the best protection against the latest and unknown threats such as ransomware, zero day malware, exploits and other undesirable software.

To reliably detect threats, SecurePrevent Endpoint uses artificial intelligence. Mathematical algorithms are created by analyzing large amounts of data that is then ported to the endpoint.

Threats are detected at an early stage, before execution, so that damage can be prevented before they attack. The impact on a company is noticeably reduced, and as a result no backup has to be restored after a Ransomware attack.

Onboarding with ThreatClean

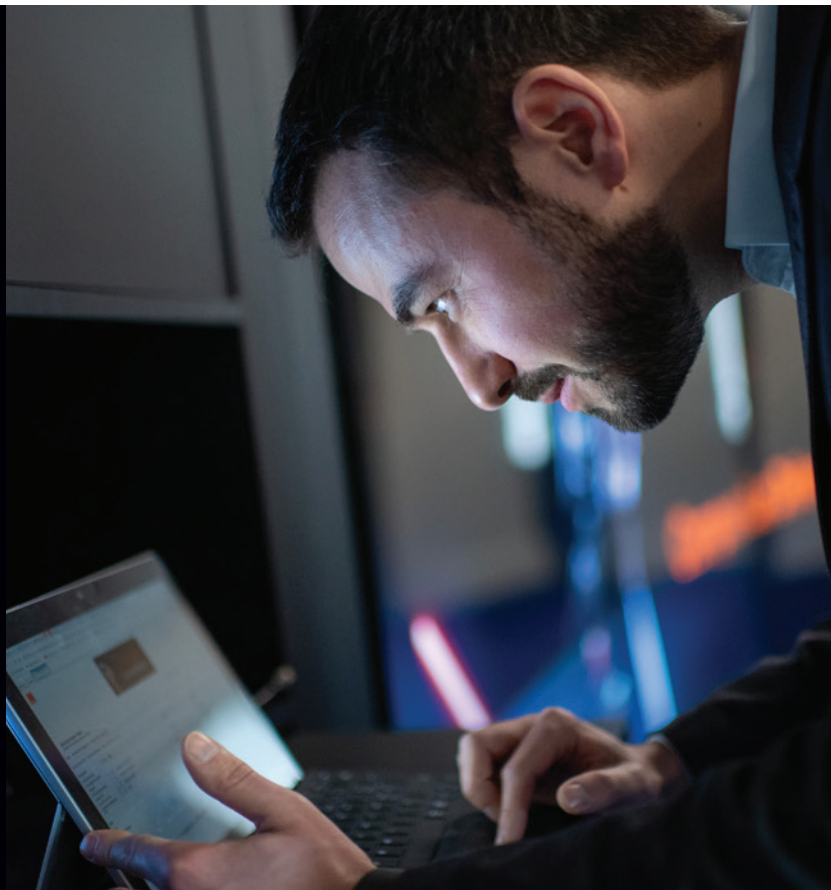
Our experience shows that when using the SecurePrevent next generation endpoint security solution for the first time, many (potentially) compromised Endpoints are found with malware or other unwanted software (PUP).

For optimal use, all endpoints must have a clean and verified status. ThreatClean is the onboarding process that makes all Endpoints part of the managed service. After a pre-defined step-by-step process, your environment is transferred into a threat free state that is fully protected.

The SecurePrevent Endpoint package includes:

- CylancePROTECT subscriptions
- ThreatClean onboarding
- 24/7 support
- On demand changes
- Updating management
- Updating agents (centrally controlled)
- Monthly pay-per-point-service
- Monthly reporting

Pro Service



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

Benefits:

- Proven solution: tested with 99,80% detection rate under real-life conditions
  (Cylance prevented WannaCry, Petya, NotPetya, TrickBot, GermanWiper, GandCrab, RYUK, Emotet and many more!)
- Professional, hassle-free setup and onboarding adapted to your requirements
- Reduce your risk of falling victim to file-based malware campaigns like typical ransomware attacks significantly
- Future-proof: AI protects your endpoints from yet unknown threats and zero-days
- Resource friendly: protect legacy systems operating on restricted hardware resources
- Signature independent: requires no infrastructure to provide daily updates or permanent online connection to maintain reliable protection
- Be aware of what's going on in your endpoints: get monthly reporting on prevented threats

ThreatClean Deployment	Week 1	Week 2	Week 3	Week 4
Consultants Guide Initial Console Setup	■	■	■	■
Status meeting	■	■	■	■
Agent installation complete by end of every week	■	■	■	■
SecureLink experts quarantine malware as alerts are generated	■	■	■	■
Consultants and malware forensic team continue monitoring console		■	■	■
All malware is quarantined			■	■
All malware alerts are classified			■	■
Potentially unwanted programs (PUPs) are reviewed			■	■
Devices are set to auto quarantine			■	■
Memory protection and script control is enabled in alert-only mode			■	■
Memory and script alerts are reviewed				■
Devices are moved to memory/scripts block/terminate policy				■
Additional testing and progress for high-risk devices				■

CylancePROTECT

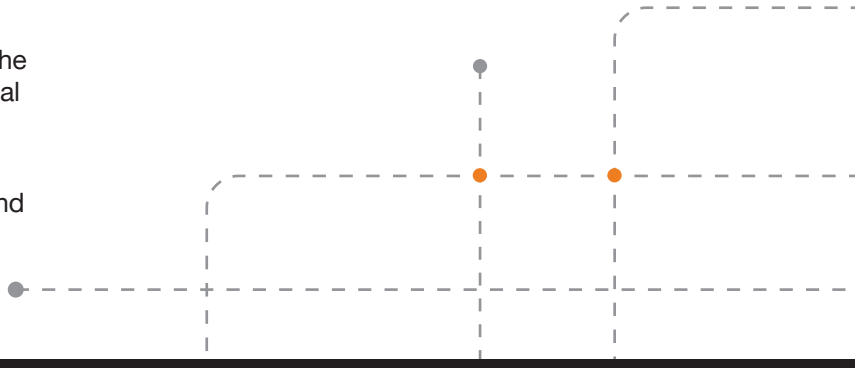
SecurePrevent is based on Cylance technology.

CylancePROTECT is an agent (Windows XP SP3, Mac and Linux) that leaves a minimal CPU and memory footprint on the Endpoint. The agent communicates with a cloud-based management environment (Cylance Console).

The mathematical model used is trained by supervised machine learning based on large data analysis, which is then deployed to the individual endpoint. In addition to the analysis of files, CylanceProtect provides many additional modules such as memory protection and script control.

Memory Protection monitors the running processes for exploits, while Script Control monitors running scripts and stops them in case of damage.

The only way to become aware of threats is to actively manage CylanceProtect in order to carry out further tests. Our security analysts analyze all reports, critically assessing them and taking any necessary actions. SecurePrevent Endpoint is managed from the 24/7 expert run Orange Cyberdefense Security Operations Center.



For more information check
https://orangecyberdefense.se

Orange Cyberdefense
Stenbärsgatan 6, 212 31 Malmö

info@se.orangecyberdefense.com
+46 10 202 20 13