

HÖCHSTE SICHERHEIT FÜR GERÄTE UND PROZESSE

Modern Secure Workplace sorgt für sichere Vernetzung
und Digitalisierung bei minimalem Aufwand



Umfassender Schutz von
Endgeräten, Netzwerk
und Kommunikation



Komfortabler Überblick
über aktuelle Bedrohungs-
und Sicherheitslage



Rasche Erkennung
und Behebung von
Vorfällen



Reduzierter
Administrationsaufwand
für IT-Team



Die VAF GmbH ist ein expandierendes mittelständisches Familienunternehmen und führender Hersteller von Sondermaschinen und Sonderanlagen für namhafte Automobilhersteller und deren Zulieferer. Das Unternehmen wurde 1983 gegründet und agiert heute mit mehr als 450 Mitarbeitenden vom Hauptsitz im schwäbischen Bopfingen und einer Niederlassung in Salzgitter weltweit. Gemeinsam mit seinen Kunden entwickelt und realisiert der Spezialist für die Entwicklung und Herstellung von Montagelinien für sämtliche Komponenten des Fahrzeugantriebs wie Motor, Getriebe und Fahrwerk komplexe Automatisierungslösungen – von der Planung bis zur Inbetriebnahme vor Ort.

MITARBEITENDE

450+

vaf-bopfingen.de

01 — AUSGANGSLAGE

Hoher IT-Aufwand für fragmentierte Sicherheitstools

Es bedarf vieler Schritte, bis Montageanlagen für Motoren, Getriebe und Fahrwerke einsatzbereit sind: von der technischen Konstruktion über die Weiterleitung in die Produktionsabteilung bis hin zur Produktion, Montage und Programmierung der Anlage und schließlich der Auslieferung an die Kunden. Dabei ist die VAF GmbH bestrebt, alle Prozesse möglichst papierlos und digital abzubilden – vom Anfang bis zum Ende. „Das erfordert viele Schnittstellen, sowohl intern als auch extern zu unseren Kunden“, erklärt Tobias Stanzel, Teamleiter Infrastruktur bei VAF. „Und die müssen vor allem eines sein: absolut sicher.“

In der Vergangenheit setzte das Familienunternehmen für die Sicherheit seiner IT-Infrastruktur vor allem auf spezialisierte Tools für die Software-Verteilung, VPN, Firewall und Antivirus. Das führte allerdings zu einer hohen Fragmentierung, weil die Tools nicht miteinander integriert waren, und so zu einem hohen administrativen Aufwand für das kleine IT-Team. Da die Gefahr von Cyberangriffen jedoch immer weiter zunimmt, war die VAF auf der Suche nach einer Lösung, um dieser Gefahr – bei überschaubarem Aufwand – zu begegnen.



”

„Wir wollen alle Prozesse möglichst papierlos und digital abbilden – vom Anfang bis zum Ende. Das erfordert viele Schnittstellen, sowohl intern als auch extern zu unseren Kunden. Und die müssen vor allem eines sein: absolut sicher.“

TOBIAS STANZEL
TEAMLEITER INFRASTRUKTUR BEI VAF

02 — ANFORDERUNGEN

Höchste Sicherheit bei minimalen Administrationsaufwand

Das Thema Sicherheit hatte für die VAF deshalb oberste Priorität bei der Modernisierung ihrer IT-Infrastruktur.

Das betrifft zum einen den Schutz der Montageanlagen und Roboter sowie der Abläufe und Software innerhalb der Fertigungsstraßen vor Datenlecks und Viren. Außerdem sollte eine sichere Kommunikation zwischen den mobilen Montageplätzen und den Konstrukteur:innen ermöglicht werden, ohne Gefahr zu laufen, dass interne technische Daten nach außen dringen. Auch im Außendienst sollen sich die Mitarbeitenden, wenn sie Maschinen vor Ort reparieren oder

warten, unterwegs sicher in fremden Netzen bewegen können, ohne ihre Endgeräte mit Malware zu infizieren. Sollte dennoch ein Problem auftreten, soll dieses schnellstmöglich erkannt und behoben werden.

Neben dem Fokus auf Sicherheitsaspekte war es der VAF ein Anliegen, die IT-Abteilung zu entlasten, die IT-Infrastruktur deutlich zu verschlanken und über eine einheitliche Plattform zum Monitoring und zur Steuerung zu verfügen. Darüber hinaus sollte die Performance stimmen und die Beschäftigten der VAF stets arbeitsfähig bleiben.

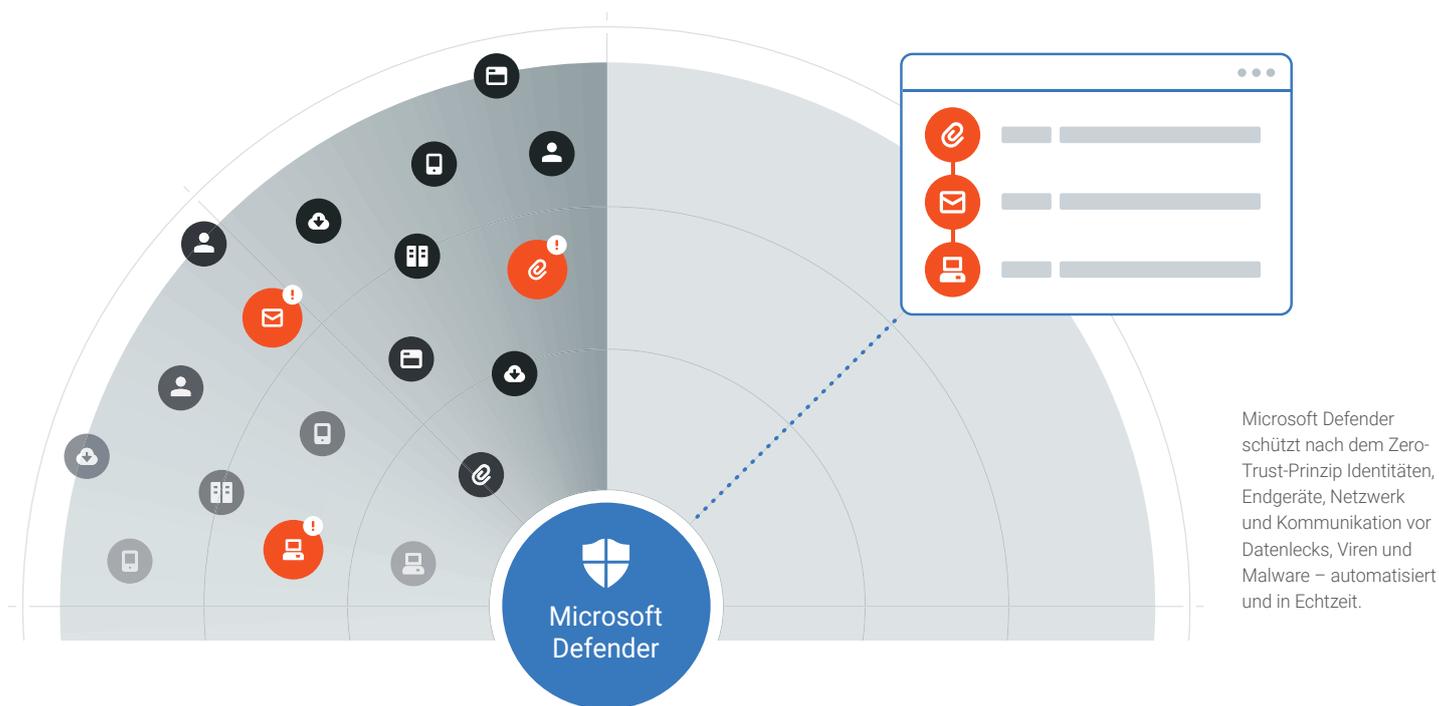
Managed Secure Workplace erleichtert Monitoring und Steuerung der IT-Infrastruktur

Die VAF entschied sich dazu, für ihr IT-Projekt die abtis GmbH als erfahrenen Partner ins Boot zu holen. Nach einer umfangreichen Bestandsaufnahme mit Risikobewertung und Aufdeckung möglicher Schwachstellen folgte das Unternehmen der Empfehlung des Pforzheimer IT-Dienstleisters und entschied sich für die Einführung einer Managed-Service-Umgebung auf der Basis von Microsoft 365.

Der Modern Secure Workplace vereint und orchestriert verschiedene Tools aus dem Portfolio von Microsoft 365. „Die Produkte aus dem Microsoft Kosmos bieten den Vorteil,

dass sie eine einheitliche Oberfläche haben. Alle Tools sind lückenlos ineinander integriert, sodass Daten aus unterschiedlichsten Systemen zusammengeführt werden können“, erläutert Tobias Stanzel. „So werden jährlich rund eine Milliarde Ereignisse verarbeitet und bewertet und anschließend auf rund 1.000 Vorfälle reduziert.

Daraus ergibt sich ein detailliertes Gesamtbild des Sicherheitsniveaus mit konkreten Handlungsempfehlungen, das sich mit geringem Aufwand administrieren lässt.“



Microsoft Defender schützt nach dem Zero-Trust-Prinzip Identitäten, Endgeräte, Netzwerk und Kommunikation vor Datenlecks, Viren und Malware – automatisiert und in Echtzeit.

Zero-Trust-Prinzip für höchste Cybersecurity

Um Identitäten, Endgeräte, Netzwerk und Kommunikation vor Datenlecks, Viren und Malware zu schützen, agieren die Bestandteile der Lösung auf unterschiedlichen Ebenen basierend auf dem Zero-Trust-Prinzip. Dabei werden Dienste, Geräte und Identitäten bis sie ihre

Vertrauenswürdigkeit nachweisen können stets als nicht vertrauenswürdig eingestuft – sowohl innerhalb als auch außerhalb der eigenen Systeme. Zunächst wird die IT-Infrastruktur durch eine sichere Konfiguration der Systeme geschützt und nahezu alle Angriffsversuche identifiziert

und abgewehrt. Verschiedene Komponenten der Microsoft Defender Suite sorgen für einen automatisierten Ablauf aller Prozesse in Echtzeit. Wird dennoch ein Vorfall erkannt, können die Mitarbeitenden der abtis im Cyber Defense Operations Center (CDOC) rund um die Uhr eingreifen und Infrastruktur und Unternehmensdaten aktiv schützen. In einem eigenen Security-Portal werden alle Informationen aus den Microsoft-Services gebündelt und in einer rollenbasierten Ansicht zur Verfügung gestellt. So wird der komplette

E-Mail-Verkehr geschützt. Es wird überwacht, ob Rechner oder Identitäten nicht mehr compliant sind, Attacken und Übernahmeversuche drohen oder ob es verdächtige Datentransfers oder Zugriffsversuche gibt. Das IT-Team der VAF kann jederzeit den Sicherheitsstatus sämtlicher Geräte und Accounts abfragen, Software remote nachrüsten, befallene Geräte schnell isolieren und mögliche Gefahren automatisiert eingrenzen.

“

„Bei unserer neuen Cybersecurity-Lösung auf Basis von Microsoft 365 kommt alles aus einer Hand. Der Plattform-Ansatz ermöglicht uns eine Administration mit geringem Aufwand, sodass wir uns auf unsere Kernkompetenzen konzentrieren können: den Schutz unserer Infrastruktur vor Cyberangriffen.“

TOBIAS STANZEL

TEAMLEITER INFRASTRUKTUR BEI VAF



Reduzierter Aufwand bei maximaler Transparenz für Sicherheitslage

„Dadurch wird die Komplexität für die Administrator:innen deutlich reduziert. Die aktuelle Bedrohungs- und Sicherheitslage ist auf einen Blick erkennbar, von der Identifikation bis zur Meldung einer Gefahr vergehen im Schnitt nur rund vier bis fünf Minuten. Bereits nach rund vier Stunden werden Incidents in der Regel abgeschlossen“, berichtet Tobias Stanzel. Auch mit einem kleinen IT-Team kann die VAF ihr Sicherheitsniveau damit konstant halten und die Lage jederzeit im Blick behalten.

Mit der neuen Security-Lösung ist VAF optimal vor Cyberangriffen geschützt und kann sich weiteren Digitalisierungen und Innovationen zuwenden. Auch in der Zukunft will das Unternehmen weiter mit abtis zusammenarbeiten – in einem nächsten Schritt ist beispielsweise die Implementierung von Azure Container Instances (ACI) geplant sowie die Migration der Serverlandschaft nach Microsoft Azure.

Mittelständischer Maschinenbauer ist gewappnet gegen Cyberangriffe

 <p>01</p> <p>Microsoft Defender sichert IT-Systeme – automatisiert und in Echtzeit</p>	 <p>02</p> <p>Security-Portal bündelt Informationen aus Microsoft Services und schafft Transparenz</p>	 <p>03</p> <p>abtis Modern Secure Workplace und CDOC bündeln und orchestrieren Security Tools für Microsoft 365</p>	 <p>04</p> <p>Verringerter Aufwand bei maximaler Handlungsfähigkeit des IT-Teams</p>
--	---	--	---

„Uns war schnell klar, dass wir hier auf die Hilfe durch einen erfahrenen Partner angewiesen waren. Deshalb haben wir abtis GmbH mit ins Boot geholt.“

AUFGABE

- Modernisierung der Security-Infrastruktur
- Bereitstellung einer einheitlichen Plattform
- Transparenz und proaktiver Blick auf Sicherheitsniveau

KONZEPT

- Einsatz verschiedener Security Tools aus dem M365-Portfolio
- Bündelung der Informationen, Monitoring, Steuerung über Security-Portal und abtis CDOC
- Managed Service Modern Secure Workplace orchestriert eingesetzte Tools

UNSERE LEISTUNG

- Beratung bzgl. der technischen Möglichkeiten und Konzeption der Lösungen
- Unterstützung bei der technischen Umsetzung und Migration
- Coaching und Support der internen IT

ERGEBNIS

- VAF löst sich von hoher Fragmentierung bei maximalem Administrationsaufwand und profitiert von einheitlicher, einfach zu administrierender Plattform
- Vorausschauende Beobachtung der Sicherheitslage, schnelle Reaktionsmöglichkeit auf Vorfälle
- Unternehmen kann sich auf Innovationen und weitere Digitalisierung fokussieren

Nehmen Sie Kontakt mit uns auf.

 www.abtis.de
 +49 7231 4431 - 100
  vertrieb@abtis.de
 [/company/abtis-gmbh](https://www.linkedin.com/company/abtis-gmbh)

