Trustwave®

# Trustwave WebDefend®

## WEB APPLICATION FIREWALL (WAF)

Trustwave WebDefend ist eine preisgekrönte, hoch skalierbare Web Application Firewall (WAF), die kontinuierliche Echtzeit-Sicherheit gegen Angriffe und Datenverlust bietet. WebDefend stellt sicher, dass Ihre Web-Anwendungen so arbeiten, wie sie sollen und wie es die Regularien vorschreiben.

WebDefend ist eine fortschrittliche Echtzeit-WAF, die individuelle, verhaltensbasierte Sicherheit für jede geschützte Anwendung bietet und mit unserem preisgekrönten Trustwave SIEM integriert ist, das Informationen über Angriffe aus vielen Quellen korreliert und konsolidiert.

WebDefend, als physische oder virtuelle Appliance implementiert*, bietet virtuelle Patches, um Ihre gefährdeten Anwendungen vor Angriffen zu schützen, ohne dass Sie auf den nächsten Release-Zyklus warten müssen. Nur WebDefend nutzt ein zum Patent angemeldetes Profilierungssystem und mehrere, gemeinsam arbeitende Erkennungs-Engines, um die Übertragung geschäftskritischer Daten sicher zu stellen und gleichzeitig umfassenden Schutz vor gezielten Angriffen zu bieten.

### Einfache Implementierung, robuste Leistung

WebDefend skaliert von einzelnen Anwendungen bis hin zum Einsatz in Großunternehmen:

- Die mehrstufige Architektur erlaubt getrennten Schutz und getrenntes Management mehrerer Rechenzentren
- Sensoren können für erhöhte Verfügbarkeit redundant eingesetzt werden
- Ein Einsatz out-of-line oder als transparente Inline-Bridge ist möglich, ohne dass Veränderungen an der Netzwerkkonfiguration oder ein Reverse Proxy notwendig wären
- Die Mandantenfähigkeit erlaubt es, mehrere Kunden oder Abteilungen in einer Appliance zu definieren und gleichzeitig zu gewährleisten, dass die Daten der verschiedenen Nutzer nicht vermischt werden – perfekt für komplexe Organisationen und Anbieter für Managed Security Services (MSSP)

Der WebDefend Manager ist optional verfügbar, um die Kontrolle und Berichterstattung von mehr als einem Sensor bzw. Rechenzentrum zu zentralisieren.

## Hauptfunktionen

Bietet den branchenweit besten Schutz vor Schwachstellen in Anwendungen und vor neu aufkommenden Gefahren. Dazu gehören beispielsweise die OWASP-Top-10-Angriffe auf Web-Anwendungen, Web Scraping/Harvesting, böswillige Bots, Google™ Hacking, Zero-Day- und gezielte Angriffe.

- Das zum Patent angemeldete Profilierungssystem für Anwendungen erstellt kontinuierlich ein dynamisches Sicherheitsmodell jeder geschützten Web-Anwendung, um zu gewährleisten, dass nur valider Traffic erlaubt wird
- Ermöglicht die Profilierung von HTML, XML und SOAP und die Überwachung komprimierten und unkomprimierten Traffics
- Die zum Patent angemeldete ExitControl Analyse-Engine prüft ausgehenden Traffic auf Datenlecks, Unleserlichkeit und Offenlegung von Sicherheitsinformationen
- Signaturen auf Anwendungsebene bieten aussagekräftige Informationen zu bereits erkannten Schwachstellen
- Geographische Sperrfunktionen bieten individuelle Sperrmöglichkeiten für Anfragen aus bestimmten Ländern
- Hoch skalierbare Sensoren decken verschiedenste Site-Definitionen und Einsatzoptionen ab und unterstützen Netzwerkkarten mit bis zu 10 GBit/s
- Erleichtert die Einhaltung der PCI-DSS-Anforderung 6.6
- Bietet verbesserte virtuelle Patches mit benutzerdefinierten Regeln, basierend auf der Mod-Security-Syntax
- Individuelle Antwortseite, um eine Kommunikations-verbindung zu einem potenziellen Hacker aufzubauen, je nach Art des eingeleiteten Angriffs

* Siehe WAF-Datenblatt für Details der physischen und virtuellen Appliance

## Sofortige Erkennung von Integritäts- und Sicherheitsproblemen

WebDefend führt eine ständige Bewertung Ihrer geschützten Anwendungen durch, um Probleme zu identifizieren, welche die Sicherheit, Funktionalität und Verfügbarkeit der Anwendung beeinträchtigen. Dazu gehören auch Programmierfehler, Anwendungsfehler und unsichere Codes.

## Virtuelle Patches

Virtuelle Patches ermöglichen Ihnen, mit benutzerdefinierten Regeln schnell auf Schwachstellen zu reagieren. Wenn Schwachstellen in einem regulären Anwendungs-Scan identifiziert werden, schützen virtuelle Patches sofort, während Ihre Entwicklungsabteilung den zugrunde liegenden Fehler beseitigt. Virtuelle Patches schützen gefährdete Anwendungen vor Angriffen, ohne dass Sie auf den nächsten Release-Zyklus warten müssen. WebDefend integriert sich mit den führenden Scannern für Web-Anwendungen.

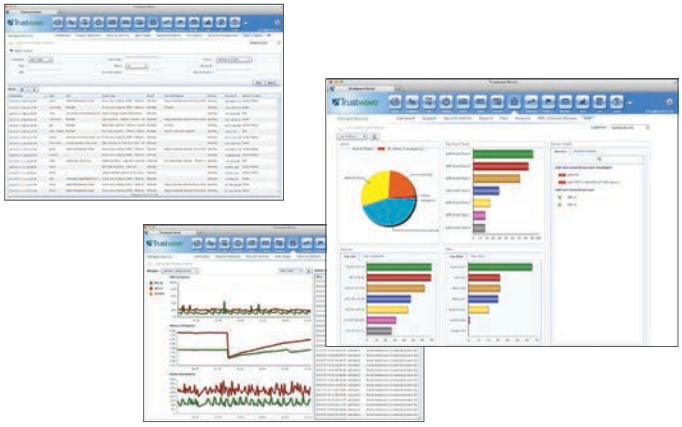
## Intuitive, informative Konsole

Die Management-Konsole bietet Ihnen die einfache Nutzung eines zentralen Punkts zur Konfiguration und Überwachung. Sie können die Konsole direkt ohne vorherige Schulung nutzen, um einen vollständigen Einblick in die Architektur und Sicherheit der Web-Anwendungen zu erhalten.

Die Konsole unterstützt Sie dabei, den Kontext von Ereignissen zu verstehen, um schnell Abhilfe zu schaffen. Zu jedem Ereignis und jedem erkannten Fehler zeigt eine detaillierte Beschreibung das Problem auf, gibt einen Einblick in die Bedeutung und erklärt die Lösung. Die Konsole bietet mehrere Ereignisansichten und Drill-Down-Fähigkeiten, die Ihnen die einfache Identifikation von Ereignissen, die Untersuchung der Gründe, die Betrachtung ganzer Transaktionen und einen Blick auf die Fehlermeldungen ermöglichen, die Besucher Ihrer Seite zu sehen bekommen. Leistungsfähige Reporting-Tools melden Sicherheitsprobleme der Anwendungsentwicklung und dem Führungspersonal, helfen bei der Einhaltung von Compliance-Anforderungen und verfolgen die Effektivität der WebDefend-Richtlinien.

## Performance-Monitoring von Web-Anwendungen

WebDefend bietet Ihnen Echtzeit-Transparenz über die Leistung Ihrer Web-Anwendungen. WebDefend Application Performance Management identifiziert Probleme und Trends auf Site-, URL- und Session-Ebene in der Web- Anwendungsumgebung – alles mit Echtzeitansichten zu den Leistungsdaten. Da WebDefend die Web-Anwendungen automatisch profiliert, müssen Sie keine Anwendungsstrukturen oder -pfade festlegen.



# Technische Spezifikationen

- Geschützte Protokolle: HTTP, HTTPS (SSL), XML, Web-Dienste, SOAP und AJAX
- Warnungs- und Überwachungsoptionen: E-Mail, Syslog, individuelle SNMP-Alerts, Ereignisanzeige, Dashboard und integriertes Reporting
- Sperroptionen: Inline-Einsatz, TCP-Reset, Webserver-Agent, Benutzerabmeldung, Firewall und andere Geräte
- Sprachen: Unterstützt die Sammlung und Analyse des Traffics von Web-Anwendungen in jeder Sprache, einschließlich Double-Byte-Sprachen
- Unterstützt VLAN-IDs
- Unterstützt Remote-Authentifizierung über LDAP-2 oder LDAP-3 für Konsolenbenutzer

## Integration mit Trustwave SIEM

WebDefend integriert sich sicher mit den Trustwave Security Information and Event Management (SIEM)-Lösungen. Die Integration mit Trustwave SIEM ermöglicht die Korrelation der WebDefend-Ereignisse mit Ereignissen, die von anderen Systemen erfasst werden – etwa Network Access Control oder Data Loss Prevention – unabhängig davon, ob diese von Trustwave oder einem Dritten stammen. Dies vereinfacht die Absicherung und erlaubt eine schnellere Reaktion auf Bedrohungen.

# Hauptvorteile

Bietet unerreichten Schutz gegen den Verlust sensitiver Informationen.

## Transparenz

Das zum Patent angemeldete Profilierungssystem und die gemeinsam arbeitenden Erkennungs-Engines gewährleisten die geschützte Übertragung Ihrer geschäftskritischen Daten, bieten branchenweit die einzige Korrelation ein- und ausgehender Ereignisse und helfen dabei, die Integrität der Anwendungen zu wahren.

## Niedrigste Total Cost of Ownership (TCO)

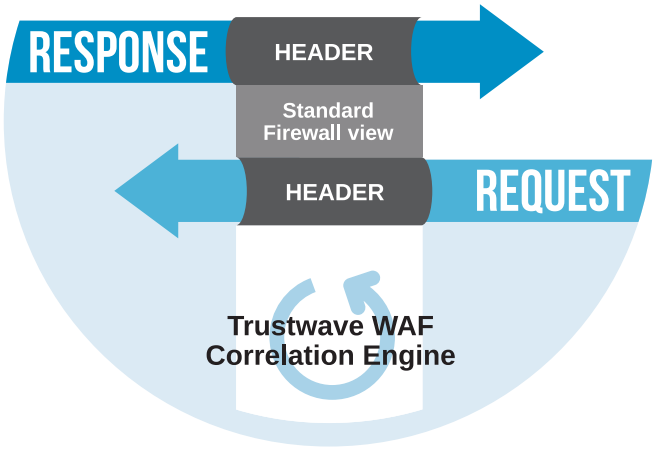
Bietet automatische und stets aktuelle Profile Ihrer Web-Anwendungen, um maximale Sicherheit bei minimalem Verwaltungsaufwand zu liefern.

## Flexibilität

Dank der einfachen Nutzung können Sicherheitsereignisse und Schwachstellen mithilfe einer intuitiven Konsole identifiziert werden, die eine zentrale Stelle zur Konfiguration und Überwachung darstellt - wahlweise für eine Appliance vor Ort (als Hardware oder virtuell) oder für einen Managed Security Service, der rund um die Uhr Analysen durch unsere Trustwave-Experten bietet.

# Minimales Risiko mit einer Application-Lifecycle-Lösung

Das Trustwave 360-Application-Security-Programm gewährleistet Sicherheit als Grundpfeiler der Software-Entwicklung und des laufenden Betriebs, indem es branchenführende, robuste Services und Technologien zum Schutz geschäftskritischer Anwendungen und sensitiver Daten bereitstellt, darunter: Schulungen zur sicheren Entwicklung, Penetration-Test für Anwendungen, Prüfungen des Anwendungs-Codes und unsere Web-Application-Firewall-Lösungen. Zusammen bieten diese Module einen ganzheitlichen Ansatz für die Sicherheit Ihrer Anwendungen.




## Global Event Manager (GEM)

Der GEM ermöglicht die Echtzeitüberwachung und -analyse von Ereignissen des Akamai WAF Service und von ModSecurity, zusammen mit den Ereignissen von WebDefend, in der Management-Konsole und erlaubt den Betrieb verteilter Architekturen zum tiefgreifenden Schutz von Cloud-Rechenzentren.

## Service-Optionen

- Der Standard-Support umfasst Unterstützung per E-Mail und Telefon während der lokalen Geschäftszeiten sowie alle Produkt-Updates.
- Der Premium-Support umfasst Unterstützung per E-Mail und Telefon rund um die Uhr, eine einjährige Hardware-Garantie und einen 24-h-Austauschservice für die WebDefend Hardware-Appliance sowie alle Produkt-Updates.
- Vor-Ort-Installation, erweiterte Hardware-Garantie und Professional Services sind zusätzlich verfügbar.

# Preisgekrönte Lösung

Trustwave WebDefend® ist nach Common Criteria der Zertifizierungsstufe EAL 2+ validiert.

# Optionale Module

## WebDefend Manager

Der WebDefend Manager fasst Sicherheitsereignisse und Fehler zusammen und bietet eine zentrale Kontrollinstanz für mehrere lokale und entfernte Sensoren.

## Hochverfügbarkeit

Ein Hochverfügbarkeitseinsatz bietet Redundanz für Sensoren und WebDefend Manager, lokal und im Rechenzentrum, um ständige Sicherheit für Web-Anwendungen zu gewährleisten.

**WEITERE INFORMATIONEN FINDEN SIE UNTER TRUSTWAVE.COM**

Trustwave ist ein führender Anbieter von Sicherheitslösungen für Compliance, Web-, Anwendungs-, Netzwerk- und Datensicherheit, die als Cloud, Managed Security Services, Software und Appliance zur Verfügung stehen. Organisationen, die sich mit dem heutigen, fordernden Sicherheitsumfeld auseinander setzen müssen, erhalten von Trustwave einen einmaligen Ansatz mit umfassenden Lösungen, die das TrustKeeper®-Portal und andere proprietäre Sicherheitslösungen umfassen. Trustwave hat bereits hunderten Organisationen, von Fortune-500-Unternehmen und großen Finanzinstitutionen bis hin zu kleinen und mittleren Einzelhändlern, geholfen, ihre Compliance zu managen und die Netzwerkinfrastruktur, Kommunikation und geschäftskritische Datenbestände zu schützen. Trustwave hat seinen Hauptsitz in Chicago und weltweite Filialen.

Trustwave®

Weitere Informationen finden Sie unter www.trustwave.com



MIDS_PCI3.1_1015