



SO VIEL SECURITY-AUTOMATISIERUNG  
IN NUR EINEM TOOL

DA WERDEN IHRE IT-MITARBEITER  
ABER  MACHEN!

Mit Enginsight erhalten Sie ein  
hoch skalierungsfähiges Produkt,  
Made in Germany.  
Mit deutschem Support  
direkt zum Hersteller.

[www.enginsight.de](http://www.enginsight.de)

 **ENGINSIGHT**



# GEMEINSAM SICHERHEIT SCHAFFEN

Mit der Erfahrung im Rücken und den alltäglichen Herausforderungen in der IT-Abteilung eines Mittelständlers vor der Brust entstand 2017 gemeinsam mit Eric Range (CTO) die Idee zu Enginsight.

**Unsere Vision:** Mit einer umfassenden Softwarelösung Übersicht herzustellen, um den sicheren Betrieb der IT-Infrastruktur zu gewährleisten.

**Der Fokus:** Für KMUs handhabbar und bezahlbar zu bleiben.

Im engen Austausch mit unseren Endkunden und Partnern, deren Anregungen uns antreiben, haben wir mit Enginsight eine umfassende Security-Software geschaffen. Heute bietet Enginsight noch mehr, als wir uns damals für unsere Arbeit gewünscht hatten.

In einer agilen und motivierten Atmosphäre entwickeln wir in Jena Enginsight immer weiter. Wir freuen uns darauf, von Ihren Erfahrungen mit Enginsight zu lernen und Ihnen neue Perspektiven in der Administration und Absicherung von IT-Umgebung zu eröffnen.

Ihr Mario Jandeck

<p><b>MARIO JANDECK</b> Position: CEO  mario.jandeck@enginsight.com</p>	
---	---

## INHALT

Enginsight .....	3
Enginsight-Prozess .....	7
Feature-Übersicht .....	8
IT-Architektur .....	9



# GANZHEITLICHE SICHERHEIT MIT ENGIN SIGHT

## So schnell und einfach war Security noch nie

Wir kennen kein Tool, welches (verglichen mit dem Funktionsumfang) so schnell einsatzbereit ist. Enginsight analysiert ganz automatisch Ihre gesamte IT. So erfahren Sie innerhalb weniger Minuten, wie es um die Sicherheit Ihres Unternehmens steht.

**Unser Versprechen:** Keine Konfigurationen, kein langwieriges Onboarding.

In 1-5 Tagen (je nach Unternehmensgröße) kennen Sie den Sicherheitszustand und haben eine dauerhafte Live-Überwachung Ihrer Systeme integriert.

## Sicherheit beginnt bei uns selbst - Enginsight ist Security by Design

Das schafft eine robuste IT-Sicherheits-Architektur, wodurch auch Sie als Kunde Ihre Angriffsflächen essenziell reduzieren.

**Unser Tipp:** Prüfen Sie dies bei jedem Tool, welches Sie in Ihrem Unternehmen einsetzen.

## Modernste Architektur spart Hardware & Geld

Enginsight wurde mithilfe modernster Technologien und Programmiersprachen entwickelt. Das schafft Ausfallsicherheit und schont Ihre Hardware und zu guter Letzt Ihren Geldbeutel.

**Unser Versprechen:** Enginsight ist eine der stabilsten und ressourcenschonendsten Security-Lösungen am Markt.

## Mandantenfähig

Enginsight bietet die idealen technischen Voraussetzungen für die tägliche Arbeit als IT-Dienstleister. Verwalten Sie Ihre Kunden und rechnen Sie über Ihren eigenen Partner-Account ab, ohne dass Ihr Kunde davon etwas mitbekommt.



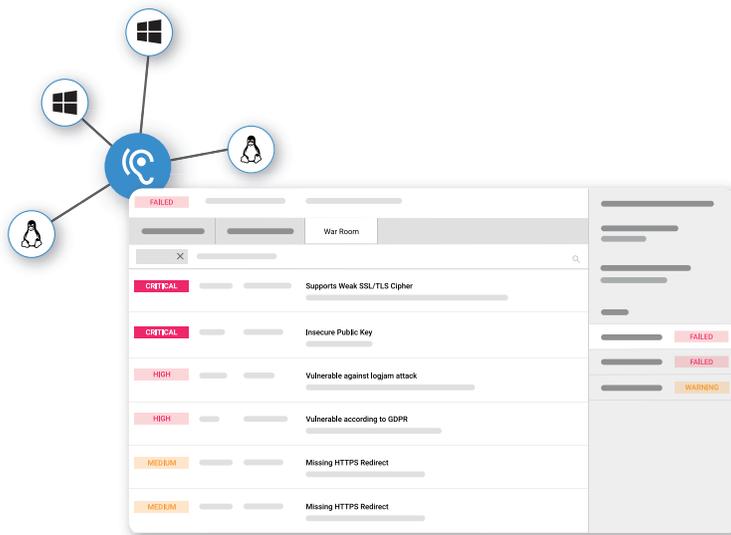
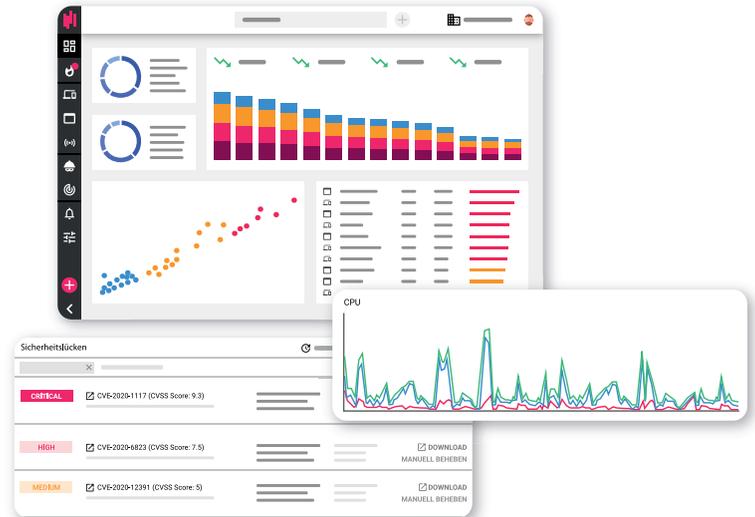


### IT-Sicherheit ist keine Raketenwissenschaft

Machen Sie es sich nicht unnötig kompliziert. Denn Enginsight gibt Ihnen die Funktionen und Informationen an die Hand, mit denen Sie einfach und nachvollziehbar zu einer sicheren Unternehmens-IT gelangen.

### Das Fundament einer weitsichtigen IT-Sicherheits-Strategie

Verabschieden Sie sich von Insellösungen und einem unübersichtlichen Toolzoo. Das durchdachte Funktionsset liefert Ihnen eine umfassende Lösung, um Ihre IT auf einen sicheren Boden zu stellen.



### Richtlinien einhalten und Rechtssicherheit herstellen

Mit Enginsight gelingt Ihnen eine effektive Umsetzung von Richtlinien und Zertifizierungen (z.B. ISO 27001). Sie stellen darüber hinaus sicher, dass Sie gesetzliche Vorgaben (z.B. DSGVO) einhalten.

### Automatisierung entlastet IT-Abteilung

Zunehmende Vernetzung und Komplexität bringen IT-Abteilungen an ihre Grenzen. Die vielfältigen Automatisierungsmöglichkeiten geben Ihrer IT-Abteilung wieder Luft zum Atmen.

### Ihre Erfahrung zählt

Wir hören auf unsere Kunden und ihre Wünsche und richten uns im agilen Entwicklungsprozess nach Ihnen. Lassen Sie uns gemeinsam Ihren Alltag vereinfachen und Enginsight immer besser machen.

„Wir hatten mit einer fehlenden Transparenz des Sicherheitszustandes unserer IT zu kämpfen. Mit Enginsight haben wir eine kleine Lampe aufgestellt, die Licht ins Dunkle bringt. Je weiter wir Enginsight ausrollen und je mehr Assets wir in die Überwachung integrieren, desto heller sehen wir. Besonders schätzen wir die gute Zusammenarbeit. Die Mitarbeiter von Enginsight haben für unsere Anregungen stets ein offenes Ohr und können durch ihre agile Arbeitsweise auch schnell auf Wünsche reagieren. Deshalb haben wir Enginsight bereits unserem IT-Berater weiterempfohlen.“

Christian Eckerle, Head of IT bei HanseYachts AG

„Schon seit 4-5 Jahren denken wir darüber nach, einen Managed Security Service anzubieten, der nicht nur Einmalbetrachtungs-Szenarien abbildet, sondern eine dauerhafte Überwachung ermöglicht. Ursprünglich wollten wir eine eigene Software entwickeln. Dabei mussten wir aber feststellen, dass der Aufwand dafür einfach zu groß ist. Das war der Grund, warum wir bei Enginsight gelandet sind. Heute können wir unsere Pläne realisieren und haben mit Enginsight als MSSP gehen gelernt. Um die volle Kontrolle zu behalten, nutzen wir die Möglichkeit, die Enginsight-Applikation selbst auf unseren Servern zu hosten. So können wir unseren Kunden anbieten, vorbeizukommen, um ihre Daten zu streicheln.“

Ralf Schwarzmeier, Geschäftsführer bei mars solutions



# WAS IST, WENN DIE FIREWALL VERSAGT?

## Enginsight verfolgt einen dezentralen Ansatz für maximale Flexibilität.

- ✓ **Kein Bottleneck**, daher problemlos skalierbar
- ✓ **Sensoren** verteilt über die gesamte IT-Infrastruktur
- ✓ **Sofort einsatzbereit**, ohne Konfigurationen

## Agents direkt auf all Ihren Servern und Clients

- ✓ **100% valider Schwachstellenscan**: Dank vollständiger Informationen über das System liefert der Pulsar-Agent CVE-Scans ohne False-Positives.
- ✓ **Hostbasierte Intrusion Detection und Prevention**: Auch Angriffe, die bereits an der Firewall vorbeikommen sind, werden erkannt und können blockiert werden.
- ✓ **Mikrosegmentierung & hostbasiertes Blocking**: Managen Sie die Netzwerkverbindung auch innerhalb von Netzwerksegmenten durch passgenaue Regelwerke für Server und Clients.
- ✓ **Leistungsfähiges Monitoring**: Überwachen Sie beliebige Leistungsdaten, Software, Prozesse und Ports.
- ✓ **Überwachung** von Servern und Clients außerhalb des Firmennetzwerks, z.B. im Homeoffice oder Datacenter.

## Security-Audits der gesamten IT-Umgebung

- ✓ **Automatische Inventarisierung** der gesamten IT zur Verhinderung von Schatten IT
- ✓ **Automatisierter Penetrationstest** aller detektierten Assets
- ✓ **Wiederkehrende Ausführung** mit vergleichbaren Ergebnissen



**Pulsar-Agents** auf allen Servern und Clients für die Live-Überwachung von innen



**Watchdog** zur IP-Inventarisierung sowie Agentless-Monitoring Ihrer IT-Peripherie



**Hacktor** zur Durchführung automatisierter Penetrationstests



**Observer** zur Live-Überwachung Ihrer Webseiten und Webanwendungen



**100 % validierte Analysen** und ein  
**hoher Automatisierungsgrad** schaffen  
**volle Transparenz** zum Sicherheitszustand  
Ihres Unternehmens.

Dies ermöglicht es Ihnen,  
mit **wenigen IT-Mitarbeitern** die **volle Kontrolle**  
über eine **immer komplexer werdende IT-Infrastruktur**  
zu behalten.

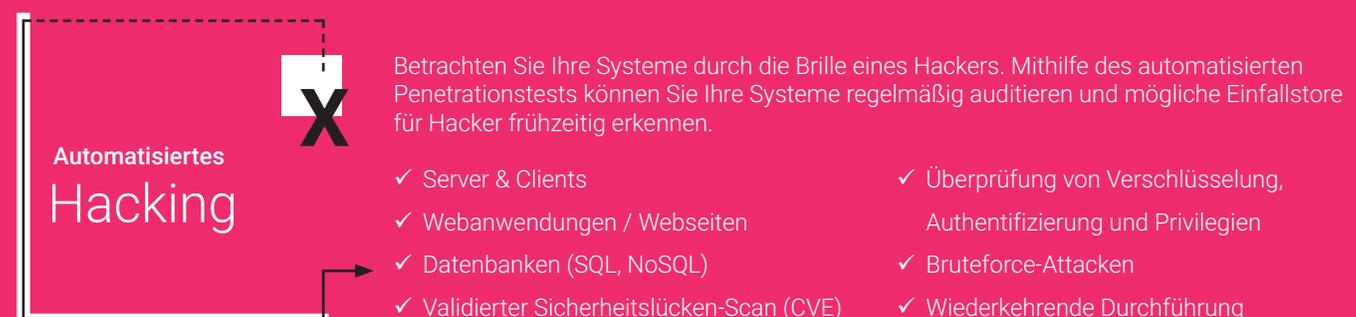
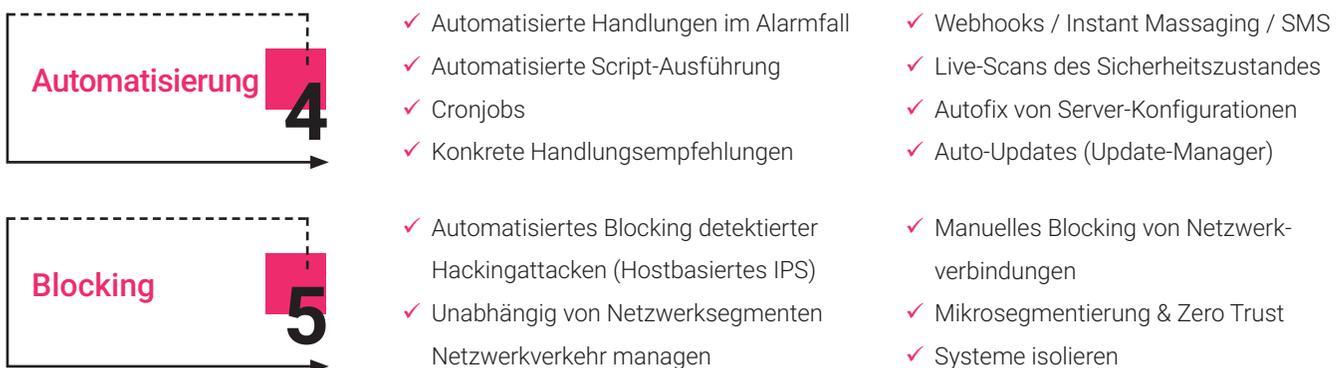
Enginsight hilft Ihnen auch  
bei Ihrer ISO-Zertifizierung.  
Fragen Sie uns gerne wie...



## ENGINSIGHT IST IHR SECURITY-PROZESS



## AKTIV WERDEN





# FUNKTIONS-ÜBERSICHT DER ENGIN SIGHT SOFTWARE

**Vier Softwaremodule** verteilen Sie in Ihrer IT-Infrastruktur. Als Sensoren sammeln Sie alle Daten und senden sie an die Enginsight Applikation, die Sie über den Browser aufrufen.

**DAS IST UNS WICHTIG:** Zur Installation der Softwaremodule und zum Start der Analyse brauchen Sie lediglich ein Skript ausführen und keine manuellen Konfigurationen vornehmen.

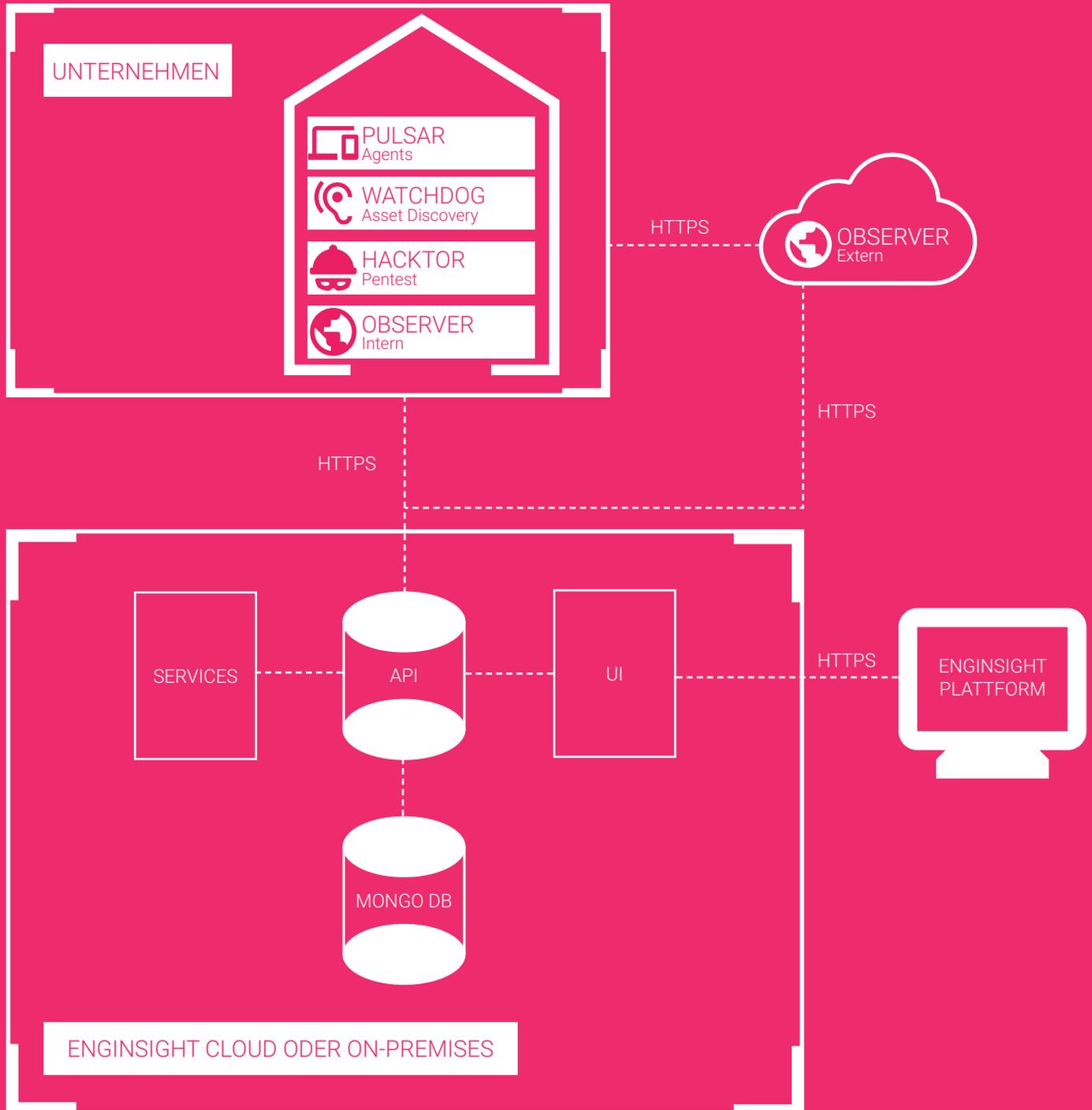
Pulsar-Agent	<p>Der Pulsar-Agent wird auf all Ihren Servern und Clients (Linux &amp; Windows) installiert, um die Systeme dauerhaft von innen zu überwachen.</p> <p><b>100% VALIDIER CVE-SCAN - KEINE FALSE-POSITIVES!</b></p> <p>Schwachstellen-Scanner (CVE)   Patchmanagement   Analyse des Netzwerkverkehrs (Deep Packet Inspection)   Dynamisches Blocking von Netzwerkattacken (IPS)   Manuelles Blocking &amp; Mikrosegmentierung   Eventlog-Analysen   IT-Monitoring   Anomalieerkennung durch Machine Learning   Prozessüberwachung   Softwareinventarisierung   Portüberwachung   Konfigurationsmanagement</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Übersichtliche Dashboards</li> <li><input checked="" type="checkbox"/> Operation Centers</li> <li><input checked="" type="checkbox"/> Risiko-Scores</li> <li><input checked="" type="checkbox"/> Risiko-Priorisierung</li> <li><input checked="" type="checkbox"/> Handlungsempfehlungen</li> <li><input checked="" type="checkbox"/> Professionelles Alarmsystem</li> </ul>
Observer	<p>Der Observer untersucht aus dem Inter- oder Intranet Ihre Webseiten und Webanwendungen auf Verfügbarkeit und Sicherheit.</p> <p>Schwachstellen-Scanner (CVE)   Uptime Monitor   SSL/TLS Check   DNS-Monitoring   Footprinting der Anwendungsumgebung   Portscan   HTTP-Header Analyse   Weiterleitungs-Monitoring</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Automatisierbare Handlungen im Alarmfall</li> <li><input checked="" type="checkbox"/> Globale Volltext-Suche</li> <li><input checked="" type="checkbox"/> Webhooks</li> </ul>
Watchdog	<p>Der Watchdog scannt ganze Netzwerke und inventarisiert automatisch alle im Netzwerk befindlichen Geräte. Gleichzeitig stellt er das agentless Monitoring bereit.</p> <p>Netzwerk-Scan   Inventarisierung   Health-Checks (Ping, Port)   SNMP</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> PDF-Berichte</li> <li><input checked="" type="checkbox"/> API-Zugriff</li> <li><input checked="" type="checkbox"/> Benutzer-Rollen</li> <li><input checked="" type="checkbox"/> Benutzer-Gruppen</li> </ul>
Hacktor	<p>Der Hacktor führt einmalig oder regelmäßig automatisierte Penetrationstests auf ganze Infrastrukturen, einzelne IP-Adressen oder Webseiten aus. Dazu muss er im Intranet oder Internet platziert werden, sodass er die Zielsysteme erreichen kann.</p> <p>Information Gathering (Footprinting)   Schwachstellen-Scan (CVE)   Bruteforce   Discovery (Checks auf Konfigurationenmängel, z.B. Verschlüsselung, Authentifizierung und Privilegien)</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Unlimited User</li> <li><input checked="" type="checkbox"/> Mandanten-Fähigkeit</li> </ul> <p><a href="https://enginsight.com/docs/">enginsight.com/docs/</a></p>

**ENGINSIGHT IST VERFÜGBAR ALS SOFTWARE AS A SERVICE (CLOUD) UND ON-PREMISES.**

Der schnellste Einstieg in die Welt von Enginsight gelingt über die Cloud. Aber auch eine eigene On-Premises Installation über Docker ist in wenigen Augenblicken erledigt.



# SOFTWARE ARCHITEKTUR SECURITY BY DESIGN





**ENGINSIGHT GmbH**  
Hans-Knöll-Straße 6  
07745 Jena

+49 (0)3641 271 49 66  
hello@enginsight.com  
enginsight.com

 **ENGINSIGHT**