CLUE
CYBER SECURE

# Advanced Endpoint Protection

## Die Angriffsfläche

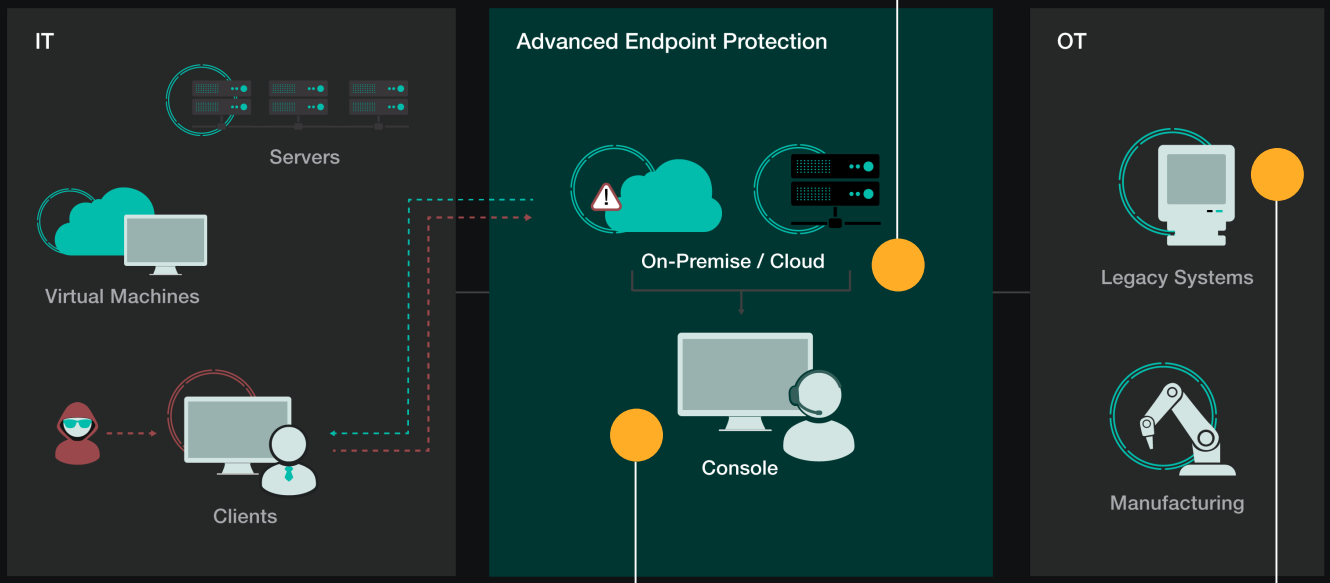
Wie belastbar ist der Schutz Ihrer Endpoints im Alltag? Geräte ändern sich, Nutzer arbeiten mobil, Konfigurationen variieren. Sicherheitslösungen sind vorhanden – dennoch entstehen Lücken durch inkonsistente Richtlinien, unvollständige Abdeckung, verzögerte Reaktionen oder fehlende Einordnung von Vorfällen. Das Risiko liegt weniger im fehlenden Tooling als in der Komplexität des Betriebs.

## Die Absicherung

Advanced Endpoint Protection adressiert genau diese operative Realität: Clients, Server und OT-Devices werden kontinuierlich überwacht, Sicherheitszustände geprüft und verdächtige Aktivitäten schnell erkannt und eingegrenzt. Automatisierte Reaktionen senken Risiken sofort, während Security-Experten Vorfälle einordnen und priorisieren. So entsteht verlässlicher Schutz.

### ON PREMISE ODER CLOUD

Die zentrale Konsole kann sowohl in der Cloud als auch Air-Gapped On-Premise eingerichtet werden. Somit können auch höchste Sicherheitsanforderungen von kritischer Infrastruktur erfüllt werden.




### ZENTRALE KONSOLE

Alle Systeme sind zentral in einer Konsole integriert. Dies ermöglicht eine zentrale und intuitive Übersicht damit Einstellungen möglichst logisch und effizient eingerichtet werden können.

### OPERATING SYSTEM SUPPORT

Umfangreiche Unterstützung von verschiedenen Operating Systems. Neben MacOS, Windows und Linux werden auch alte Versionen wie Windows XP, Windows Vista und Windows Server 2003 unterstützt.

CLUE
CYBER SECURE

# Benefits

Was uns als Security-Partner auszeichnet.

## HUMAN EDGE

CLUE kombiniert Technologie mit direktem Expertenzugang. Durch umfangreiche Projekterfahrung können wir ein EDR einrichten ohne Systeme und Prozesse zu beeinträchtigen.

- Erprobte Detection Policies minimieren False Positives
- Flexible Integration in die bestehende Tool-Landschaft
- Klare Playbooks sichern einen reibungslosen Betrieb
- Relemässige Reviews optimieren die Erkennungsqualität

## OT-SPEZIALISIERUNG

OT-Umgebungen erfordern ein besonderes Sicherheitsverständnis: Produktionsprozesse und Steuerungssysteme dürfen nicht beeinträchtigt werden. CLUE bringt diese Erfahrung mit.

- Erfolgreiche Projektumsetzung in Fertigungen und kritischen Infrastrukturen
- Einheitlicher Agent für IT/OT
- Zusammenarbeit mit führenden Branchenexperten
- Schnelle und enge Zusammenarbeit mit dem Hersteller

## EFFIZIENZ UND TRANSPARENZ

CLUE liefert eine weitgehend autonome, KI-gestützte Bedrohungserkennung und -reaktion sowie eine lückenlose Transparenz über die gesamte Angriffskette.

- Zusammenhänge werden automatisiert erkannt und analysiert
- Bedrohungen können in Echtzeit behoben werden
- Fehlalarme werden minimiert und die Arbeitslast reduziert
- Nachvollziehbare KI-Entscheide schaffen Vertrauen

# Features

Die technischen Elemente unseres Ansatzes.

### Visibility

Es werden Metadaten von dem System gesammelt und damit werden komplexe und globale Analysen über alle Systeme ermöglicht.

### Network Discovery

Findet unbekannte Systeme im Netzwerk und zeigt wo der Schutz noch erweitert werden kann.

### Storyline

Die gesammelten Daten werden aufbereitet und zeigen die Abhängigkeiten und Verbindungen zwischen Prozessen auf.

### USB-Control

Granulares Erlauben und Blockieren von USB Verbindungen auf dem System als zusätzliche Härtemassnahme

### Automatic Response

Ermöglicht eine schnelle Antwort auf Angriffe und eine nachträgliche menschliche Analyse ohne Zeitdruck

### One-Click Attack Rollback

Durch einen Klick das System auf den Zustand vor dem Angriff zurücksetzen.

**Endpoints schützen.** **Angriffe stoppen.** **Mit Advanced Endpoint Protection von CLUE.**

+41 44 667 77 66 | info@clue.ch | clue.ch

04.2026