SECURING ENTERPRISE APPLICATIONS

AppSecure and Mykonos Web Security (MWS) Provide Highly Effective Approach for Securing Applications on the Network, Device, and Cloud

Challenge

The traditional network perimeter no longer exists. Companies do not own the devices that access their systems and cannot control where all of the data lives. A new security model is needed to protect today's proliferation of applications and devices from attack.

Solution

Juniper's application security solutions offer a comprehensive application security approach to safeguard the business from an attack—whether it is a consumer or business application accessed from a mobile device, or a website application over the Internet.

Benefits

- Delivers an effective approach to securing applications on the network, device, and cloud
- Routinely scans and removes mobile applications for malicious software and infected apps
- Employs groundbreaking Intrusion Deception technology to detect and prevent a Web attack from occurring
- Provides immediate notification when a hacker is trying to access your website

The explosion of sophisticated and robust applications is changing the way employees and consumers access critical business and personal information. There are new devices and users (mobility/BYOD), new platforms and services (the cloud), and new innovations around delivery models and applications (work productivity, social media, etc.). The average enterprise is hosting more than 500 applications that employees are downloading every day to their personal and business devices. And, data is everywhere.

As consumers, we shop online, access our Facebook and YouTube accounts, and log into our financial institutions to view our balances and pay our bills. And, we are doing so at work, at home, at the airport, or at a nearby coffee shop using a variety of devices—smartphones, tablets, laptops, and desktop PCs. Moreover, public websites have become a clear and easy target, as both organized entities and skilled individuals have successfully accessed public websites to gain entry to business critical as well as personal information. Recent statistics reveal that most websites have vulnerabilities, and the motivation for malware and breaching is on the rise:

- According to Gartner and the U.S. Computer Emergency Response Team (U.S. CERT), 75% of new attacks specifically target the application layer in order to exploit these weaknesses and steal critical financial and customer data.[1]
- 73% of companies have been breached in the past two years through their web applications (Ponemon).
- Hackers are acting with impunity because they know that there is nothing to detect their malicious behavior.
- The security landscape is changing (simple algorithms can decipher your password, assume your identity, and within seconds use this information to infiltrate other websites).
- Unprotected mobile devices can be easily affected by malware.
- "Anonymous" has proven that sophisticated attacks can happen to anyone, anywhere.

Organizations like Sony, LinkedIn, NASDAQ, Zappos, CIA, and the U.S. Dept. of Commerce (just to name a few) have already been hacked, exposing hundreds of thousands of personal accounts and causing unforeseen downtime, tarnished reputations, and lost revenue adding up to millions of dollars.

The Challenge

According to a recent report, the median period between the start of an intrusion and its detection is 416 days, or more than a year.[2] In 2011, the Ponemon Institute released one report estimating the cost of a breach at $214 per stolen record. IT leaders are challenged with protecting their enterprise's reputation and exposure from this escalating threat and need a secure, proactive, and methodical approach that will help them safeguard the business.

[1] Veracode Dynamic Analysis. www.veracode.com/products/dynamic

[2] The Wall Street Journal. U.S. Outgunned in Hacker War. March 2012

The proliferation of wireless devices along with the cultural shift towards a mobile workforce has created two new challenges facing enterprises today:

1. The rise of sophisticated and robust applications running across the network.
2. The various types of attacks and sophistication of attackers going against those applications.

To complicate matters further, today's consumer and business applications are ubiquitous. They include social platforms like YouTube, Facebook, and Twitter, as well as applications that are purpose-built for a business need such as inventory management applications in manufacturing, temperature monitoring applications in healthcare, or website applications used across the typical enterprise. Businesses are also using a variety of Web applications to build their company websites, serve as a secure customer and/or partner portal, and create splash pages or registration forms. These Web applications are being introduced at a very rapid pace, and they represent one of the largest threats to any organization's network security. Traditional "perimeter" style defense systems are struggling to protect application logic flaws because there are infinite potential vulnerabilities and only a finite number of known signatures to detect. Today, the economics are in the hackers' favor, with little to effectively stop their attacks.

The type and sophistication of the attacker is also a key challenge for IT. Modern day attackers come in both human and electronic forms and fall under the following key profiles:

- **Malware intrusions:** Typically piggybacked with a software program or application and unknowingly downloaded onto a mobile, laptop, or desktop device
- **Script and tool exploits:** A less sophisticated attacker who has downloaded a script or exploit to run against a website
- **IP scan:** An automated attack where a scan is run across millions of IP addresses looking for a known vulnerability (e.g., a known WordPress vulnerability)
- **Targeted scans:** A significantly larger automated attack by a scanner that examines the entire Web application and probes for thousands of vulnerabilities
- **Botnets:** An automated attack that allows an attacker, once a vector is established, to scale the attack and hide it across many thousands of IP addresses
- **Human attacker:** Profit-driven individuals and organizations focused on compromising businesses and other organizations using sophisticated attack tools

In short, businesses today are under siege. On the one hand, more and more rich applications facilitate collaboration, deliver a greater customer experience, and dramatically improve efficiencies across the business. At the same time, the various types of attackers and the inherent risks they represent escalate, if such applications are not secured against today's increasingly sophisticated attacks. What is needed is a solution that can be trusted to instill confidence that all communication points across the business network are secure.

The Juniper-Mykonos Application Security Solution

Juniper offers a comprehensive application security solution that effectively safeguards the business from attack—whether it is coming from a social application accessed from a smartphone, tablet, laptop, or desktop; a business application using consumer or business grade devices; or an online application.

AppSecure is a suite of next-generation security capabilities for Juniper Networks® SRX Series Services Gateways that utilize advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network. Working in conjunction with the other security services of the SRX Series, AppSecure provides a deep understanding of application behaviors and weaknesses to prevent application borne threats that are difficult to detect and stop.

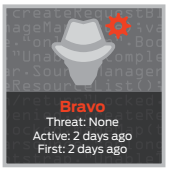
Recently acquired as a Juniper company, Mykonos offers an innovative approach to Web security, one that uses Intrusion Deception to detect hacking attempts from the start, stopping them in their tracks while collecting forensic information and recording the attack like a DVR. Attacks to business critical Web servers can not only be prevented, but the analytics that are needed to optimize network and Web security can also be captured.

With Juniper's AppSecure, customers can gain visibility into which applications are running on their network and enforce user role-based policies by application name rather than static port or IP. This advanced security capability allows customers to block out malicious or noncompliant applications that pose a security or productivity risk. With the proliferation of social media applications within corporate networks and their integration into corporate applications, AppSecure helps customers weed out malicious traffic and enforce compliance policies while allowing users to accomplish their daily tasks.

With Juniper's Mykonos Web Security solution (MWS), company websites are secured with a groundbreaking Intrusion Deception solution that detects, tracks, profiles, and prevents Web attacks. Using deceptive tar traps to detect attackers with absolute certainty, MWS inserts detection points into the code (including URLs, forms, and server files) to create a random and variable minefield all over the Web application. These tar traps allow you to detect attackers during the reconnaissance phase of the attack, before they have successfully established an attack vector. Attackers are detected when they manipulate the detection points inserted into the code. And because attackers are manipulating code that has nothing to do with your website or Web application, you can be absolutely certain that it is a malicious action, with no chance of a false positive.

Detect
Detect attackers with no false positives

Track
Track attackers beyond the IP address



Profile
Understand attackers capabilities and intent

Respond
Deceive the attacker and prevent the attack

Features and Benefits

Juniper's AppSecure and MWS in combination offer enterprises a methodical and reliable approach to securing applications across the enterprise network that will:

- Detect anomalous activity and inform stakeholders
- Prevent embedded malware or traffic storms from proceeding in the network and causing disruption
- Predict Web attacks at their launch and divert the attempt without impeding legitimate access
- Adapt and fine-tune access and security policies with forensic data
- Customize intrusion prevention system (IPS) by application, to manage traffic, compliance, and overall productivity

Mykonos Web Security is the first Web Intrusion Deception solution available in the marketplace to supplement more traditional signature-based Web application firewalls, and it is the first solution that can foil Web attackers in real time.

- MWS uses deceptive techniques and inserts detection points, or tar traps, into the code of outbound Web application traffic to proactively identify attackers before they do damage.
- MWS works out-of-the-box to improve Web application security. There are no rules to write, no signatures to update, no learning modes to monitor, and no log files to review.
- MWS captures the IP address as one data point for tracking the attacker, but recognizes that making decisions on attackers identified only by an IP address is fundamentally flawed because many legitimate users could be accessing your site from the same IP address. For this reason, MWS tracks the attackers in significantly more granular ways.
- For attackers who are using a browser to hack your website, MWS tracks them by injecting a persistent token into their client. The token persists even if the attacker clears cache and cookies, and it has the capacity to persist in all browsers including those with various privacy control features. As a result of this persistent token, Mykonos Web Security can prevent a single attacker from attacking your site while allowing all legitimate users normal access.
- For attackers who are using software and scripts to hack your website, MWS tracks them using a fingerprinting technique to identify the machine delivering the script.

Detection with no false positives and client-level tracking is vital for launching a countermeasure to prevent an attack. Only with certainty-based detection can you safely prevent an attacker and know that you are not blocking legitimate users. MWS Smart Profiling technology uses attacker profiles to determine the best response in the prevention of an attack. Responses can be as simple as a warning or as deceptive as making the site simulate that it is broken for the attacker only. Every detected attacker gets a profile and every profile gets a name. The Smart Profiling technology ultimately creates a threat level for each attacker in order to prevent attackers in real time, at the client level, with no false positives.

Smart Profiling also provides IT security professionals with more valuable knowledge about attackers and the threat that they pose than has ever been available before. With automated countermeasures, MWS works around the clock detecting and preventing attackers. It's not creating log files for you to review to find an attacker. It tells you how many attackers it has detected and what countermeasure response was applied. It's a security device that works as part of your security team even when you sleep. MWS provides an intelligent technology at the Web application layer, providing abuse detection, abuse tracking, abuse profiling, abuse response, and real-time incident management.

Table 1: AppSecure Features and Benefits

Feature	Feature Description	Benefit
Application awareness and classification	Context, protocol information, and signatures used to identify applications on any TCP or UDP port	Enables all AppSecure capabilities by exposing application information to advanced, next-generation security services for increased visibility, control, and protection
Nested application support	Accurate identification of applications running on top of, or embedded into approved/trusted services and protocols	Provides enhanced protection against modern evasion techniques that utilize trusted services
User/role-based policies	Fine-grained policies, including application security, based on user role and identity for all endpoints including mobile devices	Superior protection and easier policy management as user and user groups reduce the number of policies and rules needed to account for other elements such as location, device, and IP address
SSL inspection	Inspection of HTTP traffic encrypted in SSL on any TCP/UDP port	Combined with AppSecure, provides visibility and protection against threats embedded in SSL encrypted traffic
Purpose-built platform	Built from the ground up on dedicated hardware	Delivers unrivaled performance and flexibility to protect service provider, enterprise, and data center environments
Juniper Networks Junos® Operating System service integration on SRX Series	Rich set of native network and security services including: firewall, AppSecure, IPS, IPsec VPN, Network Address Translation (NAT), Quality of Service (QoS), routing, and switching	Provides consolidation and optimization of application-aware security services for maximum scale

Table 2: Mykonos Web Security Features and Benefits

Feature	Feature Description	Benefit
Abuse detection processors	A library of HTTP processors that implement specific abuse detection points in application code. Detection points identify abusive users who are trying to establish attack vectors such as cross site request forgery	• Detect attackers with no false positives
Abuse tracking	Full HTTP Capture that captures and displays all HTTP traffic for security incidents.	• Track attackers with device-level tracking that allows for accurate profiling of the attacker
Abuse profiling	Maintains a profile of known application abusers and all of their malicious activity against the application.	• Understand the attacker's capabilities and intent • Watch attackers live and record the attack like a DVR
Abuse response	Enables administrators to respond to application abuse with session-specific warnings, blocks, and additional checks. Provides single-click automation of responses during configuration.	• Deceive and frustrate the attacker • Prevent attacks
Real-time incident management	Sends alert emails when specific incidents or incident patterns occur. Command-line interface for custom reporting, reporting management system with user interface, and SNMP system logging.	• Around the clock security • Immediate notification if a hacker is attempting to access your site

Solution Components

The old network protected the perimeter; the new network needs to protect the device and the application as well. Juniper's AppSecure and MWS can be deployed together or separately to deliver the visibility, security, and reliability you need to ensure this kind of comprehensive protection.

Components of AppSecure are:

- **Application visibility with AppTrack** – AppTrack collects byte, packet, session, and time statistics while accurately identifying hundreds of applications and giving network administrators detailed analysis of application data. AppTrack quickly and easily provides visibility into the types of applications traversing through the SRX Series gateway and allows classification based on risk level, user ID, zones, source, destination addresses, and volumes. This information can be used to assess adherence to usage policies, help address bandwidth management, or simply report on the most active users and applications. Juniper Networks STRM Series Security Threat Response Managers for centralized logging and reporting provide a flexible and extensible way to analyze data from a centralized location. Using a variety of predefined report formats, the STRM Series can generate reports based on AppTrack application log data to inform needed actions.
- **Application enforcement with AppFW** – AppFW allows administrators to create fine-grained application control policies to allow or deny traffic based on dynamic application name or group names rather than static IP/port information. It is designed to simplify security policies by using application white lists and black lists, as well as to define what actions to perform on matched traffic, while taking default action against all other traffic.
- **Application control with AppQoS** – With the increased use of web-based Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), and other commonly used business tools, network administrators need a way to prioritize business critical traffic over the network. AppQoS provides the ability to meter and mark traffic based on application policies set by the administrator. This allows lower priority Web traffic to continue whenever network bandwidth allows, while ensuring that mission critical traffic is delivered when usage levels surge.
- **Application protection with AppDoS** – AppDoS identifies attacking botnet traffic against legitimate client traffic based on application-layer metrics and remediates against these botnet attacks. Employing a multi-stage approach that includes server connection monitoring, deep protocol analysis, and bot-client classification, AppDoS provides the ability to detect subtle changes in traffic patterns and client behaviors that could indicate an application-level Denial-of-Service (DoS) attack. Once suspicious activity is detected, AppDoS can then issue an alert, block offending IP addresses, or completely drop irregular sessions and packets. AppDoS is typically deployed with the SRX Series integrated IPS service to increase protection.
- **Application protection with IPS** – Intrusion prevention system tightly integrates Juniper's latest and most advanced security features with the network infrastructure to provide threat mitigation and protection from a wide range of attacks and vulnerabilities. IPS subscribes to the results of application identification and contextualization to determine the appropriate protocol decoding and attack objects to use for the permitted incoming traffic that will be processed by the IPS software services module.

Components of MWS are deployed in three ways:

- **Internal data center** – Software deployment on any approved hardware.
- **Virtualized** – Deployment in VMware environments.
- **Cloud** – For deployments to protect sites in the Amazon cloud.

Summary – AppSecure and MWS Solutions for Enterprise Application Security

The level of sophisticated and robust consumer and business applications available today is staggering. Increasingly, malicious software has found a way to penetrate enterprises through all types of applications—whether masked in an application or game downloaded on a mobile device, or hidden in malicious scripts targeting company websites. IT leaders are faced with the challenge of securing against all types of attacks to protect their company's reputation and business from exposure and risk.

Juniper's AppSecure and MWS solutions offer a comprehensive application security approach to safeguarding the business—whether an attack is coming from a consumer or business application accessed from a mobile device or from a Web application. AppSecure is a suite of next-generation security capabilities for Juniper Networks SRX Series Services Gateways using advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network. MWS provides an intelligent technology at the Web application layer for abuse detection, abuse tracking, abuse profiling, abuse response, and real-time incident management. It detects, tracks, profiles, and responds with automated countermeasures that work around the clock frustrating and blocking attackers. It tells you how many attacks it has detected and what countermeasure response was applied, even when you sleep.

Hacking has become a business and can take a short amount of time to steal a very large amount of data that can be misused or sold for a profit. Together, the AppSecure and MWS solutions change the economics of hacking from an inexpensive and relatively simple exercise, to a scenario where attackers are blocked at every turn and must reconsider what and how they attack to have any hope of success.

Next Steps

For more information about Juniper Network's security solutions, please contact your Juniper Networks sales representative or visit **www.juniper.net/security**.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3510459-001-EN Jun 2012 Printed on recycled paper