Managed Intrusion Detection
powered by Trustwave®

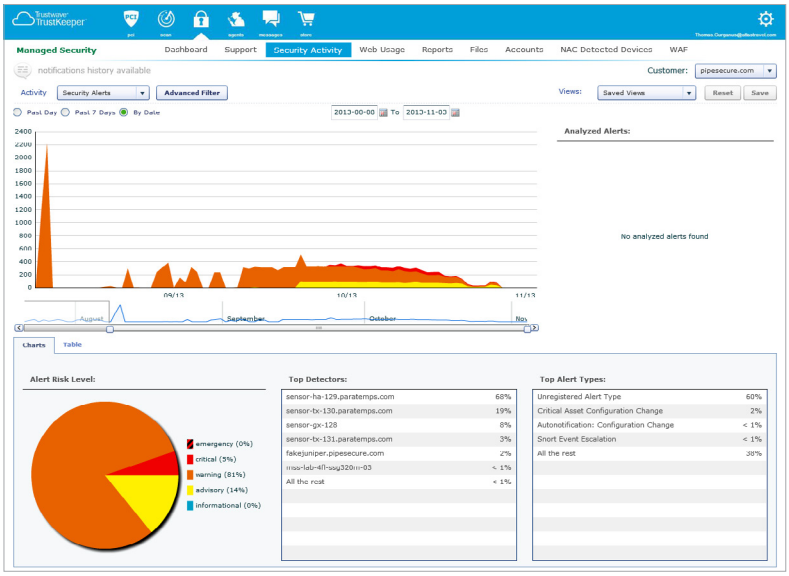
Identify attacks on your network assets yes

Optus Managed Intrusion Detection powered by Trustwave® delivers customised, comprehensive security for organisations that need data security experts to monitor network and application-layer traffic via an Intrusion Detection System.

Perimeter defences alone are not enough to secure your network. Round-the-clock, expert human analysis that complements investments in security technology and controls is essential to help detect potentially malicious activity within your network.

An Intrusion Detection System (IDS) plays an integral role in supplementing other security measures in modern corporate networks. To be effective an IDS implementation requires disciplined processes and experienced staff, carefully configured systems and consistent tuning and updates of the IDS device itself. That's why organisations entrust their IDS management to Optus.

- **Consultation and design** – Following an extensive network review and scoping exercise, Optus Managed IDS powered by Trustwave will recommend the most effective placement of IDS sensors within your network.
- **Configuration and policy development** – Once our experts work with you to identify the subnets and VLANs you wish to monitor, they will tune the IDS to your environment and test and deploy the customised configuration. After initial deployment – and before the service becomes fully operational – our engineers will continue to monitor and adjust IDS policy to establish a baseline in order to optimise device performance.
- **Ongoing device management and signature updates** –Trustwave network security engineers manage the IDS service remotely from Trustwave's network of globally federated Advanced Security Operations Centres (ASOCs). Trustwave's attack-tracking libraries are regularly correlated, tested and updated by Trustwave SpiderLabs team to ensure emerging threats are monitored and brought to the appropriate parties' attention.
- **Continuous event identification** – Events from your IDS logs are continuously reviewed to identify threats. To minimise false-positive events, qualified network security engineers will analyse event logs and notify you in the case of an actual or potential threat.
- **Timely response and escalation** – When an issue arises, the ASOC powered by Trustwave will notify designated personnel within your company as a first step in your incident response policy.
- **Managed intrusion detection** –The Managed IDS Service deploys sensors at key locations on your network to identify patterns of suspicious activity. Network security engineers then analyse event and traffic data 24x7 to assess a threat's potential to harm corporate assets.
- **Proactive 24x7 notification** – Notification is conducted in accordance with pre-approved policy. Security events are classified as "low" "medium," "high" and "critical," and customers can tailor notification guidelines to their preference. Interaction with your staff is carried out in a secure manner – through strict authentication and confirmation protocols either through Trustwave's TrustKeeper® portal or over the phone.

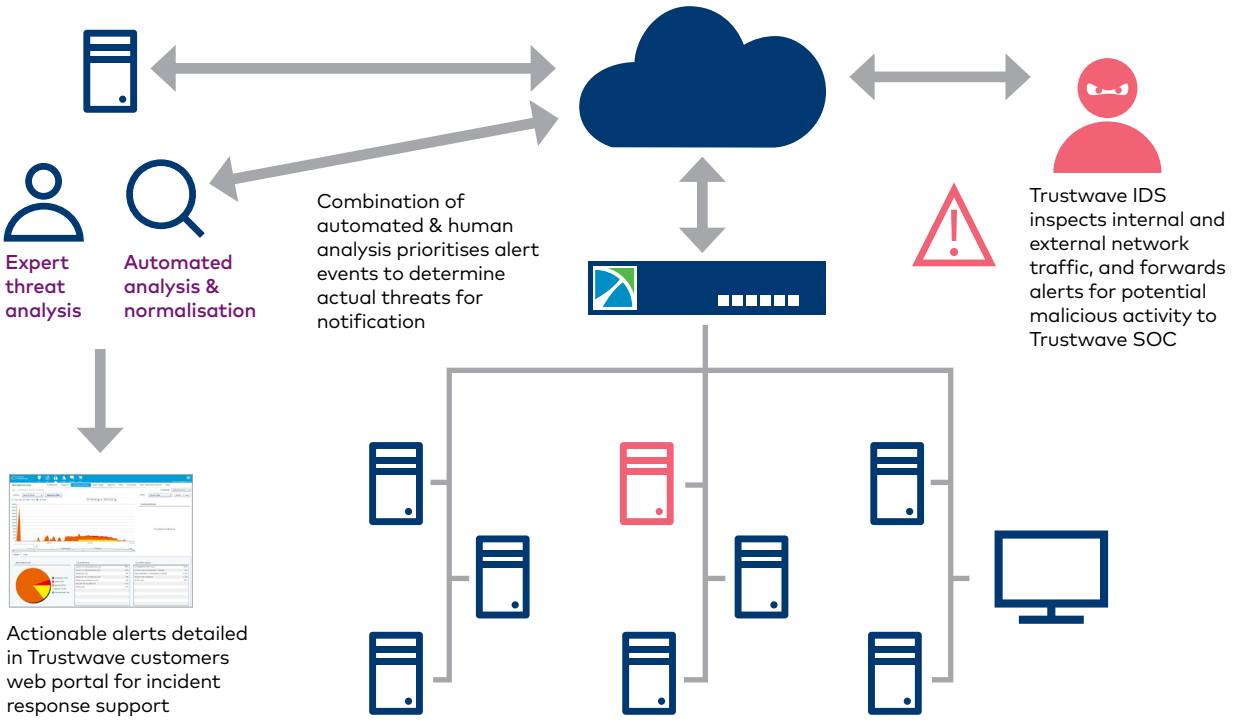


IDS event report details

OPTUS | Trustwave®

- **Dynamic online reporting and documentation** – A record of alerts is documented along with the actions taken in response to each attempted intrusion. Via a secure portal, you have round-the-clock access to all captured events and those that warranted additional action.
- **How it works** –The Managed IDS Service adheres to best practice standards. Following an initial consultation, Trustwave network security engineers configure and thoroughly test the IDS sensors. Once the device is installed on the customer site, Trustwave engineers then perform further tuning on the device.
- **Why it's effective** – Our IDS utilises a combination of signature and anomaly detection to identify potentially malicious activity. Optus Managed IDS powered by Trustwave's network security experts respond to events triggered by policy exceptions based on signature match or observed traffic anomalies, such as malformed or atypical packets, to ensure that appropriate actions are taken.
- **Benefits** – Managed IDS provides a full-service solution that eliminates the following:
  - Hassles of in-house management
  - Costs associated with staffing a 24x7 operation
  - Recruiting, hiring and retaining qualified staff
- **Results delivered** – Unlike hardware or software-oriented solutions, the foundation of Optus' Managed IDS Service rests upon expert human analysis. Through Trustwave's online, secure portal, you have continuous access to reporting that includes real-time and historical event information (stored for an agreed upon length of time). To assist with internal control and compliance requirements, a record of attack events and their severity is automatically posted to the portal for review and assessment-support purposes.
- **Related services** – The Managed IDS Service can be deployed alone or in concert with other Optus data security and compliance services as required by your organisation.

Trustwave IDS threat analysis and alerting



GMO_N 0460 1116MZ