

## hyperguard und ZXTM: Web Application Firewalling und Load Balancing der nächsten Generation

Kundenportale, Online-Shops oder Internet-Filialen von Banken sind verwundbar: Angriffe wie SQL-Injection, Cross Site Scripting oder Session Hijacking zielen auf Schwachstellen in den Web-Anwendungen selbst – und nicht auf der Netzwerk-Ebene. Das eigentliche Angriffsziel bleibt aber gleich: Ihre vertraulichen Unternehmensinformationen.

Mit ZXTM und hyperguard können Sie Ihren gesamten Web Application Traffic managen und schützen - mit der hochperformanten Web Application Firewall (WAF) von art of defence und Zeus. hyperguard ist ein Plug-In für ZXTM. Da beide Produkte rein software-basiert sind, lassen sie sich einfach zu einer kompletten und leicht zu bedienenden Lösung integrieren. Diese bietet Ihnen höchste Flexibilität: Sie können sie heute auf dem schnellsten Server in Ihrem Rechenzentrum einsetzen – und jederzeit später auf einen noch schnelleren migrieren. Sogar der Einsatz in virtuellen Umgebungen, wie z.B. VMware Virtual Infrastructure 3 oder Windows Server 2005 R2 ist möglich. Und eine rein software-basierte Lösung kostet Sie weder Platz noch Strom, wenn sie gerade nicht in Betrieb ist.

### Was ist ZXTM?

Zeus Extensible Traffic Manager (ZXTM) verwaltet Ihren Applikationsverkehr, indem es Anfragen analysiert, transformiert und so innerhalb der Applikationsinfrastruktur weiterleitet, dass die Last gleichmäßig verteilt wird. Mit der leistungsstarken TrafficScript™ Engine können Sie die für Ihr Unternehmen am besten geeigneten Traffic-Management-Regeln implementieren und schöpfen so den gesamten Funktionsumfang von ZXTM optimal aus.

### Was ist hyperguard?

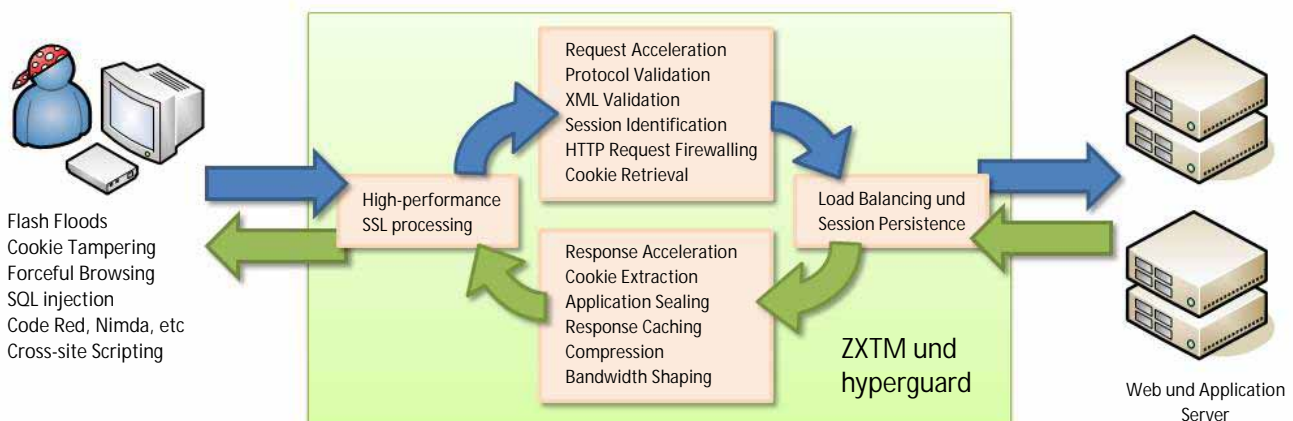
Die Web Application Firewall hyperguard schützt Ihre Unternehmensinformationen umfassend gegen Angriffe auf Web-Anwendungsebene, erfüllt höchste Anforderungen im Enterprise-Markt – und ergänzt Ihre bestehende Sicherheitsinfrastruktur optimal und komplementär.

hyperguard identifiziert und klassifiziert Requests und verhindert unberechtigten Zugriff auf die hinter den Web-Anwendungen liegenden Datenbanken und operativen Systeme – auch während laufender Transaktionen, wenn diese Systeme offen und damit angreifbar sind.

### Compliance & Security – ohne Nebenwirkungen für berechnete User

Egal ob Handel, Finanzbereich, öffentlicher Sektor oder SaaS (Software as a Service), Online-Dienste benötigen den höchsten Sicherheits-Standard, um gegen gezielte Hacker-Angriffe oder Traffic Floods gewappnet zu sein - tatsächlich gegen jede Art von Diebstahl, Manipulation oder Zerstörung vertraulicher Information. Neueste Richtlinien, wie z.B. der PCI Data Security Standard der Kreditkarten-industrie, sehen hier den Einsatz einer Web Application Firewall zusätzlich zur bestehenden Load Balancer- und Netzwerk-Firewall-Infrastruktur als Best Practice vor.

Kombiniert man die WAF von art of defence mit dem leistungsstarken TrafficScript™ von ZXTM, kann man sehr einfach Regeln dafür erstellen, ob und wie sich der Traffic in Ihr Netzwerk hinein- und hinausbewegt – und wie er sich in Ihrem Netzwerk verhalten soll. Um keine sensiblen Daten preiszugeben, können sogar URL-Inhalte überschrieben werden.



Datendiebe und Hacker haben in ZXTM und hyperguard ihren Meister gefunden.

Die Kombination von Zeus' leistungsstarker Traffic-Management-Technologie und der Enterprise Web Application Firewall von art of defence schafft eine einzigartige Lösung, die Web-Anwendungen aller Art gegen ein breites Spektrum von bekannten Angriffen und auch „Zero-Day-Attacks“ absichert und Datenverlust verhindert – und gleichzeitig wird der Traffic beschleunigt und die Last so verteilt, dass die Online-Dienste jederzeit verfügbar bleiben.

#### Hauptvorteile

Mit ZXTM und hyperguard erhalten Sie die europäische „Best-of-Breed“-Lösung für:

- Applikations-Beschleunigung
- Applikations Sicherheit
- Service Level Monitoring
- Automatische Failover und Health Checks
- Beschränkung von Transaktionen und Requests
- „Unsichtbarkeit“ von Daten-Formaten, auch im unwahrscheinlichen Fall, dass eine Applikation gehackt wurde
- Off-loading von rechenintensiven Aufgaben wie SSL, HTTP und XML
- Content Caching

#### Typische Einsatzszenarien

- Absicherung von Diensten gegen Datenverlust und 'Flash-Floods'
- Verhinderung von Cookie Manipulationen und Forceful Browsing
- Verhinderung von SQL-Injection, Cross-Site-Scripting-Angriffen u.ä.
- Absicherung von Websites durch URL-Verschlüsselung
- Site Usage Enforcement

#### art of defence im Überblick:

Die art of defence GmbH ist das europaweit einzige Unternehmen, das Sicherheits-Produkte für Web-Anwendungen über den gesamten Applikations-Lebenszyklus anbietet. Führende Banken, Finanzdienstleister und E-Commerce-Unternehmen setzen beim Schutz ihrer internen und externen Web-Anwendungen auf art of defence und erfüllen so Gesetzesauflagen und Industrie-Standards wie die Sicherheitsrichtlinien der Kreditkartenindustrie (PCI-Compliance).

Das Web Source Code Analyse-Tool hypersource erkennt die genaue Lage von Schwachstellen im Quell-Code von Web-Anwendungen mittels automatisierter statischer Analyse. Es unterstützt CIOs, Sicherheitsverantwortliche und Entwickler rollenbasiert durch Status-Berichte und detaillierte Vorschläge zur Behebung der entdeckten Schwachstellen – ohne clientseitige Installation, nur über einen Webbrowser.

Für den Schutz produktiver Web-Anwendungen bietet art of defence hyperguard, die Enterprise Web Application Firewall (WAF) der zweiten Generation. Mit ihr definieren Security-Verantwortliche das Verhalten von Web-Applikationen nach außen und können so Manipulationen und unberechtigte Zugriffe auf die hinter den Web-Anwendungen liegenden Datenbanken und operativen Systeme verhindern.

Für weitere Informationen senden Sie bitte eine Email an [sales@artofdefence.com](mailto:sales@artofdefence.com) oder besuchen Sie unsere Website: [www.artofdefence.com/en](http://www.artofdefence.com/en)

**Download einer kostenlosen Test-Version von hyperguard unter:**  
<https://mydefence.artofdefence.com/register/>

#### Zeus im Überblick:

Zeus Technology hat einen wohlverdienten Ruf dafür, robuste, sichere und skalierbare Traffic-Management-Lösungen für Unternehmen vieler Branchen anzubieten wie z.B. Medien- und Content-Anbieter, Telekommunikations- und Hosting-Unternehmen, Online-Händler sowie Organisationen aus dem Finanz-, Bildungs- und Behördenumfeld.

Zeus ist in einer einzigartigen Position, jedem Unternehmen zu helfen, das seine geschäftskritische Internet-Infrastruktur verbessern will. Denn Zeus kann die Erfahrungen von Kundenbeziehungen mit so unterschiedlichen Organisationen wie Federal Railroads Administration, NEC, British Telecom, PLAY.COM, Telewest, Thus Plc., TD Waterhouse, Telecom Italia Mobile, Ciao Group, We Energies und Paxonix einbringen.

Für weitere Informationen besuchen Sie bitte unsere Website unter <http://www.zeus.com>

Weitere Informationen erhalten Sie per Email: [info@zeus.com](mailto:info@zeus.com) - unter [www.zeus.com](http://www.zeus.com) finden Sie auch die Kontaktdaten des nächsten Zeus-Büros.

**Laden Sie eine kostenlose Test-Version von ZXTM herunter!** Überzeugen Sie sich selbst und testen Sie ZXTM kostenlos. Als reine Software ist ZXTM einfach herunterzuladen.

**Gehen Sie dazu auf unsere Homepage unter:**  
[www.zeus.com/downloads](http://www.zeus.com/downloads)  
Technischer Support steht Ihnen während Ihrer Test-Phase zur Verfügung.

Zeus Technology Limited (UK)  
The Jeffreys Building  
Cowley Road  
Cambridge CB4 0WS  
United Kingdom  
Sales: +44 (0)1223 568555  
Main: +44 (0)1223 525000  
Fax: +44 (0)1223 525100  
Email: [info@zeus.com](mailto:info@zeus.com)  
Web: <http://www.zeus.com/>

Zeus Technology, Inc. (U.S.)  
1955 Landings Drive  
Mountain View  
CA 94043  
United States of America

Phone: 1-888-ZEUS-INC  
Fax: 1-866-628-7884  
Email: [info@zeus.com](mailto:info@zeus.com)  
Web: [www.zeus.com](http://www.zeus.com)