

Ihre Vorteile

- Applikationssicherheit als Service
- Schwachstellenschutz dank Virtual Patching
- Einhaltung von Compliance Vorschriften
- Marktführende Technologie
- Skalierbare und kalkulierbare Kosten von Anfang an
- Keine Investition in künftige jährliche Software-Wartungsverträge, Consulting oder Trainings
- indevis übernimmt das komplette Setup und Design
- indevis stellt ein Helpdesk zur Verfügung – und entlastet damit Ihre eigene IT-Abteilung



SIE WOLLEN MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

INDEVIS WEB APP SECURE

SCHUTZ FÜR IHRE WEB APPLIKATION

Anwendungen sind heute die Hauptziele von Angriffen und für viele Unternehmen sind die Verfügbarkeit und Integrität dieser Applikationen und Daten äußerst geschäftskritisch. Aktuell wird der Hauptteil der Security-Investitionen in Netzwerksicherheit getätigt, obwohl mehr als zwei Drittel der Angriffe direkt die Anwendungen attackieren. Die Bedrohungen für Anwendungen und Daten sind jedoch hartnäckig und nehmen jeden Tag zu. Daher müssen diese Angriffe identifiziert und abgewehrt werden, ohne die Anwendungsleistung zu lähmen und die Daten des Unternehmens zu beeinträchtigen.

indevis Web App Secure basiert auf der marktführenden Sicherheitstechnologie von F5 Networks. Der Application Security Manager (ASM) von F5 ermöglicht die Abwehr ausgeklügelter, komplexer Bedrohungen mit einer Sicherheitseffizienz von 99,89 Prozent. Gleichzeitig bleibt durch die SSL-Auslagerung die Performance bei Anwendungen und die Verhinderung des Caching böswilliger Inhalte erhalten.

ENTERPRISE APPLICATION SECURITY SERVICE

Der *indevis Web App Secure Service* begegnet diesen Bedrohungen durch eine Kombination führender Verfahren für die Verteidigung gegen Layer-7-DoS-Angriffe, erweiterte Techniken für die Erkennung und Risikominderung, tiefgehende Bedrohungsanalyse, virtuelles Patching und eine granulare Angriffstransparenz.

indevis Web App Secure bietet zudem einen Überblick über den HTTP- und WebSocket-Datenverkehr zum Schutz vor Angriffen, die sich unter den normalen Webdatenverkehr, Streaming-Datenfeeds und Chatsitzungen mischen.

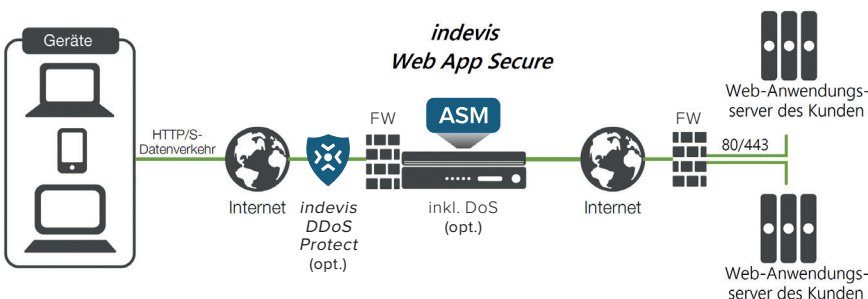
VON INDEVIS WEB APP SECURE GESCHÜTZTE APPLIKATIONEN

- Dank Virtual Patching lassen sich sofort Schwachstellen von Anwendungen mithilfe des *indevis Tech Supports* patchen, bis vom Hersteller der Software ein offizieller Patch erhältlich ist.
- Webentwicklung ist dynamisch. Bei der Konzentration auf Funktionen und Zeitpläne treten Fehler auf. So weiß jeder Entwickler, dass ein eingehender Aufruf nie für eine Datenbank verwendet werden darf. Trotzdem tauchen eingehende Datenbankaufrufe immer wieder in App-Code auf.
- Verhinderung des Verlusts sensibler Informationen durch einen angepassten Schutz, den *indevis* mit dem Servicenehmer individuell passend einrichtet. Die Einhaltung von PCI-DSS, HIPAA, SOX, Basel II und anderer Compliance-Standards wird erleichtert.
- Geolocation-basiertes Blocking erlaubt es, den Zugang zur Website von bestimmten Ländern und Regionen einzuschränken.



FEATURE-ÜBERSICHT DER EINZELNEN SERVICE-VERSIONEN

| Features WAF | OWASP Top 10 Ready | Standard | Advanced |
|---|--------------------|----------|----------|
| HTTP Protocol Compliance | - | ✓ | ✓ |
| Attack Signatures Protect for SQL-Injection, XSS, Known Vulnerabilities etc. | ✓ | ✓ | ✓ |
| Device-ID Detection / Fingerprinting | - | - | ✓ |
| IP-Intelligence (BotNets, Scanners, DoS etc. Categories) | - | - | ✓ |
| Brute Force Protection | - | - | ✓ |
| Web Scraping Protection | - | ✓ | ✓ |
| Session Tracking | - | - | ✓ |
| Login Enforcement | ✓ | - | ✓ |
| Cookie Protection | ✓ | - | ✓ |
| Dynamic Parameter Protection | ✓ | - | ✓ |
| DataGuard Response Checking | ✓ | - | ✓ |
| CSRF Protection | ✓ | ✓ | ✓ |
| GeoLoc-Enforcement | - | ✓ | ✓ |
| Policy Fine Tuning, Add All Entities Mode (Whitelisting URLs, File Types, Parameters and Cookies) | ✓ | - | ✓ |
| Violation Summaries / Traffic Stats / Learning | ✓ | ✓ | ✓ |
| WEB 2.0 Protection für XML und Web-Services. JSON, SOAP, WSDL | ✓ | - | ✓ |



OPTIONAL: DOS-SCHUTZ ALS ADD-ON

Durch einen Denial-of-Service-Angriff werden Dienste in ihrer Funktionalität beeinträchtigt und stehen Nutzern sowie Unternehmen nur eingeschränkt zur Verfügung. Ein DoS-Angriff besteht heute meist aus einer Kombination verschiedener Angriffsvektoren, die gleichzeitig aktiv sind, um eine Schwachstelle in der Infrastruktur zu finden und auszunutzen – seien es nun Netzwerkgeräte, Anwendungen oder Netzwerkbandbreite. Unterschiedliche Angriffe müssen auch mit unterschiedlichen Maßnahmen bekämpft werden. Der DoS-Schutz von indevis bietet eine Verteidigungslösung auf mehreren Ebenen, die vor kombinierten Netzwerkangriffen und fortschrittlichen Anwendungsattacken schützt.

Sie wollen *indevis Web App Secure* kennenlernen? Auf Wunsch führen wir Ihnen diesen Service gerne in einer Demo-Session vor und erläutern Ihnen die Vorteile eines umfassenden Web Application Security Services.

Über die indevis GmbH

Die ISO 27001 zertifizierte indevis GmbH bietet seit 1999 IT-Sicherheits-, Data-center- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT-Sicherheit und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT Sicherheit passiert nicht von alleine, sondern muss strategisch geplant werden.

indevis betreibt zwei Niederlassungen: in München und Hamburg. Weitere Mitarbeiter agieren von mehreren Standorten über Deutschland verteilt aus.



indevis GmbH

Koppstraße 14
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de