Trustwave®
a Singtel company

DATA SHEET

Trustwave Intrusion Detection/Prevention System

TRUSTWAVE DEVELOPED, MANAGED SERVICE READY

Benefits

- Reduce risk of downtime or data loss resulting from malicious network traffic
- Reduce costs associated with regulatory or compliance fines
- Identify or block the latest attacks detected using integrated threat intelligence from SpiderLabs
- Improve customer satisfaction by avoiding attacks, downtime, and data loss
- Enjoy long-term predictable costs and zero capital investment

Your IP safeguarding and services needs have grown, and your network is filled with ever-changing potential threats. Trustwave can help with both. Trustwave's Intrusion Detection/Intrusion Prevention system (IDPS) leverages Trustwave's SpiderLabs Threat Intelligence database for monitoring and alerting on attacks and for blocking malicious traffic. By providing these security tools as a customizable full service, Trustwave can eliminate the hassles of in-house system management and costs associated with staffing a 24x7 operation, even in the most complex deployments.

Comprehensive, Up-To-Date Protection

SpiderLabs threat intelligence attack signatures differentiate Trustwave Intrusion Detection and Prevention systems. Attack signatures coupled with anomaly detection allow administrators to govern whether activity is either flagged or blocked. SWF signatures are also blocked optionally by the engine.

Trustwave IDPS can be deployed in multiple ways, but the largest ROI is deploying this tool through Trustwave's managed service offering. As a 2017 Gartner Magic Quadrant Leader in managed security services, Trustwave's expertise has been validated both by third parties and our customer base.

Key Capabilities

Trustwave's IDPS offerings are configurable to deployments, ensuring that monitoring and protection are in effect in any environment. Key capabilities include:

- **A first class, high speed intrusion detection engine** which enables your organization to control access inside the network to secure assets with full-state inspection.
- **As a transparent Layer 2 appliance,** neither IP address nor routing changes are necessary. Your organization can easily protect assets without redesigning your network.
- **Targeted signature sets** to tailor control to meet the specific needs of the environment.
- **Regular signature updates** from Trustwave SpiderLabs that address the latest network-based threats. In some cases, updates may include protection against zero-day attacks.
- **SWF signature support.**

Choosing a Trustwave Product with a Trustwave Managed Service

Organizations struggle to find skilled security personnel, and in many cases, admins need to cover a dispersed network. Partnering with Trustwave's managed security offerings using a "follow the sun" model reduces time to delivery and implementation, regardless of geographic location. With a direct line to Trustwave product management, feature requests, modifications, and bug notification from the SOC to Trustwave's product team are streamlined, providing the best service and turnaround time if issues arise at any point during your journey.

With a managed IDPS service, Trustwave delivers:

- **Installation and Configuration.** Trustwave will recommend where to place IDS/IPS sensors within your network, install them, and finally configure them to ensure all supported capabilities will be able to be managed by Trustwave analysts.
- **Ongoing IDPS Management.** As part of managing the IDS/IPS itself, Trustwave analysts will perform regular health and availability monitoring, change management activities when needed, and will apply product and security updates.
- **Continuous Event Identification.** Events from your IDS/IPS logs are continuously reviewed to identify threats. To minimize false-positive events, Trustwave analysts analyze event logs and notify you in the case of an actual or potential threat.
- **Proactive 24x7 Notification.** You decide what events you want Trustwave to proactively notify you about. Security events are classified as "potential," "medium," "high" and "critical," and you can tailor notification guidelines to your preference.
- **Dynamic Online Reporting and Documentation.** A record of alerts is documented along with the actions taken in response to each attempted intrusion in the secure TrustKeeper portal, giving you round-the-clock access to all captured events and those that warranted additional action.

Trustwave®
a Singtel company

For more information: www.trustwave.com