# Integrity360 Managed Intrusion Detection and Prevention (IDPS) Service

## Service Definition

### Managed Security

A Managed Security service can help simplify and strengthen an enterprise's security posture while allowing them to avail of 24x7 access to some of the best cyber security expertise and technology in the industry, ensuring ongoing monitoring and instant response to new threats and incidents. Integrity360's full managed security service includes Managed Firewall, Managed SIEM, Managed IPS and Vulnerability Management.
Integrity360 holds the highest level of certifications and accreditations with the industry's leading IT security partners. In addition to vendor and solutions-based training Integrity360 strongly encourages and funds all technical members of staff to undertake vendor agnostic security training and certification in the form of SANS GIAC. Our customers can be assured that Integrity360 will provide the highest level of cyber security knowledge and skills available. Due to the extensive skill set of the Integrity360 security teams, Integrity360 has the expertise to integrate, support and manage these leading solutions in our client environments.
With a 24x7 Security Operations Centre (SOC) the company boasts a global security capability with a local presence and personalised service offering.

### Managed IDS/IPS Service

Included as a component element of the Managed Firewall solution is the Managed IDS/IPS Service. It is tightly integrated with the Managed Firewall solution and can only be provided in conjunction with Check Point firewalls.

### Technical Overview

Integrity360 offers a fully managed intrusion detection and prevention system (IDPS) to detect signs of network intrusion, raise alerts and take actions to block unwanted and harmful traffic from entering your network. Suspicious content is flagged, assessed and subjected to an automated, predefined action, resulting in it either being blocked or allowed.
Crucially, the system learns about the normal network and traffic patterns over time, building greater accuracy and reducing false positives. Our managed IDS/IPS is a truly dynamic service.
Integrity 360's managed IDS/IPS follows a series of stages, from setting initial rules through to tuning and updating. It incorporates:

- **Traffic baseline and rule-setting**, to understand your network, the essential traffic you need to operate and the traffic that might be suspicious. Automated rules are applied to different content types.
- **Continual analysis**, identifying any suspicious activity and content.
- **Automated, pre-defined actions** according to the content type: it may be dropped, blocked or allowed access. Certain traffic may be blocked by default.
- **Tuning and adaptations** as security devices 'learn' the characteristics of the network, to ensure that legitimate traffic is not blocked, and false positives are reduced.
- Our expert security analysts take charge of configuring your network devices, enabling you to benefit from their years of expertise and training, while the devices themselves become absolutely tailored to your organisation.

- Over time, the number of alerts will decrease as the IPS rules begin to closely reflect the traffic on your network. In turn, this reduces the traffic burden on your network (as unnecessary traffic is seamlessly blocked) and the management burden on your IT function (as false positives are minimised).

## Key Features

The Managed Intrusion Detection and Prevention Service includes the following key features:

- Monitors logs and sends alarms
- Integrity360 Security Analyst detects signs of intrusion in networks/systems and takes appropriate action
- Analyses traffic and automatically executes predefined actions if suspicious activities are detected. Actions may include: dropping the traffic, blocking traffic or allowing specific traffic.
- Stops common attacks and blocks traffic by default
- Proactive tuning on a regular basis to ensure the system knows what to look for and to ensure that legitimate traffic is not being blocked
- As the knowledge system builds, then fewer alerts will occur as the Managed IDS/IPS fine-tunes
- This service compliments the normal firewall protection service
- Integrates with other services from Integrity360

## Major Deliverables

- Integrity360 will ensure that the following deliverables are managed to meet the associated service levels on the supported domain.
- Provide a secure path to take log feeds from the IDS/IPS systems
- Perform proactive tuning and management of the IDS/IPS Systems based on expert knowledge and knowledge of the customer environment
- Manage signature updates following a scheduled structured process
- Provide monthly reporting detailing signature changes and IDS/IPS tuning recommendations
- Conduct service review meetings on a quarterly basis