# m2v IT-Security

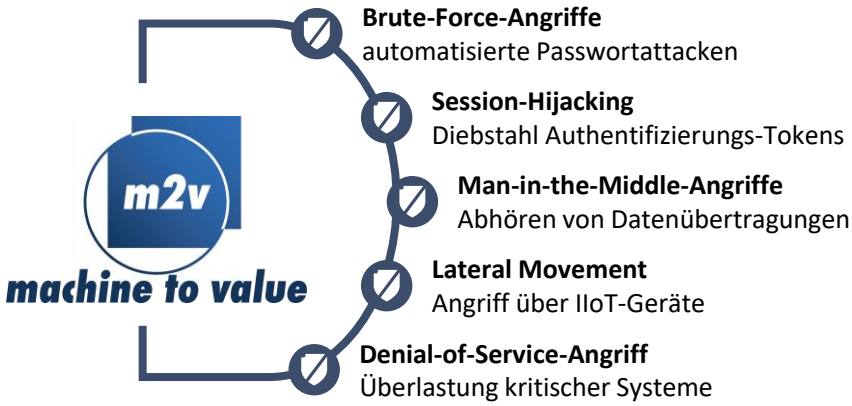
Modernste IT-Sicherheitsarchitekturen ganzheitlich umgesetzt.

*Eine Vorstellung der **eurogard GmbH***
*IT-Security Systeme und Maßnahmen*

# m2v Plattform

## Modernste Sicherheitsarchitektur gegen Cyberbedrohungen

Die **m2v Plattform** bietet ein durchdachtes Sicherheitskonzept, das speziell auf die Herausforderungen moderner IIoT- und Remote-Access-Umgebungen ausgelegt ist. Durch den **Defense-in-Depth-Ansatz**, eine **granulare Zugriffskontrolle** und **moderne Verschlüsselungstechniken** erfüllt sie höchste Standards in Datenschutz, IT-Sicherheit und Compliance. Cyberbedrohungen entwickeln sich stetig weiter - die eurogard Systemlandschaft daher auch. Wir arbeiten kontinuierlich an technischen Gegenmaßnahmen für verschiedene Bedrohungen.



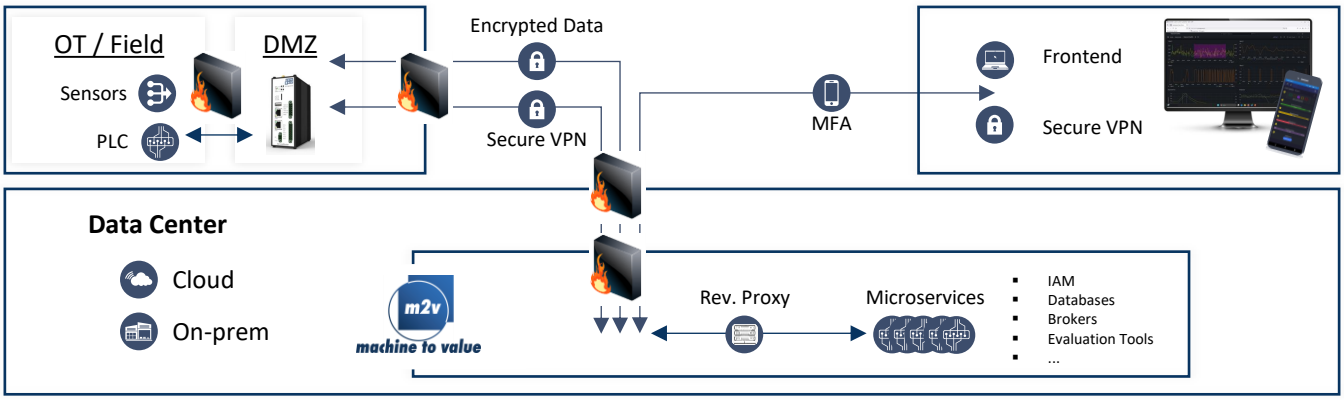

- Egal, ob in einer zertifizierten Cloud-Umgebung in Deutschland und Europa oder on-premises in der eigenen IT-Infrastruktur – die grundlegende Sicherheitsarchitektur bleibt stets gleich.

- Mehrstufige Schutzmechanismen in Technologie, Infrastruktur und Zugriffskontrolle stellen sicher, dass sensible Daten zu jedem Zeitpunkt geschützt bleiben.

# m2v Plattform

## Modernste Sicherheitsarchitektur für Remote Access und IIoT

Die m2v Plattform basiert auf einer **modularen, mehrschichtigen Sicherheitsarchitektur**, die sich flexibel in verschiedene IT-Umgebungen integrieren lässt. Sie kann **in einer zertifizierten Cloud-Umgebung, on-premises oder über einen eigenen Cloud-Dienstleister** betrieben werden – der konzeptionelle Sicherheitsansatz bleibt dabei identisch.




**Technische Sicherheitsarchitektur:** Die technische Sicherheitsarchitektur sichert sämtliche Systemkomponenten und Kommunikationswege durch den gezielten Einsatz modernster Technologien und Strategien ab.

- **Firewall:** Kontrolle und Filterung des ein- und ausgehenden Datenverkehrs zur Abwehr unautorisierter Zugriffe.
- **Verschlüsselter Datenverkehr:** Einsatz modernster Verschlüsselungsverfahren zum Schutz aller Kommunikationskanäle.
- **Netzwerkisolation & Zugriffskontrolle:** Strikte Trennung und Beschränkung der Netzwerkzugriffe zur Minimierung potenzieller Angriffsflächen.
- **Docker-Netzwerke mit Segmentierung:** Isolierung von Container-Diensten durch gezielte Netzwerksegmentierung.
- **Container-Härtung:** Anwendung von Best-Practice-Sicherheitsmaßnahmen zur Reduktion von Schwachstellen in den Docker-Containern.
- **Trennung von IT und OT durch Edge Devices:** Eine zusätzliche Schutzebene direkt an der Quelle der Daten wird durch das **ER1601 Edge Device** geschaffen, mit integrierter intelligenter Firewall und strikter Netzwerktrennung.

**Zugriffsschicht:** Die Zugriffsschicht implementiert mehrstufige Authentifizierungs- und Autorisierungsverfahren, um sicherzustellen, dass ausschließlich berechtigte Nutzer und Systeme auf die Plattform zugreifen können.

- **Zwei-Faktor-Authentifizierung (2FA):** Erhöhter Schutz durch den Einsatz zusätzlicher Authentifizierungsfaktoren.
- **Session-Tokens:** Kurzlebige Authentifizierungstokens zur Minimierung des Risikos von Session-Hijacking.
- **Admin-Zugriffe über IP-Whitelist:** Beschränkung administrativer Zugriffe ausschließlich auf vordefinierte, vertrauenswürdige IP-Adressen.
- **JWT-Signatur:** Sicherstellung der Integrität und Authentizität von JSON Web Tokens.
- **Web-Security-Header:** Einsatz von X-Frame-Options, Content-Security-Policy, X-XSS-Protection und HTTP Strict Transport Security (HSTS) zur Abwehr von webbasierten Angriffen.
- **Brute-Force Detection:** Frühzeitige Erkennung und Blockierung von unautorisierten Zugriffen durch automatisierte Überwachung.
- **Edge Security:** Eine lokale Authentifizierungsebene kombiniert mit physischen Schlüsselschaltern sorgt für volle Kontrolle vor Ort. Die Kommunikation mit der Cloud erfolgt verschlüsselt und zertifikatsbasiert.

# m2v Plattform & Edge Security

## Industrial Edge Computing Gateway als Sicherheitsverstärker

Die zentrale Absicherung von Cloud- und Netzwerkressourcen reicht nicht aus, wenn Angreifer ungesicherte **Edge Devices** als Einfallstor nutzen können. In der industriellen Umgebung sind **Maschinen, Sensoren und Produktionsnetzwerke** zunehmend über IIoT-Plattformen vernetzt, wodurch zusätzliche Angriffspunkte entstehen. Ein sicheres Edge-Computing-Modell ist daher essenziell, um industrielle Netzwerke zuverlässig gegen Manipulation, Datenlecks und Angriffe abzusichern. Daher setzt eurogard auf eine Kombination aus:

- Gehärteten Edge Devices mit zertifikatsbasierter Kommunikation
- Fleet-Management für schnelles Patch- und Update-Management
- Segmentierter Netzwerksicherheit mit VLANs und Firewalls
- Isolierung von IT- & OT-Systemen zur Vermeidung v. Bedrohungsausbreitung

Der **ER1601** ist ein hochsicheres Edge Device, das **Datenverarbeitung direkt an der Quelle** ermöglicht und dabei höchste IT-Sicherheitsstandards erfüllt Durch seine **stabile Cloud-Verbindung,** wahlweise über Ethernet, Wifi oder Mobilfunk**, hardwaregestützte Sicherheitsmechanismen, modulare Software-Integration** und konsequentes **Patch-Management** integriert er sich nahtlos in die vorhandene Sicherheitsarchitektur der m2v-Plattform.

- Härtung der Edge Devices
- Strikte Internet/OT-Trennung für maximale Netzwerksicherheit
- Zertifikatsbasierte, verschlüsselte Kommunikation auf allen Kanälen
- Interne Firewall & Netzwerktrennung mit VLANs
- Fleet-Management für schnelles Patch-Management und Updates
- Physikalische und virtuelle Steuerung kritischer Dienste
- Isolation von VPN- und MQTT-Diensten innerhalb der Cloud

## m2v Plattform

# Zusätzliche Sicherheitsmaßnahmen – Kontinuierliche Verbesserung für nachhaltige IT-Sicherheit

IT-Sicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. eurogard verfolgt daher einen **dynamischen Sicherheitsansatz**, der sich fortlaufend an neue Bedrohungslagen, technologische Entwicklungen und regulatorische Anforderungen anpasst. Neben bewährten Schutzmechanismen setzt eurogard auf eine **kontinuierliche Sicherheitsverbesserung**, um Risiken frühzeitig zu erkennen, zu analysieren und zu minimieren. Dies umfasst **regelmäßige Prüfungen, Audits** und **Feedbackprozesse**, um die Sicherheitsarchitektur stetig zu optimieren. Ergänzende Sicherheitsmechanismen zur Stabilität des Gesamtsystems sind:

- **Verschlüsselte Backups:** Regelmäßige, verschlüsselte Datensicherungen gewährleisten die Integrität und Wiederherstellbarkeit sensibler Informationen.
- **Patch-Management:** Zeitnahe Implementierung von Sicherheitsupdates und Patches zur Schließung bekannter Schwachstellen.
- **Monitoring und Logging:** Permanente Überwachung und Protokollierung aller Systemaktivitäten zur schnellen Identifikation und Reaktion auf sicherheitsrelevante Ereignisse.
- **Zero Trust Ansatz:** Jeder Zugriff wird als potenziell unsicher betrachtet und muss daher durch strenge Authentifizierungs- und Autorisierungsmaßnahmen validiert werden.
- **Secure-by-Design:** Sicherheitsaspekte werden von der Entwicklungsphase an integriert, um höchste Sicherheitsstandards zu gewährleisten.
- **IEC62443 Zertifizierung in progress:** Die Umsetzung der Anforderungen der IEC62443 wird kontinuierlich vorangetrieben, um zukünftige Zertifizierungsstandards zu erfüllen.

# m2v Plattform

## Sichere und flexible Hosting-Optionen

Die m2v Plattform bietet Unternehmen maximale Entscheidungsfreiheit, indem sie sowohl als Cloud-Lösung als auch on-premises in der eigenen Infrastruktur betrieben werden kann. So können Unternehmen ihre IT-Strategie individuell anpassen und zwischen Skalierbarkeit und voller Datenkontrolle wählen – ohne Kompromisse bei Sicherheit oder Funktionalität.

## On-Premises

Maximale Kontrolle über Ihre Daten. Für Unternehmen mit besonders hohen Datenschutz- und Compliance-Anforderungen bietet die m2v Plattform eine vollständig On-Premises-fähige Architektur.

- **Datenhoheit und Compliance:** Sensible Unternehmensdaten verbleiben vollständig in der eigenen IT-Umgebung, wodurch höchste Datenschutzanforderungen erfüllt werden.
- **Individuelle Sicherheitsrichtlinien:** Unternehmen können ihre eigenen Firewalls, Zugriffskontrollen und Sicherheitsprotokolle anpassen und erweitern.
- **Betrieb in geschlossenen Netzwerken:** Die Plattform kann vollständig isoliert und ohne permanente, externe Internetverbindungen betrieben werden, um maximale Sicherheit zu gewährleisten.
- **Einfache Integration in bestehende IT-Infrastrukturen:** Unterstützung für Virtualisierungsplattformen, Container-Technologien (Docker, Kubernetes) sowie Anpassungen an unternehmenseigene Sicherheitsstandards.
- **Unabhängigkeit von Drittanbietern:** Unternehmen sind nicht an einen bestimmten Cloud-Dienstleister gebunden und können die Plattform autark in ihrer eigenen Infrastruktur betreiben.
- **Flexibles Lizenzmodell:** Auch die On-Premises-Version bietet flexible Zu- und Abschaltung von Maschinen inkl. eines Managed Service mit regelmäßigen Updates und Support durch eurogard.

# m2v Plattform

Sichere und flexible Hosting-Optionen

## Cloud Hosting

Das Hostingkonzept kombiniert eine zertifizierte, regionale Infrastruktur mit umfassenden Sicherheits- und Datenschutzmaßnahmen, um ein höchstmögliches Maß an Datensicherheit zu gewährleisten.

- **Zusammenarbeit mit Spezialisten:** Die Cloud-Sicherheit und das Hostingkonzept beruhen auf dem Betrieb in zertifizierten Rechenzentren in Deutschland und Europa.
- **Zertifizierte Rechenzentren:** Die Cloud-Infrastruktur wird in Rechenzentren betrieben, die nach DIN ISO 27001 zertifiziert sind, wodurch ein adäquates Sicherheitsmanagement und kontinuierliche Verbesserungen garantiert werden.
- **Sicherheitsmanagement und Datenschutz:** Ein robustes Informationssicherheits-Managementsystem (ISMS) stellt die Vertraulichkeit, Integrität und Verfügbarkeit aller Daten sicher.
- **Technisch-organisatorische Maßnahmen (TOMs):** Regelmäßige Überprüfung und Aktualisierung der Sicherheitsmaßnahmen durch externe Datenschutzorganisationen sorgen für eine kontinuierliche Sicherheitsprozessoptimierung.
- **Interne Sicherheitsdokumentation:** Ein internes Statement of Applicability (SoA) dokumentiert sämtliche umgesetzte Maßnahmen gemäß ISO 27001 ohne Ausschlüsse und wird fortlaufend evaluiert.
- **Erfüllung internationaler Standards:** Neben ISO 27001 fließen auch Aspekte von SOC 2 sowie nationale Rahmenwerke wie BSI-Grundschutz, NIST und COBIT in das Sicherheitskonzept ein – aktuelle Entwicklungen im Rahmen der „C5-Äquivalenz-Verordnung“ werden kontinuierlich verfolgt.

**Cloud Hosting & Verantwortlichkeiten**

| Bereich | eurogard | Hosting-Partner |
|---|---|---|
| Physische Sicherheit | ✓ IEC 62443 in progress | ✓ ISO 27001-zertifiziert |
| Virtuelle Infrastruktur | ✓ Docker-Härtung | ✓ Hypervisor-Sicherheit |
| Applikationssicherheit | ✓ Secure-by-Design | / |

## m2v Plattform

Maximale Sicherheit für Ihre IIoT- und Remote-Access-Umgebung

Die **m2v Plattform** demonstriert, wie modernste **IT-Sicherheitsarchitekturen** ganzheitlich umgesetzt werden – von der physischen Serverinfrastruktur und containerisierten Anwendungen bis hin zur **Cloud-Sicherheit, Zugriffskontrolle und Edge Protection**. Für Sie und Ihr Unternehmen bedeutet dies:

**Schutz geschäftskritischer Daten & geistigen Eigentums:** Ihre sensiblen Produktions-, Prozess- und Unternehmensdaten sind durch **mehrschichtige Verschlüsselung, Firewalls und Zugriffskontrollen** vor Cyberangriffen, Industriespionage und Datenverlust geschützt.

**Einhaltung regulatorischer Anforderungen & Compliance:** Die m2v Plattform unterstützt Sie dabei, **gesetzliche Vorgaben und Zertifizierungen** (ISO 27001, IEC 62443 in progress, DSGVO) zu erfüllen.

**Maximale Betriebsstabilität & Vermeidung von Ausfallzeiten:** Dank **automatischer Updates, kontinuierlichem Monitoring und frühzeitiger Bedrohungserkennung** bleibt Ihr IIoT-System jederzeit stabil und einsatzbereit – **Ausfallzeiten und Produktionsunterbrechungen werden minimiert**.

**Stärkung des Kunden- & Marktvertrauens:** Ein **sicheres IT-System** ist heute ein entscheidender Wettbewerbsfaktor. Die m2v Plattform gibt Ihren Kunden, Partnern und Auditoren die Gewissheit, dass ihre Daten und Systeme nach höchsten Standards geschützt sind.

**Sicherheit ist kein einmaliger Zustand – sie ist ein kontinuierlicher Prozess**. eurogard entwickelt seine Lösungen konsequent weiter, um Ihre Infrastruktur jederzeit gegen aktuelle und zukünftige Bedrohungen abzusichern.

**Erfahren Sie mehr darüber, wie Sie Ihre IT- und OT-Sicherheit mit der m2v Plattform optimieren können**. Kontaktieren Sie uns für eine individuelle Beratung.


**Kontakt eurogard**

**Mail:** info@eurogard.de
**Tel.:** +49 2407 95160