DATASHEET

DEFIANCE TMS
Web Application Threat Management

HACKER SAVVY. ENTERPRISE SMART.

Defiance™ TMS is the first comprehensive threat management system to support large-scale deployment of Web application and Web services security for the distributed enterprise.

WEB APPLICATION SECURITY: THE ENTERPRISE CHALLENGE

Enterprises across multiple industries—ranging from financial services to healthcare, government, and manufacturing—are increasingly moving their critical applications online. Web applications and Web services bring tremendous economic advantages, but they also bring increased security risks. Traditional security measures—such as network intrusion prevention systems and firewalls—fail to prevent attacks at the application layer, leaving sensitive customer and corporate data and information assets exposed to business and compliance risks. A security breach can temporarily shut down business operations and cause irrecoverable damage to reputation, customer confidence, and brand value.

Web application security can protect organizations from attacks to their most critical Web-based applications. However, addressing the vulnerabilities of a single application or a single location is not enough, since hackers usually instigate multiple probes across the enterprise before identifying points of weakness. Organizations need a Web application security solution that can be managed centrally but broadly deployed across applications, locations, user roles, and businesses. This solution must be coordinated so that an attack at one location triggers a rapid response across the rest of the organization. Scalability and performance are also key to ensuring that security measures do not impact productivity or operational performance.

TAKING WEB APPLICATION SECURITY TO THE NEXT LEVEL

Defiance TMS is the first comprehensive threat management system to support large-scale deployment of Web application and Web services security for the distributed enterprise. It incorporates scalable intrusion detection and prevention systems that work seamlessly to detect threats, generate alerts, and block both internal and external attacks against critical corporate data without impacting day-to-day operations.

BUSINESS VALUE

- **Protect valuable corporate intellectual property and assets**
- **Control regulatory, legal, and audit exposure**
- **Maintain credibility with consumers and the business**
- **Reduce downtime and lost transactions from security breaches**

TECHNOLOGY BENEFITS

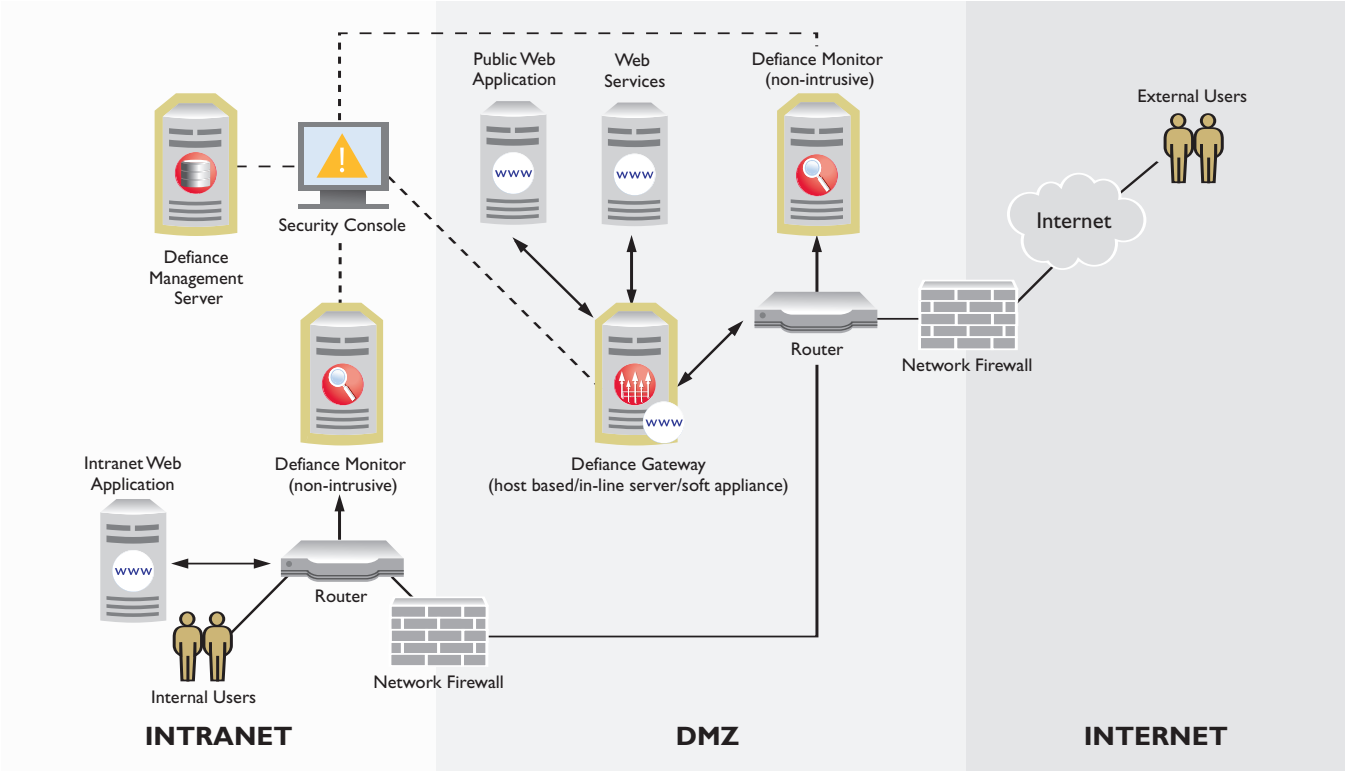
- **Positive and negative security models provide maximum attack protection**
- **Intelligent Escalation maximizes security without impacting normal operations**
- **Scalable solution supports the distributed enterprise**
- **Defiance Security Console provides centralized management and control across organizational roles**
- **Platform supports existing IT infrastructure and integrates with leading Enterprise Management Systems**
- **Out-of-the-box security policies enable rapid deployment**

DEFIANCE TMS OVERVIEW

Defiance TMS (Threat Management System) consists of four major components that together provide a scalable, manageable solution for securing Web applications:

- **The Defiance Monitor Web application Intrusion Detection System (IDS)**
- **The Defiance Gateway Web application Intrusion Prevention System (IPS)**
- **The Defiance Management Server, a centralized repository of Web application security data and logs**
- **The Defiance Security Console for unified administration, management, reporting, and forensics**

Defiance Gateways and Monitors leverage patent-pending Intelligent Escalation™ technology and work in unison across the distributed enterprise to intelligently detect and block internal and external attacks to Web applications without impacting operational performance. The centralized Security Console and Management Server support scalable deployment of Defiance Gateways and Defiance Monitors across multiple applications and locations while providing critical real-time and historical data for decision-making.



INTELLIGENT ESCALATION TECHNOLOGY

Defiance Gateways are deployed in-line for intrusion prevention, while Defiance Monitors are deployed out-of-band for continuous intrusion detection. They offer multiple modes of operation:

- In ***Bypass Mode***, Defiance Gateways and Monitors allow traffic to pass through with zero performance impact
- In ***Passive Mode***, they examine inbound and outbound traffic to detect security violations
- In ***Active Mode***, Defiance Gateways provide full intrusion prevention to immediately detect threats, generate alerts, and block attacks

Kavado's Intelligent Escalation technology grants superior control over Web application security. It allows organizations to establish policies that trigger the escalation of Defiance Gateways and Monitors across the enterprise. For example, an organization could deploy Defiance Gateways and Monitors in Bypass or Passive Modes to optimize operational performance and capacity until there is reason to believe the enterprise is under attack. Intelligent triggers can then immediately escalate the security posture proportionally to the estimated level of risk, configuring all Defiance Monitors into Passive Mode and all Defiance Gateways into Active Mode.

This unprecedented intelligence provides organizations with maximum flexibility in weighing the tradeoffs between business needs, operational performance, and information risk. It also ensures that an attack against a single location triggers rapid and appropriate responses throughout the distributed enterprise.

MAXIMUM ATTACK PROTECTION

Distributed Threat Management

Defiance TMS provides intelligent threat management with real-time intrusion detection and prevention to protect enterprise information assets across the organization. With Kavado's Intelligent Escalation technology, a violation of security policies at one location can escalate the readiness of Defiance Gateways and Monitors in other locations. This ensures comprehensive enterprise-wide control and rapid response to attacks.

Both Positive and Negative Security Models

Defiance TMS implements a positive security model that explicitly defines acceptable application behavior and automatically blocks any behavior that deviates from policy, providing reliable protection without the need for continual updates or new attack signatures. It also supports a negative security model to ensure that fields that can be defined by custom patterns—such as Social Security numbers, major credit card numbers, check routing numbers, user ID codes, or account codes—can be automatically blocked or masked to prevent theft.

Out-of-The-Box Protection

Default security policies eliminate major threat categories and provide instant protection for popular enterprise, custom, and third-party applications.

ENTERPRISE-CLASS SCALABILITY AND INTEGRATION

Simplified, Centralized Management and Control

The Defiance TMS Security Console provides simplified and centralized management, fast-and-efficient policy refinement, and detailed dashboard and server statistics for all Defiance Monitors and Gateways across the enterprise. It offers access to both real-time activity and historical information captured by a centralized Defiance Management Server, and allows the enterprise to provide distinctive security analysis and reports based on the needs of various user roles within the organization.

Modular, Flexible Architecture

Defiance TMS application security management solutions are designed to work with existing security, network, and enterprise IT management infrastructure. Defiance Gateways can be deployed on a separate server or on the application server itself based on the needs of the enterprise. The highly flexible Event Publisher supports ODBC, SNMP traps, syslogs, and text files, allowing the enterprise to automatically relay security events into Enterprise Management System (EMS) applications for centralized aggregation, control, and insight into operations. The Event Publisher also supports industry-leading EMS platforms including those offered by Symantec and IBM Tivoli. Defiance TMS is a software solution that runs on any supported Linux, Windows, or Sun server. Defiance Gateway and Monitor can also be deployed as soft appliances (Defiance Gateway Plus and Defiance Monitor Plus).

SECURITY CONSOLE

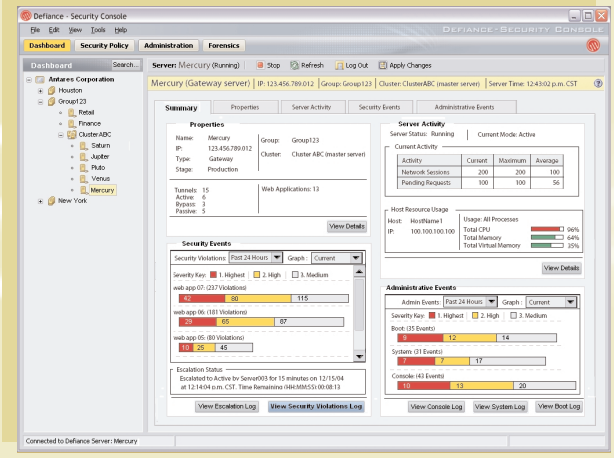
The Security Console provides centralized administration, management, reporting, and forensics for all Defiance Gateways and Monitors across the enterprise. This information is presented through four views based on the individual's role in the organization:

The Admin View allows IT and/or security personnel to physically configure Defiance Monitors and Gateways. They can also establish and manage user privileges for viewing threat information and policies.

The Security Policies View is where security rules and filters—as well as Intelligent Escalation triggers—are defined via a flexible and powerful interface.

The Dashboard View offers at-a-glance views of the entire Web applications security posture of the enterprise. Authorized users can view real-time security events, respond to violation alerts, and check on the status of servers, gateways, and monitors across the organization.

The Forensics View provides access to historical information, allowing users to perform detailed analysis of event logs to identify trends and needed areas of improvement.



SUPERIOR FLEXIBILITY AND CONTROL

On-Demand Threat Management

Defiance Monitors can detect and log security events out-of-band with zero impact on operational performance, while Defiance Gateways are deployed in-line and can operate in Bypass or Passive Mode until a pre-defined event trigger escalates the threat level. This unprecedented intelligence allows the enterprise to optimize performance and capacity until there is reason to believe it is under attack. Security policies that define event escalation triggers can be customized from the global enterprise level down to the application, location, or individual server levels to provide maximum flexibility and control.

Customized Protection

Defiance TMS allows the enterprise to easily refine security policies for each application, with granularity down to the page or parameter level. This provides the enterprise with maximum flexibility to tailor the level of security based both on the needs of the business and on the level of risk.

VISIBILITY ACROSS ORGANIZATIONAL ROLES

Defiance TMS allows the enterprise to implement security management across a variety of roles and users needs. Organizations can implement security as a business process to optimize both productivity and security readiness. Defiance TMS roles are categorized and profiled to accommodate the information access level needs of users throughout the enterprise, including:

- Senior security officers
- Line-of-business managers
- Distributed security audit personnel
- Security staff
- IT professionals
- IT administrative employees

RAPID DEPLOYMENT

Out-of-the-box security policies eliminate major threat categories and provide instant protection, allowing the enterprise to deploy Web application threat management solutions in hours—instead of in days or weeks. Defiance TMS policies are defined based on the unique structure, characteristics, and vulnerabilities of third-party or internally developed applications. Policies developed for one deployment can be quickly replicated for Defiance Gateways and Monitors in other locations.

THREATS PREVENTED

- **SQL injection**
- **Cross-site scripting**
- **Parameter tampering**
- **Hidden field manipulation**
- **Cookie poisoning**
- **Stealth commanding**
- **Backdoor and debug options**
- **Application buffer overflow attacks**
- **Data encoding**
- **Unauthorized navigation**
- **Gateway circumvention**
- **Web server reconnaissance**
- **SOAP and Web services manipulation**

Corporate Headquarters
Kavado Inc.
1 Canterbury Green
12th Floor
Stamford, CT 06901-2034

(800) 239-3203
(203) 325-0575
E-mail: info@kavado.com

R&D Center
Kavado Israel Ltd.
23 Hamelacha Street
Afeq Industrial Park
Rosh Ha'ain 48091
Israel

972 (3) 910-2800

European Headquarters
Kavado Europe Ltd.
Gainsborough House
33 Throgmorton Street
London EC2N 2BR
England

44 (207) 397-3450

www.kavado.com