

Advanced Endpoint Protection

The Attack Surface

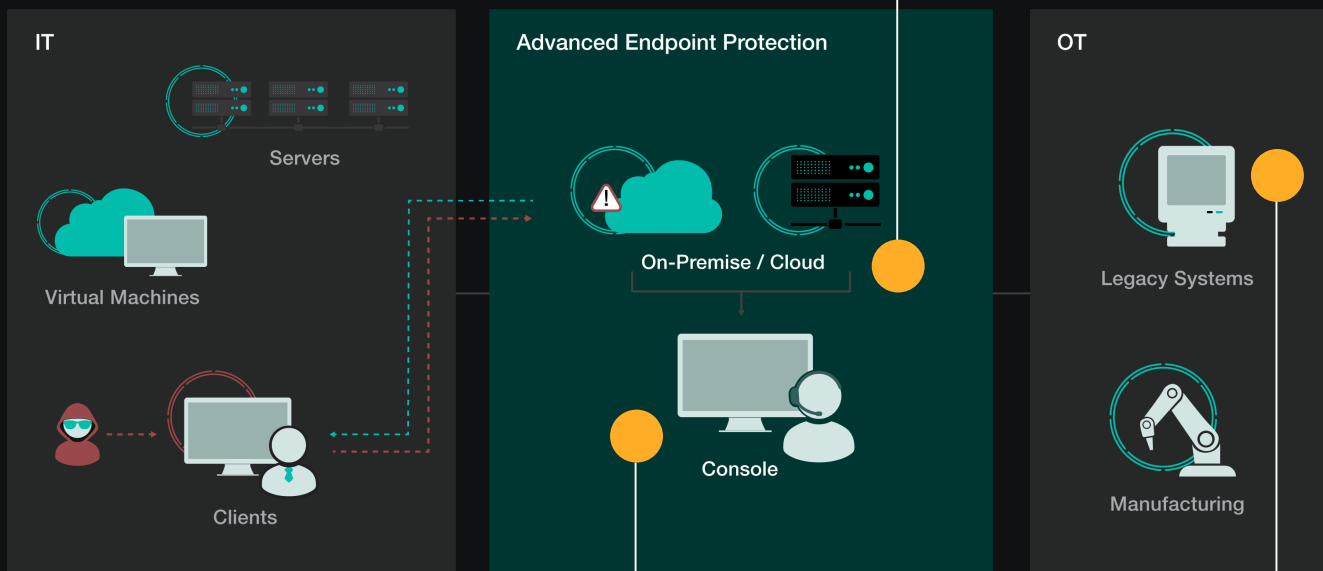
How resilient is your endpoint protection in day-to-day operations? Devices change, users work remotely, and configurations vary. Security solutions are in place—yet gaps still arise due to inconsistent policies, incomplete coverage, delayed responses, or a failure to classify incidents. The risk lies less in a lack of tools than in the complexity of operations.

The Protection

Advanced Endpoint Protection addresses precisely this operational reality: Clients, servers, and OT devices are continuously monitored, security statuses are checked, and suspicious activities are quickly detected and contained. Automated responses immediately mitigate risks while security experts assess and prioritize incidents. This ensures reliable protection.

ON PREMISE OR CLOUD

The central console can be deployed both in the cloud and on-premises in an air-gapped environment. This ensures that even the most stringent security requirements for critical infrastructure can be met.



CENTRAL CONSOLE

All systems are integrated into a single central console. This provides a comprehensive and intuitive overview, allowing settings to be configured as logically and efficiently as possible.

OPERATING SYSTEM SUPPORT

Extensive support for various operating systems. In addition to macOS, Windows, and Linux, older versions such as Windows XP, Windows Vista, and Windows Server 2003 are also supported.







Benefits

What sets us apart as a security partner.

HUMAN EDGE	OT-SPECIALISATION	EFFICIENCY AND TRANSPARENCY
<p>CLUE combines technology with direct access to experts. Thanks to our extensive project experience, we can implement an EDR without disrupting systems or processes.</p> <ul style="list-style-type: none"> • Proven detection policies minimize false positives. • Flexible integration into your existing tool landscape. • Clear playbooks ensure smooth operations. • Regular reviews optimize detection quality. 	<p>OT environments require a specialized understanding of security: production processes and control systems must not be compromised. CLUE offers this expertise.</p> <ul style="list-style-type: none"> • Successful project implementation in manufacturing and critical infrastructure environments. • A unified agent for IT/OT integration. • Collaboration with leading industry experts. • Rapid and close collaboration with the manufacturer. 	<p>CLUE provides largely autonomous, AI-powered threat detection and response, as well as complete visibility across the entire attack chain.</p> <ul style="list-style-type: none"> • Correlations are automatically identified and analyze • Threats can be resolved in real time • False positives are minimized and the workload is reduced • Transparent AI decisions build trust

Features

The technical elements of our approach.

<p> Visibility</p> <p>The system collects metadata, enabling complex and comprehensive analyses across all systems.</p>	<p> Network Discovery</p> <p>Identifies unknown systems on the network and shows where security can be enhanced.</p>	<p> Storyline</p> <p>The collected data is analyzed to reveal the dependencies and connections between processes.</p>
<p> USB-Control</p> <p>Granularly allow and block USB connections on the system as an additional security measure.</p>	<p> Automatic Response</p> <p>Enables a rapid response to attacks and subsequent human analysis without time pressure.</p>	<p> One-Click Attack Rollback</p> <p>Reset the system to its state prior to the attack with the click of a button.</p>

<p>Threats Target Endpoints.</p>	<p>So Should Your Defense.</p>	<p>Advanced Endpoint Protection, always one step ahead.</p>
---	---------------------------------------	--