

Warum IT-Union?

- Seit 2003 Partner von FORTINET
- Managed Service & 24x7 Support
- Schnelle Reaktionszeiten & hohe Flexibilität
- 25+ Jahre Erfahrung & tiefgreifendes Know-how
- 15+ zertifizierte System-Ingenieure in DACH (NSE 4-8)

Warum Fortinet?

- Support-Center in Deutschland
- Zentrales Management und Reporting
- Einheitliche Funktion und Benutzeroberfläche
- 343 Patente veröffentlicht, 280 Patente ausstehend
- Hard-, Software & Services sind Eigenentwicklungen von Fortinet (keine Abhängigkeiten von 3rd Party)
- Unlimitierte Benutzeranzahl (einfaches Lizenzmodell)
- Lösungen für PKI, Email- & Web-Security, Sandboxing
- Gegründet 2000, NASDAQ: FTNT, Marktkap. >5 Mrd. USD
- Eigene FortiASIC Security Prozessoren für Echtzeit-Schutz (bis 1Tbit+ Performance, geringe Latenz)
- 4.650+ Mitarbeiter, davon 25% in Research & Development

200+ Auszeichnungen, inkl.:

- Security Product of the Year
- 5 ICSA Security Certifications
- Breaking Point Resiliency Score
- Best Integrated Security Appliance
- FIPS & Common Criteria Certification
- NSS recommended (NGFW, IPS, WAF, Sandbox)



IT-Union GmbH & Co. KG

KIEL – HAMBURG – LEIPZIG – KÖLN – FULDA – SCHWEINFURT
STUTTGART – MÜNCHEN – WIEN (A) – MALTERS (CH)

NORD

Kiel

BMA networks GmbH
Preetzer Chaussee 55
24222 Schwentinental

Telefon 0431 97449 0
Email vertrieb.ki@it-union.eu

Hamburg

BMA networks GmbH
Albert-Einstein-Ring 5
Arelia-Haus, 22761 Hamburg

Telefon 0431 97449 0
Email vertrieb.hh@it-union.eu

MITTE

Köln

GORDION
Data Systems Technology GmbH
Mottmannstraße 13
53842 Troisdorf

Telefon 02241 4904 0
Email vertrieb.kln@it-union.eu

Fulda

VINTIN GmbH

Rangstraße 39
36043 Fulda

Telefon 0661 250359 0
Email vertrieb.fd@it-union.eu

Schweinfurt

VINTIN GmbH
Felix-Wankel-Straße 4
97526 Sennfeld

Telefon 09721 67594 10
Email vertrieb.sw@it-union.eu

Leipzig

VINTIN GmbH
Arthur-Hausmann-Straße 14
04129 Leipzig

Telefon 09721 67594 126
Email vertrieb.sw@it-union.eu

SÜD

Stuttgart

indasys connectivity GmbH
Leitzstraße 4c
70469 Stuttgart

Telefon 0711 896659 115
Email vertrieb.st@it-union.eu

München

VINTIN GmbH
Max-Planck-Straße 10
85716 Unterschleißheim

Telefon 089 37427 909 0
Email vertrieb.muc@it-union.eu

A CH

Wien (Servicestützpunkt)

Email vertrieb.a@it-union.eu

Malters

VINTIN GmbH
Bahnhofstrasse 7
CH-6102 Malters

Telefon +41 41 5600067
Email vertrieb.ch@it-union.eu

Weitere Informationen:
www.it-union.eu/fortinet

Copyright 2017 IT-Union GmbH & Co. KG.
Änderungen und Irrtümer vorbehalten. Alle Rechte vorbehalten.
Alle Logos, Marken, Firmennamen und Produktdesigns gehören ihren jeweiligen Eigentümern.

www.it-union.eu



FortiSIEM



SECURITY INFORMATION & EVENT MANAGEMENT



FORTINET
SECURITY
FABRIC





Warum FortiSIEM?

FortiSIEM umfasst den zentralen Ansatz für das Controlling von kritischen Informationen und Daten zu sicherheitsrelevanten Ereignissen / Vorfällen in Ihrer Netzwerk-Infrastruktur.

FortiSIEM liefert eine automatisierte Einsammlung sowie das Parsing von Log-Daten unternehmenskritischer IT-Geräte/-Dienste, u.a.:

- Anwendungen, z.B. Mail-Dienste
- Betriebssysteme & Firmwares
- IT-Sicherheitslösungen
- Netzwerke & Clouds

FortiSIEM unterstützt hierbei eine zeitnahe Erstellung von Compliance-Nachweisen zur IT-Sicherheit und ermöglicht eine optimierte Aufdeckung von Sicherheits-Risiken bzw. genutzten Schwachstellen, welche von Angreifern missbraucht wurden.

FortiSIEM ist somit u.a. ein ideales Werkzeug zur Einhaltung gesetzlicher Vorgaben, u.a. im Hinblick auf KRITIS, ISO-27001 & BSI-Standard-100 (ISMS), PCI, europäische Datenschutz-Grundverordnung (EU-DSGVO / GDPR).

Highlights

- Mandanten-fähig
- MSP/MSSP ready
- Selbstlernende Bestandsaufnahme
- Security & Compliance Out-of-the-Box
- Übergreifende Netzwerk-Analysen in Echtzeit
- Korrelation von Informationen aus SOC & NOC
- Umfassende Regelsätze & Device-Templates Out-of-the-Box vorhanden
- Definition von unternehmenskritischen Diensten (z.B. Email) & Alarmierung bei Beeinträchtigung beteiligter, kritischer Komponenten
- Einstieg ab 50 Devices möglich, flexibel skalierbar (Start mit unternehmenskritischen Geräten & Diensten)
- Zentralisiertes Management (Single Pane of Glass)



Fortinet Security Fabric

ermöglicht dynamische Sicherheit - organisationsweit

Jedes Element der Fortinet-Lösung ist wie ein Teil einer "Security Fabric", welche Policies und aktuelle Infos zu Gefahren entsprechend nutzt. Ausgehend von den Next Generation Firewalls (FortiGate, skalierbar bis 1Tbps(!) Throughput) ermöglicht insbesondere eine Erweiterung der Lösung mit den Elementen "Email Security (FortiMail)", "Web Application Firewalling (FortiWeb)" und "Advanced Threat Protection (FortiSandbox)" ein globales, zukunfts-sicheres und ganzheitliches Security-Konzept.

SECURITY FABRIC



Haben Sie Ihre Log-Daten im Blick?

Zentrale Korrelation & automatisierte Echtzeit-Analyse von Log- / Ereignisdaten, inkl. Alarmierung.

FortiSIEM ermöglicht eine Echtzeit-Analyse von Ereignis-Daten verschiedener Quellen Ihrer kritischen Netzwerk-Infrastruktur.

FortiSIEM prüft nach Ihrer Vorgabe:

- Logs & Performance-Metriken
- SNMP-Traps & Security-Alerts
- Konfigurations-Änderungen von:

- Servern
- Diensten
- Applikationen
- Netzwerk-Systeme
- Security-Systeme

FortiSIEM strukturiert die verschiedenen Daten, analysiert mögliche Korrelationen, unterstützt eine Auswertung nach geforderten Such-Kriterien, inklusive Alarmierung und Security / Compliance Reporting. Dies erfolgt automatisiert, in Echtzeit.

Weitere Features

- Baselining
- Performance-Monitoring
- Security Analysen in Echtzeit
- Einfache & flexible Administration
- Integration von 3rd-Party Devices
- Umfassende, skalierbare Analysen
- Statistiken zur Anomalie-Erkennung
- Out-of-the-Box Compliance-Reports
- Notification- & Incident-Management
- Einfache Skalierung auf Basis von VM-basierter Architektur (u.a. Worker)
- Integration externer Threat-Intelligence
- Monitoring der Verfügbarkeit kritischer Systeme
- Skalierbare, flexible (Ein-)Sammlung von Log-Daten