Magenta Managed Detection & Response Endpoint

Effective protection through comprehensive SOC service bundled with Endpoint Security

Red alert: This is how vulnerable companies are

Not only the number of cyber attacks is continuously increasing but also the complexity of attackers is constantly growing and makes it more and more difficult to detect attacks on one's own company. The consequences of attacks range from data theft and operational downtime to espionage and massive damage – monetary wise, but also to the company's image.

One thing is clear: the costs in the event of an attack are serious. It doesn't matter whether these costs are material in the case of a loss of business or immaterial in the form of reputational damage. It is time to act. Conventional firewalls and antivirus solutions are not sufficient to adequately protect corporate assets. At the same time, however, there is often a lack of time and money to implement holistic security projects.

Increasing complexity of attacks requires professional response

Magenta MDR Endpoint combines intelligent defense mechanisms with the knowledge and experience of our SOC specialists. The use of a state-of-the-art Endpoint Protection and Endpoint Detection & Response solution enables our experienced security analysts to continuously monitor all activities on your endpoints to analyze and evaluate suspicious events and filter false alarms. This enables us to quickly respond to ongoing threats, stop processes before they run, and isolate endpoints from the network before they can cause further damage.

Your benefits at a glance:

1. Full-scale SOC with continuous analysis

2. Ability to trigger and perform response measures

3. Regular review processes and threat hunting to detect sophisticated attackers

4. Weekly consultation from our security experts and continuous improvement of your security level

5. More than 20 years of experience in security projects

T··Systems·

Let's power
higher performance

Components for your cybersecurity perfectly combined

T-Systems Security Operations Center
Continuously analyzes suspicious activities

Access to the knowledge of our security experts of one of the biggest SOC providers in Europe

1. Ongoing information and reporting on the current security status
2. Weekly sessions of consultation about the current security status and possible improvements
3. Real-time support for security incidents
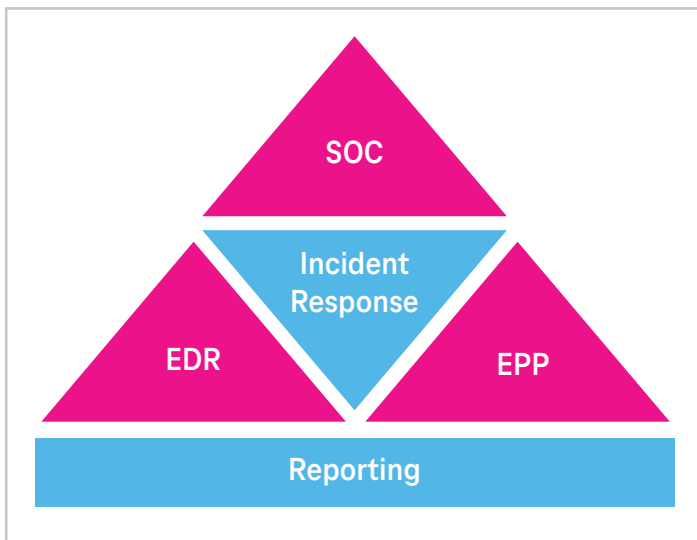
- EDR: Endpoint Detection & Response
- EPP: Endpoint Protection
- SOC: Security Operations Center

Protection: Endpoint Protection
Blocks the execution of suspicious files or processes

1. Protection of all endpoints such as clients and servers
2. State-of-the-art security solutions enable multi-level protection mechanisms
3. Machine learning algorithms prevent the execution of malicious processes, threats can be detected and averted at an early stage
4. Central management platform enables comprehensive security analysis and replaces the existing anti-virus solution

Detection: EDR and SOC
Collects process information for analysis by SOC experts

1. Review and triage of alerts to determine severity and recommended action
2. Continuous finetuning by our SOC analysts to reduce false positives
3. EDR enables in-depth analysis of processes causing suspicious behaviour
4. Remote sessions on endpoints for advanced analysis and hunting via EDR
5. Regular threat hunting is performed in addition by experienced analysts to investigate potentially existing compromises and find sophisticated low-profile attackers that avoid generating alerts

Response: EDR and Incident Response
Initiation of countermeasures in the event of an attack

1. SOC can trigger response measures remotely based on analysis results

   - Isolation of hosts
   - Stopping of processes
   - Blocking of executables

2. T-Systems has an incident response team ready to respond to large scale compromises

---

- Do you want to increase the security of your endpoints, but don't have enough experts?
- Do you have problems ensuring the security and compliance of your endpoints?
- Are you uncertain about which is the right security solution for your needs?

Get to the next level of cybersecurity now!
Use state-of-the-art security tools and trust our experts, who always support and guide you in the defense and handling of security incidents.

Expert Contact

Silvija Andjelovic
Cyber Security Expert
silvija.andjelovic@t-systems.com

Contact

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: cyber.security@t-systems.com
Internet: www.t-systems.com

T··Systems·

**Let's power
higher performance**