Endpoint Detection & Response (EDR)

Endgeräte sind primäre Angriffsziele in Unternehmen. Sie sind vielfältig und weichen häufig von der Standardkonfiguration ab, da sie oftmals ungesicherten Netzwerken ausgesetzt sind.

Über 70% der Angriffe auf Endgeräte verwenden fortschrittliche Techniken, die nicht mehr durch den Virenschutz erkannt und geschützt werden.

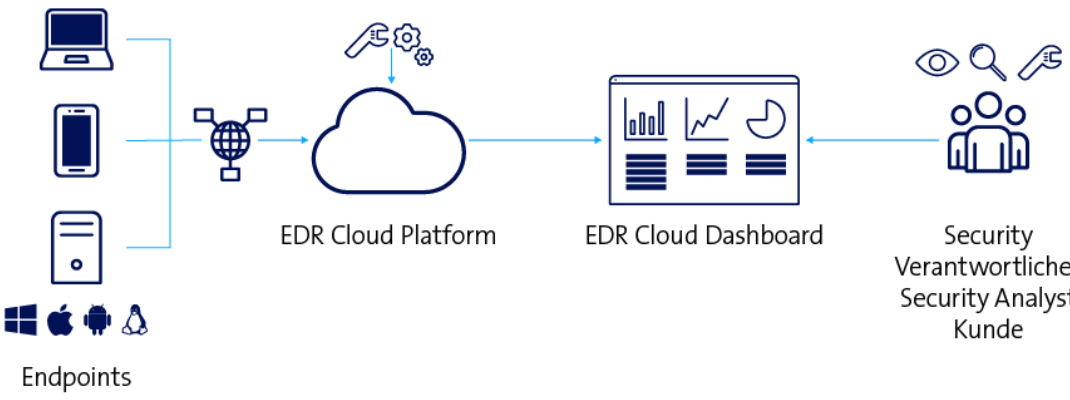
Was ist Endpoint Detection & Response (EDR)?

Endpoint Detection & Response überwacht Endgeräte, sogenannte Endpoints, in Unternehmensnetzwerken, mittels Sicherheitsanalysen und Vorfallsreaktionen. Die Lösung bietet eine End-to-End-Sichtbarkeit über die Aktivität jedes Endpoints (Client, Server, Mobile) in der Unternehmensinfrastruktur. Der Service wird von einem zentralen Dashboard aus verwaltet und liefert so wertvolle Erkenntnisse für die IT-Sicherheit in Ihrem Unternehmen.

Ihr Nutzen mit Endpoint Detection & Response

- End-to-End Sichtbarkeit über alle Endpoint-Aktivitäten (Client, Server, Mobile) in ihrem Netzwerk
- Automatisierte Untersuchung und Behebung von Endpoint Security Alerts, um das Volumen der generierten Alerts erheblich zu reduzieren und so das Security Betriebsteam zu entlasten.
- Managed Service – Sie profitieren von ausgewiesener, langjähriger Erfahrung unserer Experten.
- Schutz vor komplexen, dateilosen Angriffen wie Malware, bösartige Software und Zero-Day-Exploits
- Advanced Threat Hunting sowie Remote Remedation Capabilities in Echtzeit, dank Dashboard.
- Mit weiteren Swisscom Services kombinierbar (z.B. SOC as a Service, CSIRT as a Service)

Die Lösung im Überblick



swisscom

Facts & Figures

Basisleistungen	Der Service basiert auf einem **Partner Cloud Service**
	Cloud Tenant Management wird durch den Kunden erbracht
	Endpoint Detection & Response ermöglicht eine End-to-End-Sichtbarkeit über alle Endpoints wie Client, Server oder Mobile hinweg, um fortgeschrittene Attacken zu verhindern.
	Mit **Endpoint Protection** werden die Endpoints geschützt, um Malware, Attacken und bösartige Aktivitäten zu verhindern.
	Das **EDR Cloud Dashboard** bietet eine Übersicht der entstandenen Alerts und Advanced Threat Hunting sowie Remote Remedation Capabilities für die Endpoints.
	Projektleistungen für das Onboarding des Service
	Die **monatliche Verrechnung** erfolgt anhand der Preisklasse nach Anzahl User und Server von S bis XL. Die benötigten Lizenzen sind nicht Bestandteil des Service.
Optionale Leistungen	**Consulting, Customizing und Changes** (nach Aufwand)
	Mit **Endpoint Threat & Vulnerability Management** werden Schwachstellen und Fehlkonfigurationen in Echtzeit auf den Endpoints entdeckt, ohne dass periodische Scans nötig sind.
Zusatzservices	**Cloud Service Provider (CSP)** Lizenzierung durch Swisscom
	Mit **Threat Detection & Response – SOC as a Service** erhalten Sie via Dashboard einen Überblick über potentielle und bestätigte Sicherheitsvorfälle aus definierten Log-Daten Ihrer Unternehmung sowie Analysen mit konkreten Handlungsempfehlungen. Auf kritische Security Incidents reagieren Sie selbständig.
	Mit **Threat Detection & Response – CSIRT as a Service** ziehen Sie Experten von Swisscom zur Analyse und Bewältigung von Vorfällen bei. Wir leiten den Security Incident Management Prozess Remote oder bei Ihnen vor Ort, unterstützen Sie bei der Beweissicherung sowie der Kommunikation zu Kunden und Partnern.
	Cloud Tenant Management durch Swisscom
	Smart, Connected oder Rich Workplace: vom digital smarten Arbeitsplatz, den die Benutzer selbständig ohne IT einrichten können, bis hin zu einem ganzheitlich gemanagten Client-Arbeitsplatz, inklusive Software Verteilung, Software-Paketierung, Asset-Management und Good Practice Security.

Erfahren Sie mehr zu Endpoint Detection & Response unter www.swisscom.ch/edr

Swisscom (Schweiz) AG Enterprise Customers, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise