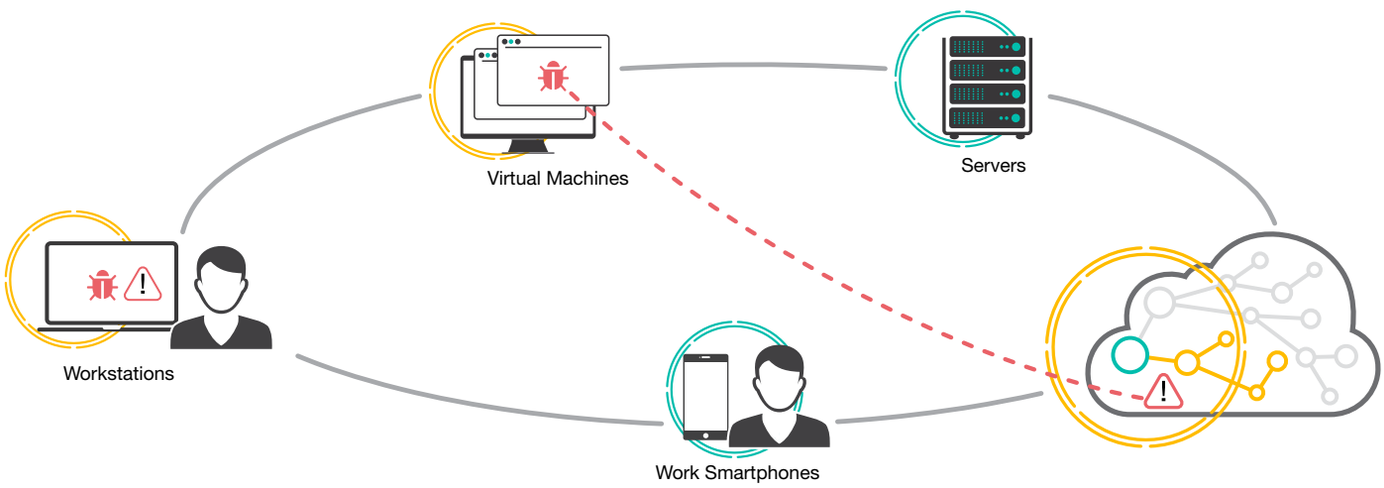
SECURITY SERVICES AG

CLUE

ADVANCED ENDPOINT PROTECTION

Threats caused by cyber-attacks are currently greater than ever before, and attacks are increasingly becoming more automated and complex. Newly discovered vulnerabilities for which no patch exists, also called zero-day vulnerabilities, are increasing in frequency and scope. As a result, the effort required to protect endpoints continues to increase. Classic, signature-based antivirus programs are no longer effective enough to solve this problem, since these can only react to known attacks. Clue's Advanced Endpoint Protection successfully re-establishes protection in the face of cyber threats and establishes an optimal defense against the current threat environment.



AI BASED DETECTION ENGINE

Cyber attacks are becoming increasingly difficult to detect. The Advanced Endpoint Protection Service therefore uses artificial intelligence (AI) in addition to traditional detection via hash values to identify attacks on IT systems. The AI is used locally so that basic protection is guaranteed even if the endpoint cannot connect to the central console. Additionally, a powerful AI that runs centralized can leverage data over long periods of time and across devices to detect even the most complicated attacks.

STORYLINE

Cyber attacks are complex operations which consist of various processes that perform individual malicious subtasks. With Storyline you get an overview of all processes – how they are connected and in which order individual steps were executed. Many sub-processes from an attack are combined into a single notification and depicted in a central dashboard. This structured overview enables a fast and targeted response.

AUTOMATIC RESPONSE

Advanced Endpoint Protection not only provides rapid attack detection, but can also respond immediately. In case of an attack, the process and affected files are automatically quarantined so that they can no longer affect the endpoints. In addition, changes to system settings and registry can be restored back to the state they were in before the attack, either automatically or with a single click.

ADVANCED ENDPOINT PROTECTION FEATURES

ONE-CLICK ATTACK ROLLBACK
If files were encrypted or destroyed by a malicious process, there is a possibility to restore them to the state before the attack. This allows ransomware attacks to be cleaned up with a simple click.

CUSTOM DETECTION RULES
In addition to automatic detection, it is also possible to write custom detection rules. These can be used to react quickly to new types of attacks and they are explicitly marked as such.

DEEP VISIBILITY
Collected data from all endpoints is subsequently examined to allow complex queries to be made and necessary detection exceptions to be estimated.

FILE FETCH
If there is an incident, it is crucial to examine the potentially malicious file. Because of this, there is the possibility to reload the files directly from the dashboard for examination. This eliminates the need to examine them at the end point..

SECURE REMOTE SHELL
Remote investigation of an endpoint through the operating system shell can be easily performed after an incident. This feature avoids the need of shipping the device around. This saves time and costs.

HOST-BASED FIREWALL RULES
In order to further strengthen the protection of the endpoint, the firewall of the endpoint can be used to further restrict unwanted connections (e.g. network connections, internet connections, etc.). This allows the host firewall rules to be centrally managed and set up.

AUTONOMOUS HOST ISOLATION
Endpoints can be automatically disconnected from the network when attacks are detected to further mitigate the spread of attacks. Only the connection to the central platform remains, which allows the attack to be analyzed and resolved.

OPERATING SYSTEM SUPPORT
In addition to good protection, a broad coverage of operating systems is also necessary to guarantee protection for devices from different manufacturers. Clue's endpoint protection covers all currently popular operating systems (MacOS, Windows clients and servers, Linux distributions, virtual machines).

AUTONMOUS INCIDENT ANALYSIS
In the event of an attack, it is important to quickly identify and understand it. For this purpose, the individual procedures and processes are enhanced with additional information in the event of an attack. The steps are thus enriched with references from the MITRE ATT&CK framework in order to better understand the attacks.

UNSER SERVICE

Our Advanced Endpoint Protection Service provides protection through a wide range of detection mechanisms. With this approach, endpoints can be optimally protected from very complex attacks. Through a design that is customized to suit your business, we ensure that you benefit from the same high level of security around the clock.

CLUE-LESS?

Clue Managed Services expands your team by giving you reliable access to security experts who help you to strengthen the security of your company. Proven products, tailor-made features and your very own personal support structure – we meet your requirements at a low TCO. The monthly service fee eliminates high investments and training costs, enabling you to use our services in a modular way.

NEXT STEPS

Are you interested in upgrading the security in your company? Do you want to learn more about the benefits of Managed Advanced Endpoint Protection? Do not hesitate to contact us and we will be happy to discuss these and further questions with you.