





## Case Study

# Policy Manager für weltweite Compliance

## Herausforderung

- Umfassender Schutz aller Clients im Unternehmen weltweit
- Einhaltung der Unternehmens-Policies
- Zero Day-Attacken verhindern einen reibungslosen Betriebsablauf
- Kurze Reaktionszeit im Notfall und schnelle Bereitstellung von Updates

## Lösung

- Umfassende IT-Sicherheitslösung  G DATA Endpoint Protection mit Web-Filter und Policy-Management
- Individuelle Betreuung durch den  G DATA Premium Support

## Vorteile

- Rundumschutz vor Cyberbedrohungen
- Einheitliche Umsetzung der weltweit gültigen Unternehmens-Richtlinien
- Schnelle Hilfestellung und Problemlösung durch geschultes Service-Personal von G DATA



**Branche:**  
Maschinenbau/Industrie



**Umfang:**  
> 1.000 Clients



**Standort:**  
Deutschland, Eislingen  
(Hauptsitz) mit Niederlassungen  
im Ausland

Europa, Asien, Nord-Amerika – längst sind Maschinenbau-Unternehmen wie die MAG IAS GmbH als Teil der globalen FFG Gruppe weltweit vertreten. Das gilt auch für die angestellten Fachkräfte, die nicht nur in Europa arbeiten. Trotz der räumlichen Trennung vom Unternehmenshaupt-sitz in Eislingen müssen die IT-Security-Compliance-Richtlinien auf internationaler Ebene funktionieren – ganz egal, ob auf dem Notebook oder dem Smartphone. G DATA hat sich dieser Herausforderung erfolgreich angenommen.

Durch permanente technologische Innovationen und den hohen Qualitätsstandards ist der deutsche Maschinenbau weltweit sehr gut positioniert – so auch die MAG IAS GmbH. Das in Eislingen beheimatete Unternehmen wurde 2005 gegründet. Es erstellt Werkzeugmaschinen und übernimmt Bearbeitungsaufgaben in der Fräs- und Drehbearbeitung für Turn-Key Fertigungssysteme. Mit über 1.000 Mitarbeitern ist die MAG global vertreten: USA, China, Indien, Ungarn und die Schweiz sind nur einige Standorte.

Als internationales Unternehmen hat die MAG weltweit Mitarbeiter. Dadurch steigt nicht nur die Heterogenität der Geräte, sondern auch die Komplexität der Administrierbarkeit. Da die Notebooks weltweit im Einsatz sind

und außerhalb deutscher Grenzen bedient werden, bedarf es einer individuellen IT-Sicherheitslösung auf breiter Ebene. Dieser Herausforderung war sich auch Axel Weiler bewusst. Er ist Senior Manager IT-Infrastructure bei der MAG IAS GmbH und hatte Ende 2017 die Aufgabe, eine Lösung zu finden.

„Die Flexibilität, die wir in unserem Betrieb benötigen, war durch die alte Antiviren-Lösung schlichtweg nicht gegeben“, sagt Weiler. „Die zentrale Steuerbarkeit der Clients war praktisch nicht möglich.“ Die Folge: „Zero Days“. Man habe versucht, den Antiviren-Anbieter zu kontaktieren, um schnellstmöglich Updates einspielen zu können, doch das habe sehr lange gedauert, erklärt Weiler. Der IT-Dienstleister von MAG, der die gesamte

„Einer der ausschlaggebenden Gründe für G DATA war der Web-Filter, mit dem wir nun vom Hauptsitz aus die vordefinierten Policy-Richtlinien global vollumfänglich durchsetzen können.“

**Axel Weiler, Senior Manager IT-Infrastructure**

Mehr als nur  
Virenschutz

Wartung und Pflege der IT-Infrastruktur vornimmt, habe hier einen sehr hohen Aufwand zur Behebung des Problems betreiben müssen. Die Kommunikation ging dabei bis zur höchsten Management-Ebene“, erinnert sich der IT-Infrastruktur Experte.

### **Es wird Zeit für eine Änderung**

Nach den beiden Vorfällen und weiteren Problemen im Feld der Performance und des Kundensupports, machten sich Weiler und sein Vorgesetzter auf die Suche nach einem anderen IT-Sicherheitslösungsanbieter. „Wir waren mit der bisherigen Antivirenlösung nicht mehr zufrieden. Da herrschte einfach kein Vertrauen mehr“, sagt Weiler. Schließlich habe man sich explizit nach deutschen IT-Lösungen umgesehen und die beiden Marktkonkurrenten miteinander verglichen. Daraus ergab sich für die Zukunft, dass die IT-Sicherheitslösung von G DATA eingesetzt werden sollte. Hierbei wurden in Zusammenarbeit mit dem Premium-Support Migrations-Strategien entwickelt. Knapp 2.000 Software-Lizenzen sollten in einem Zeitraum von sechs bis neun Monaten umziehen. Konkret wurde G DATA Endpoint Protection in Verbindung mit dem Modul Policy Manager als Lösung ausgewählt.

„Einer der ausschlaggebenden Gründe für G DATA war der Web-Filter“, sagt der IT-Infrastructure Manager. MAG hat Unternehmensrichtlinien festgelegt, die den Zugriff auf bestimmte Webseiten einschränkt. Mitarbeiter können beispielsweise daran gehindert werden, Webseiten zu besuchen, die mit der aktuellen Aufgabe nichts zu tun haben oder ungesetzlich respektive unangemessen sind. Weiterhin kann der IT-Administrator vordefinierte Webseiten-Kategorien blockieren. Jede Kategorie besteht aus einer Liste von URLs, die auf die Blacklist gesetzt wurden und blockiert werden können.

Diese Herangehensweise war Weiler besonders wichtig, denn die international verteilten Notebooks sind weltweit aktiv und für den IT-Administrator nicht in unmittelbarer Reichweite verfügbar. „Wir haben hier bei MAG einen zentralen Webfilter-Schutz etabliert. Dieser greift aber nicht, sobald unsere Mitarbeiter mit ihrem Notebook außerhalb der Organisation sind“, erklärt Weiler. Die Service-Techniker von MAG konnten bis dato auf jede beliebige Webseite zugreifen – egal ob auf einer Baustelle in China oder in Deutschland. Folglich bestand die Gefahr, dass Mitarbeiter

auf einer Internetseite mit Schadsoftware landen würden. „Mit dem Web-Filter können wir nun am Hauptsitz die vordefinierten Policy-Richtlinien offline auf die Notebooks einspielen, hinterlegen und somit global vollumfänglich durchsetzen.“

Neugierig, wie auch Sie Ihr Unternehmen mit G DATA absichern können?

Hier erfahren Sie mehr:



[gdata.de/business](https://gdata.de/business)



[vertrieb@gdata.de](mailto:vertrieb@gdata.de)



0234 / 9762-170



TRUST IN  
GERMAN  
SICHERHEIT

© Copyright 2020 G DATA CyberDefense AG. Alle Rechte vorbehalten. Kein Teil dieses Dokuments darf ohne vorherige schriftliche Genehmigung der G DATA CyberDefense AG Deutschland kopiert oder reproduziert werden.

Microsoft, Windows, Outlook und Exchange Server sind eingetragene Marken der Microsoft Corporation. Alle anderen Marken- oder Produktnamen sind Warenzeichen ihrer jeweiligen Eigentümer und sind daher entsprechend zu behandeln.