IMPERVA®

Imperva SecureSphere Web Application Firewall

DATENBLATT

Schützen Sie Ihre kritischen Web-Anwendungen und -Daten

Web-Anwendungen sind eines der Hauptziele von Cyber-Angriffen, denn sie sind problemlos zugänglich und bieten einen einfachen Zugangspunkt zu wertvollen Daten. Zur Abwehr von Cyber-Angriffen müssen Unternehmen Websites und Anwendungen vor vorhandenen und neuen Cyber-Bedrohungen schützen, ohne die Anwendungsleistung oder -verfügbarkeit zu beeinträchtigen.

Für den Schutz ihrer kritischen Web-Anwendungen setzen immer mehr Unternehmen auf Imperva. Die Imperva Web Application Security-Lösungen passen sich nahtlos in physische, virtuelle und cloud-basierte Rechenzentren ein. Sie bieten den fortschrittlichsten Web-Anwendungsschutz auf dem Markt und werden kontinuierlich anhand der Erkenntnisse des renommierten Imperva Defense Center-Forschungsteams aktualisiert.

SecureSphere Web Application Firewall analysiert jeden Benutzerzugriff auf Ihre geschäftskritischen Web-Anwendungen und schützt Ihre Anwendungen und Daten vor Cyber-Angriffen.

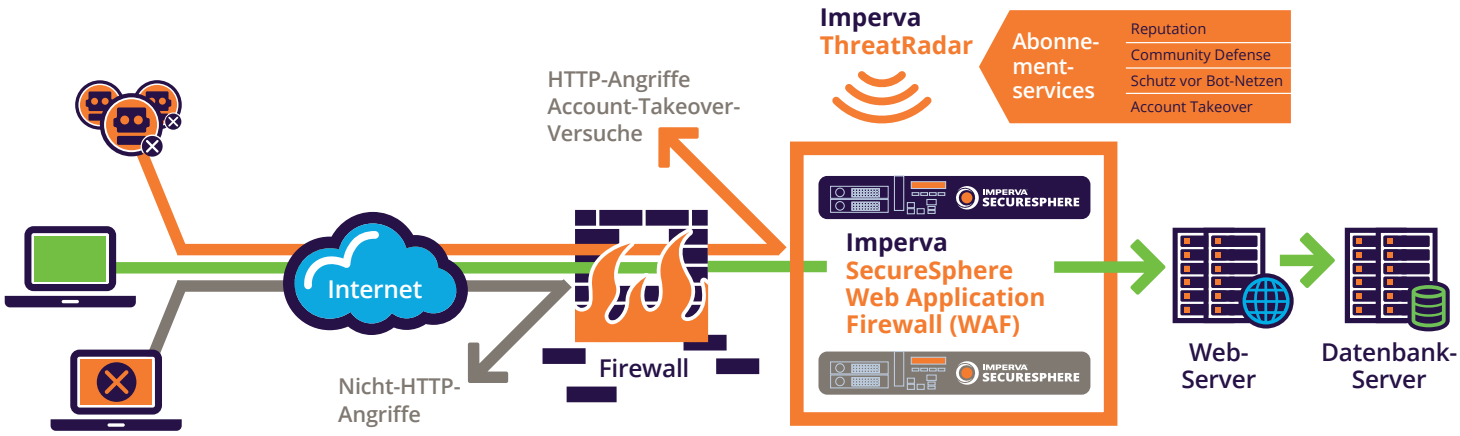
Imperva SecureSphere Web Application Firewall

SecureSphere Web Application Firewall analysiert jeden Benutzerzugriff auf Ihre geschäftskritischen Web-Anwendungen und schützt Ihre Applikationen und Daten vor Cyber-Angriffen. Die SecureSphere Web Application Firewall lernt das „normale" Verhalten Ihrer Anwendungen automatisch und korreliert diese Informationen mit den branchenführenden Bedrohungsdaten, die mittels weltweitem Crowd-Sourcing gewonnen und in Echtzeit aktualisiert werden, um effektiven Schutz zu bieten.

Imperva wurde als einziger Anbieter im Gartner Magic Quadrant für Web Application Firewalls als „Leader" eingestuft.[1] Die branchenführende SecureSphere Web Application Firewall identifiziert Bedrohungen, die in böswilliger Absicht in harmlos erscheinenden Website-Verkehr eingebunden sind und reagiert darauf. Solche Angriffe umgehen traditionelle Abwehrmaßnahmen. Die Firewall blockiert technische Angriffe wie SQL-Injection, Cross-Site Scripting und Remote File Inclusion und Angriffe auf die Geschäftslogik wie Site Scraping und Kommentar-Spam, Bot-Netze und DDoS-Angriffe. Außerdem verhindert sie die Account-Takeover-Versuche in Echtzeit, bevor ein Betrug ausgeführt werden kann.

[1] Gartner Magic Quadrant für Web Application Firewalls, Jeremy D'Hoinne, Adam Hils, Claudio Neiva, 19. Juli 2016

Gartner empfiehlt keine der in seinen Forschungsberichten dargestellten Anbieter, Produkte oder Services und rät den Nutzern der Technologie nicht zu Anbietern mit den höchsten Bewertungen oder anderen Bezeichnungen. Die Forschungspublikationen von Gartner enthalten die Meinungen des Gartner-Forschungsinstituts und sollten nicht als Tatsachenangaben ausgelegt werden. Gartner schließt alle ausdrücklichen und stillschweigenden Gewährleistungen in Bezug auf diese Forschungsarbeit aus, einschließlich der Gewährleistung der Marktfähigkeit oder der Eignung für einen bestimmten Zweck.



ThreatRadar Intelligent Feeds:

- **Reputation Service** – Filtert Verkehr auf Grundlage der neuesten Echtzeit-Reputationsquelle
- **Community Defense** – Spezielle Bedrohungsinformationen, die mittels Crowd-Sourcing von Imperva-Benutzern gewonnen werden
- **Bot Protection** – Erkennt Bot-Netz-Clients und DDoS-Angriffe auf Anwendungen
- **Account Takeover Protection** – Schützt Website-Benutzerkonten vor Angriffen und Übernahmen
- **Fraud Prevention** – Vereinfacht die Implementierung marktführender Partnerprodukte für Fraud Prevention

Kernkompetenzen von Imperva SecureSphere

Automatisches Lernen von Benutzer- und Anwendungsverhalten

Um Angriffe präzise erkennen zu können, muss eine Web Application Firewall Struktur und Elemente der Anwendung kennen und das erwartete Benutzerverhalten verstehen. Die zum Patent angemeldete Dynamic Profiling-Technologie automatisiert diesen Prozess durch das Erstellen von Profilen für geschützte Applikationen und den Aufbau einer „White List" für akzeptables Benutzerverhalten. Darüber hinaus lernt sie im Laufe der Zeit automatisch Anwendungsveränderungen. Dynamic Profiling macht die manuelle Konfiguration – und Aktualisierung – zahlloser Anwendungs-URLs, Parameter, Cookies und Methoden überflüssig.

Sicherheitsrichtlinien aus der Forschung

Mit Unterstützung des Imperva Defense Centers – einem Forschungsteam aus weltweit führenden Experten für Daten- und Anwendungssicherheit – bietet SecureSphere die umfangreichste verfügbare Zusammenstellung von Anwendungssignaturen und -richtlinien. Imperva Defense Center untersucht Schwachstellen, die von Bugtraq, CVE®, Snort® und Untergrundforen gemeldet werden. Darüber hinaus führt das Team eigene Untersuchungen durch, um die aktuellsten und umfangreichsten Bedrohungsinformationen bereitzustellen und so für den optimalen Schutz Ihrer Webanwendungen gegen Angriffe zu sorgen.

Flexible Implementierungsoptionen

SecureSphere ist als physische oder virtuelle Appliance, über Amazon Web Services oder in einer Mischform daraus implementierbar. Das Deployment kann flexibel den individuellen Kundenanforderungen angepasst werden, weil sich SecureSphere transparent implementieren lässt und dafür praktisch keine Veränderungen am Netzwerk erforderlich sind. Ein granulares Regelwerk ermöglicht darüber hinaus höchste Präzision und einmalige Kontrollmechanismen, um die spezifischen Sicherheitsanforderungen jedes einzelnen Unternehmens erfüllen zu können.

Umfassende Bedrohungsinformationen

Um sich vor den heutigen Cyberkriminellen und ihren umfangreichen Ressourcen zu schützen, ist ein hochentwickeltes Warnsystem erforderlich, das die sich ständig weiterentwickelnden web-basierten Angriffe erkennt und davor schützt. Imperva ThreatRadar[2] aktualisiert die SecureSphere Web Application Firewall mit Echtzeit-Bedrohungsinformationen, die mittels weltweitem Crowd-Sourcing gewonnen und vom Imperva Application Defense Center betreut werden. ThreatRadar bietet besseren Schutz, erhöht die WAF-Genauigkeit und lässt das Sicherheitsteam effizienter arbeiten, denn es filtert proaktiv Verkehr von bekannten Gefährdungsquellen, sodass das Sicherheitsteam sich auf das konzentrieren kann, was wirklich wichtig ist.

Virtuelles Patching

Über einen integrierten Schwachstellen-Scanner kann SecureSphere ein „virtuelles Patching" für Ihre Web-Anwendungen durchführen. Nach der Identifizierung einer Schwachstelle bleibt eine Web-Anwendung oft wochen- oder monatelang ungeschützt, bis der Code angepasst wurde. In solchen Fällen schützt virtuelles Patching Web-Anwendungen umgehend vor Angriffen. So kann das Zeitfenster, in dem eine Anwendung angreifbar ist, verkleinert werden, bis zu dem Zeitpunkt, an dem ein Patch auf dem Zielsystem eingespielt wird.

HTTP-Protokoll, Plattform und XML-Schutz

SecureSphere setzt die Einhaltung von HTTP-Standards durch, und verhindert so, dass Protokollschwachstellen ausgenutzt und Verschleierungstechniken eingesetzt werden können. Mithilfe granularer Richtlinien können Administratoren die strenge Einhaltung von RFC-Standards durchsetzen oder geringfügige Abweichungen zulassen. Mit über 8.000 Signaturen sichert SecureSphere die gesamte Anwendungsinfrastruktur einschließlich Anwendungen und Web-Server-Software. Flexible, automatische XML-Sicherheitsrichtlinien schützen Web-Services, SOAP, HTML 5-Web-Sockets und Web 2.0-Anwendungen.

Granulare Korrelationsrichtlinien verhindern „False Positives" (falsche Alarme)

SecureSphere unterscheidet Angriffe von ungewöhnlichem, jedoch zulässigem Verhalten, indem es die Web-Anfragen über einen längeren Zeitraum und mehrere Sicherheitsebenen hinweg korreliert. Die SecureSphere-Funktion „Correlated Attack Validation" prüft verschiedene Merkmale wie HTTP-Protokollkonformität, Profilverletzungen, Signaturen, Sonderzeichen und die Benutzerreputation, um präzise Alerts oder das Blockieren von Angriffen zu ermöglichen. Dabei erzielt sie branchenweit die geringste False-Positive-Rate. ThreatRadar-Bedrohungsinformationen können als Merkmal eingebunden werden. So wird sichergestellt, dass die Richtlinienbeurteilung im Hinblick auf die globale Bedrohungslandschaft auf dem neuesten Stand ist.

Anpassbare Berichte für Compliance und Forensik

Dank der umfangreichen grafischen Berichtsfunktionen von SecureSphere können Kunden ihren Sicherheitsstatus ganz einfach erkennen und damit gesetzliche Vorschriften einhalten. SecureSphere beinhaltet sowohl vordefinierte als auch vollständig anpassbare Berichte. Auf diese Weise können Sie Ihren Sicherheitsstatus schnell beurteilen und den Compliance-Nachweis für PCI, SOX, HIPAA und FISMA sowie andere Compliance-Standards optimieren.

Überwachung für die tiefgreifende Analyse von Angriffen

Alerts können ganz einfach gesucht, sortiert und direkt mit den zugehörigen Sicherheitsregeln verknüpft werden. Das Überwachungs- und Berichts-Framework von SecureSphere macht alle Compliance- und Sicherheitsbelange sofort sichtbar. Ein Echtzeit-Dashboard vermittelt einen Überblick über den Systemstatus und Sicherheitsereignisse.

[2] ThreatRadar-Bedrohungsinformationen stehen als Jahresabonnements zur Verfügung

Imperva SecureSphere Cyber Security

Imperva SecureSphere ist eine umfassende, integrierte Sicherheitsplattform. Sie umfasst Module für die Sicherheit von Webanwendungen, Datenbanken und Dateien. Sie lässt sich so dimensionieren, dass sie auch die Sicherheitsanforderungen von Rechenzentren der größten Unternehmen erfüllt. Das Imperva Application Center ist ein Forschungsteam aus weltweit führenden Experten für Daten- und Anwendungssicherheit. Es sorgt dafür, dass die Plattform immer auf dem neuesten Stand ist und Ihre Anwendungen auch vor neuen Bedrohungen schützt.

IMPERVA SECURESPHERE

SICHERHEIT FÜR WEBANWENDUNGEN	
SecureSphere Web Application Firewall	Präziser, automatischer Schutz vor Online-Bedrohungen
SecureSphere ThreatRadar	Globale Bedrohungsinformationen in Echtzeit, um bekannten schädlichen Datenverkehr zu erkennen, zu filtern und zu blockieren
SICHERHEIT FÜR FÜR DATENBANKEN	
Database Activity Monitor	Vollständige Überprüfung und Transparenz der Nutzung von Datenbankdaten
Database Firewall	Aktivitätsüberwachung und Echtzeitschutz für kritische Datenbanken
Bewertung für Datenbanken	Schwachstellenbeurteilung, Konfigurationsverwaltung und Datenklassifizierung für Datenbanken
User Rights Management für Datenbanken	Überprüfung und Verwaltung von Benutzerzugriffsrechten auf sensible Datenbanken
ADC Insights	Vorbereitete Berichte und Regeln für SAP-, Oracle EBS- und PeopleSoft-Compliance und -Sicherheit
SICHERHEIT FÜR DATEIEN	
File Activity Monitor	Vollständige Überprüfung und Transparenz der Nutzung von Dateidaten
File Firewall	Aktivitätsüberwachung und Schutz für kritische Dateidaten
User Rights Management für Dateien	Überprüfung und Verwaltung von Benutzerzugriffsrechten auf sensible Dateien
Directory Services Monitor	Überprüfen von Änderungen, die im Microsoft Active Directory vorgenommen wurden, und Erstellen entsprechender Alerts und Berichte
PRODUKTE FÜR SHAREPOINT-SICHERHEIT	
SecureSphere für SharePoint	Übersicht und Analyse von SharePoint-Zugriffsrechten und Datennutzung sowie Schutz vor Web-basierten Bedrohungen
MANAGEMENTPRODUKTE	
MX Management Server	Zentrale Schnittstelle für die Verwaltung, Überwachung und Berichterstellung zu Aktivitäten verschiedener SecureSphere-Gateways
Manager of Managers	Verbindet Multi-Domain- und Multi-Tenant-Umgebungen, die mit mehreren MX Management-Servern implementiert werden