

# Secure Web Gateway

## MOBILE MALWARE UND BYOD

Das Trustwave Secure Web Gateway (SWG) bietet einen einzigartigen Lösungsansatz, mit dem es in Echtzeit vor Bedrohungen der aktuellen Generation schützt. Durch die akkurate Erkennung zielgerichteter Angriffe vermeidet diese Lösung sowohl eine unnötige als auch eine unzureichende Blockierung von Inhalten. Dieses Modell erlaubt es den Anwendern, das Internet zugleich sicher und produktiv zu nutzen. Mit den flexibelsten Einsatzmöglichkeiten am Markt integriert sich das SWG auf einfache Weise in bestehende Infrastrukturen und bietet dabei maximalen Schutz für alle Anwender, unabhängig von deren Verbindung oder Standort.

### Hauptfunktionen

- Mehrschichtige Anti-Malware-Engine
- Produktivitätskontrollen für Web 2.0
- Fortschrittliche Anwendungs- und Betriebskontrollen
- Robuste Einsatzmöglichkeiten
- Flexible Tools für Richtlinien
- Detaillierte, individualisierbare Berichte
- Benutzerauthentifizierung und -identifikation
- Web-Filter
- Data Loss Prevention auf höchstem Niveau
- Prüfung und Validierung SSL-verschlüsselter Daten

### Überblick

Organisationen, die die Vorteile des Web und der sozialen Medien sicher nutzen möchten, schützen sich mit dem Trustwave Secure Web Gateway (SWG) gegen dynamische, komponentenübergreifende Malware-Bedrohungen. Verwirklicht wird dieser Schutz mittels patentierter Code-Analyse in Echtzeit, die den Aufbau einer Webseite vollständig untersucht.

Trustwave ist damit der einzige Web Security-Anbieter, der mit einer einzigen Lösung effektiv gegen dynamische und komponentenübergreifende Web-2.0-Bedrohungen schützt. Mit dem Trustwave SWG können Organisationen sicher auf Web-2.0-Anwendungen zugreifen, das Risiko einer Verletzung der Datensicherheit verringern und ihre Produktivität optimieren.

Das Trustwave SWG ist das zurzeit vielseitigste und kosteneffizienteste Web-Gateway am Markt, das mit seinen flexiblen Einsatzoptionen all Ihre unternehmerischen Anforderungen erfüllt.



### Hauptvorteile

#### Intelligenter Malware-Schutz

Die mehrschichtige Anti-Malware-Engine umfasst intelligente Technologien, die Malware der jeweils aktuellsten Generation erkennen und blockieren, auch wenn diese andere Sicherheitslösungen passieren konnte. Dieses Merkmal hilft bei der Aufrechterhaltung der Produktivität, verringert kostenintensive Maßnahmen wie Desktop-Re-Imaging und -Bereinigung und schützt Daten vor Diebstahl durch trojanische Pferde und Spionageprogramme.

#### Sichere und produktive Web 2.0-Nutzung

„Granular Social Media Control“, kombiniert mit der mehrschichtigen Anti-Malware-Engine, erlaubt es den Anwendern, sicher auf Web 2.0 und soziale Medien zuzugreifen. Über Malware-Infektionen, Datenlecks und Produktivitätsverluste müssen sich Ihre Mitarbeiter dann keine Gedanken mehr machen.

## Sicherheit für alle Anwender, unabhängig von Standort und Verbindung

Mit den Einsatzmöglichkeiten als klassische Appliance, virtuelle Appliance oder als Hybridlösung (vor Ort und Cloud-basiert) erweitert das Trustwave SWG Sicherheitsmaßnahmen und Richtlinienkontrolle auf mobile und remote zugreifende Anwender.

## Gemeinsame Lösung für Sicherheit, Richtlinienkontrolle und Berichte

Unabhängig von der gewählten Einsatzoption können Unternehmen ihre Sicherheitseinstellungen und Berichte bequem und einfach über eine einzige, zentrale Schnittstelle verwalten.

## Compliance mit Regularien und Acceptable Use Policy

Das einfache, aber robuste Reporting-System des SWG vereinfacht die Nachverfolgung und Analyse potentieller Richtlinien- und Regelverstöße. Da das Trustwave SWG Datenverluste verhindert, garantiert es die Compliance zu Vorschriften, die Datensicherheit und -integrität fordern. Dabei erlaubt der flexible Mechanismus zur Durchsetzung von Policies und Regeln die Anpassung an verschiedenste Regularien.

## Eine bezahlbare Lösung mit niedrigen Total Cost of Ownership (TCO)

Die Optionen, die das SWG zur Senkung der Gesamtkosten bietet, umfassen bequeme, flexible Einsatzmöglichkeiten, einfache Wartung, Skalierbarkeit, anpassbare Malware- Erkennung und -Abhilfe, ein zukunftssicheres Design und zentralisiertes Management. Diese Funktionalitäten bieten maximalen Nutzen bei niedrigen TCOs.

## Erweiterte Integrationsoptionen

ICAP RESPMOD (Response Modification) und ICAP REQMOD (Request Modification) erlauben es dem Trustwave SWG, mit jeglichen ICAP-Servern und -Clients zu kommunizieren. ICAP (Internet Content Adaption Protocol) ist ein einfaches Protokoll, um einen „Remote Procedure Call“ für HTTP-Daten auszuführen. ICAP wird häufig dafür genutzt, Systemfunktionen zu ergänzen und so die Anbindung von DLP-Software oder Virenscannern zu ermöglichen. Das System lässt sich außerdem um interne Syslog-Funktionen erweitern, um Log- Daten an das SIEM-System von Trustwave weiterzugeben.

## Belastbare, flexible und einfache Berichte

Das Trustwave SWG umfasst ein vollständiges Out-of-the-Box-Reporting. Zusätzliche Berichtsfunktionen können mit dem Trustwave Security Reporter in das Trustwave SWG integriert werden, um umfangreiche und dennoch einfach zu nutzende Berichte (aus Vorlagen oder individuell), Echtzeit-Dashboards und weitere Informationen für verschiedene Empfänger zusammen zu stellen.

## Verbesserter Schutz vor Bedrohungen

### Code-Analyse in Echtzeit

Mit der Echtzeit-Code-Analyse können Kunden fortschrittliche, dynamische Malware präzise und akkurat erkennen und abwehren. Ein- und ausgehende Web-Kommunikation wird im Moment des Auftretens dynamisch analysiert und durch mehrere Malware-Engines betrachtet, um die Absicht festzustellen. Diese Engines laufen parallel und bieten so die schnellste und genaueste Erkennungsleistung am Markt, was Latenzen minimiert und Ungenauigkeiten, wie sie bei anderen Sicherheitslösungen auftreten, praktisch eliminiert.

- Erkennt und blockiert fortschrittliche, dynamische Malware aus Cross-Component-Angriffen
- Extrem genaue Erkennung schädlichen Codes auf HTTP- und HTTPS-Webseiten
- Schnelle Erkennung und Mängelbeseitigung für produktiven Web-(2.0-)Einsatz
- Umfassende Analyse von Webseiten auf Einzel- und Mehrkomponentenangriffe
- Verfolgt ausgehenden Verkehr, um die Kommunikation eines Trojaners zu seinem steuernden Server zu erkennen

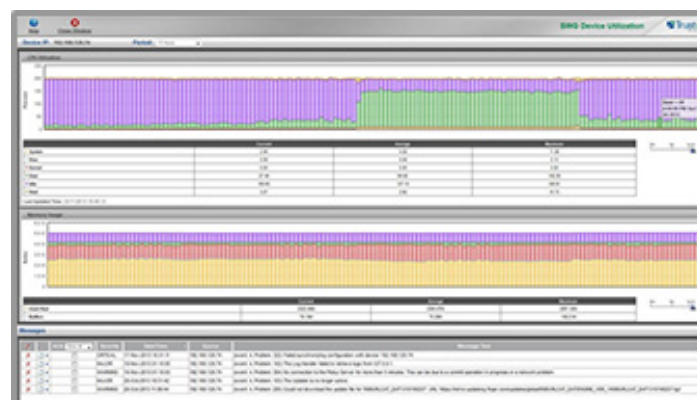
## Sofortschutz

Anstatt schädliche Inhalte zu blockieren, die einem gewissen Muster, einer Signatur oder einem Algorithmus entsprechen, blockiert Vulnerability Anti.dote von Trustwave schädliche Inhalte, die versuchen, bekannte Schwachstellen auszunutzen (indem Schwachstellen erkannt werden, bevor ein Patch aufgespielt wird) – und eliminiert so die Angriffsfläche für den Schadcode. Dies ist die einzige Technologie, die echten Sofortschutz gegen bisher unveröffentlichte Schwachstellen bietet.

## Data Loss Prevention

Mit „Granular Social Media Control“ können Unternehmen den Zugang zu Social-Media-Webseiten bedenkenlos freigeben, da Beiträge, Kommentare und Uploads überwacht und kontrolliert werden. Zusätzlich ist das Trustwave SWG die beste Lösung zum Schutz vor komplexen Angriffen, die für den Datendiebstahl entwickelt wurden. Das bedeutet zusätzlichen Schutz für Ihre sensiblen Daten. Diese Kombination aus genauer Kontrolle und fortschrittlichem Schutz verhindert Datenverluste, setzt Richtlinien zum Umgang mit vertraulichen Informationen durch, wahrt Compliance zu datenbezogenen Richtlinien und schützt sensible Informationen zu schützen. Wer bereits DLP einsetzt, kann Trustwave SWG als vollständigen ICAP-Proxy nutzen und damit die Kommunikation mit einer DLP-Lösung seiner Wahl herstellen.

## Produktivität



## Anwendungskontrolle

Mit dem Trustwave SWG werden Kosten, die durch übermäßige Bandbreitennutzung und Schadensbehebung nach Malware-Angriffen auf Desktop-PCs anfallen, drastisch reduziert. Die Trustwave Granular Social Media Control erlaubt es Organisationen, all jenen vollen Web-Zugriff zu geben, die ihn benötigen. Gleichzeitig lassen sich Beiträge, Kommentare und Uploads blockieren, die von Unbefugten auf Seiten wie Facebook oder LinkedIn geladen werden.

## Globale Richtlinienkontrolle

Das Trustwave SWG erweitert das vor Ort gewohnte Sicherheitsniveau einschließlich der Richtlinienkontrolle auf den Bereich mobiler Mitarbeiter und Filialen. Damit wird konsistenter Echtzeitschutz vor dynamischen Internet-Bedrohungen umgesetzt, unabhängig vom Aufenthaltsort der Anwender.

## Trustwave Web-Filter-Liste

Trustwave Web Filtering bietet Kunden eine marktführende Filtertechnologie mit über 100 Kategorien zur Durchsetzung einer granularen Acceptable Web Use Policy.

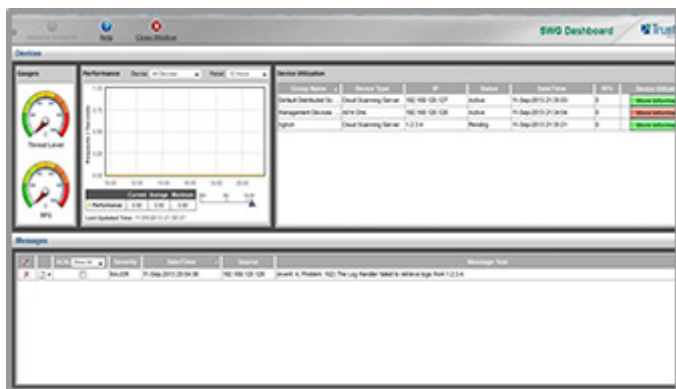
## Caching/Beschleunigung von Inhalten

Die Beschleunigung von Inhalten mit integrierten Cache-Funktionalitäten bietet Anwendern eine kurze Ladezeit von Webseiten bei gleichzeitigem Schutz vor schädlichen Inhalten. So wird die Arbeit sicherer und effektiver zugleich.

## Management

### Berichte

Der Trustwave Security Reporter ist eine schnelle, hoch leistungsfähige Lösung für Sicherheitsberichte. Sie erfasst den Web-Verkehr einer Organisation vollständig und erlaubt Organisationen die Analyse von Trends bei der webgestützten Kommunikation, um Mängel zu beheben, pro-aktive Benachrichtigungen zu verschicken und Sicherheitsanalysen kritisch zu prüfen. Der Security Reporter bietet die breiteste Palette entsprechender Datenverarbeitung, die zurzeit erhältlich ist.



## Compliance mit brancheninternen und behördlichen Vorschriften

Kunden benötigen Lösungen, die Compliance mit brancheninternen und behördlichen Vorschriften nachweisbar machen. Der Trustwave Security Reporter bietet hierzu eine einfache Schnittstelle, konsolidierte Gefahrenüberwachung und eine Verlaufsfunktion mit einer überragenden Archivkapazität von bis zu 12 TB.

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 auseinandersetzen müssen, erhalten von Trustwave einen einmaligen Ansatz mit umfassenden Lösungen, die das TrustKeeper®-Portal und andere proprietäre Sicherheitslösungen umfassen. Trustwave hat bereits hunderte Organisationen, von Fortune-500-Unternehmen und großen Finanzinstitutionen bis hin zu kleinen und mittleren Einzelhändlern, unterstützt, ihre Compliance zu managen und die Netzwerkinfrastruktur, Kommunikation und geschäftskritische Datenbestände zu schützen. Trustwave hat seinen Hauptsitz in Chicago und weltweite Filialen.

## Flexible Einsatzoptionen

Der Scan-Server des Trustwave SWG ist für eine Vielzahl von Plattformen verfügbar, darunter die klassische Appliance, die virtuelle Appliance, die Cloud-basierte virtuelle Appliance und der virtuelle Appliance-Plattform-Service.

Diese Plattformoptionen können in einer Hybrid-Umgebung kombiniert werden, was zwei wichtige Vorteile bietet: Die volle Sicherheit kann auf entfernte und mobile Anwender ausgedehnt werden und die Flexibilität der Architektur erlaubt eine enge Anpassung an die bestehende Netzwerkinfrastruktur, die geographische Verteilung und die Kosten- und Ressourcen-Anforderungen des Unternehmens.



„Das SWG bietet eine einzigartige und äußerst effektive Palette an Sicherheitsmaßnahmen gegen Internet-Bedrohungen. Es lässt sich einfach einrichten und konfigurieren; in der neuesten Version sind einige nützliche Funktionen hinzugekommen, darunter das stark verbesserte Reporting“

—Dave Mitchell, SC Magazine UK

## Secure Web Gateway, Mobile Malware und BYOD

Das Secure Web Gateway (SWG) ist ein integraler Bestandteil der Mobile-Security-Lösung von Trustwave. Trustwave sichert Ihre BYOD-Umgebung mit einer Kombination integrierter Security-Technologien für Netzwerke, Anwender und Daten. Erfahren Sie mehr unter: [www.trustwave.com/mobilesecurity](http://www.trustwave.com/mobilesecurity).