

Essant Managed Intrusion Detection & Intrusion Prevention Service

Firewalls are a core component of an organisations security strategy. However, businesses are now developing a “Borderless Network” approach to provide access to mobile employees and to foster collaboration across suppliers, partners and customers. Although firewalls establish a strong perimeter security they are configured to allow certain applications to pass through, it is the vulnerabilities in these applications that attackers now target to compromise the services allowed through firewalls, which are also obviously powerless when dealing with an internal attack.

To combat this, an IDS or IPS device is placed in a key location, or locations, in the network and analyses the content of individual packets for malicious traffic. However, configuring and initial tuning takes time and expertise to ensure total confidence in the protection provided, without the fear of legitimate traffic being dropped. Ongoing Signature Management requires expert, timely distribution, upgrading and re-tuning of the system sensors to ensure protection is maintained and benign alarms are avoided.

Service Overview

Essant offer both Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as Managed Services, built around the Cisco Adaptive Security Appliance (ASA) 5500-series platform and the Cisco 4200-series sensors. The IDS provides out-of-band service designed as a forensic tool, it alerts a security analyst of suspicious behavior while the IPS service deploys sensors inline within the network between identified security zones, to mitigate attacks in real time - which service is right for your organisation depends on your specific circumstance and what is to be achieved our Security Consultants can explore this further with you.

The Essant IDS & IPS services compliment firewalls in offering a more granular inspection model than a traditional firewall by inspecting the data within a packet as well as risk rating of the destination to allow a sensor to alert (IDS),

or make an instant decision on whether to allow the traffic to pass or not (IPS). Essant configure, deploy and tune sensors, in accordance with your security policy (which we can help you develop and document when required) as part of the Managed Service.

Post deployment Essant provide 24x7 expert monitoring and best-practice IDS/IPS device management, realtime response and escalation of unauthorised activities and security events in accordance with the pre-agreed customer alerting and escalation process. In addition Signature Pack Updates are remotely distributed to devices under management, typically during the agreed weekly Change Management Window, which are then re-tuned with appropriate filters applied to reduce repetitive false-positive alarms following evidence of benign event triggers.



Services Features:

All IDS/IPS devices are monitored and managed from the Essant Monitoring and Management Centres (EMMC) located in Wakefield and Leeds. The specific connectivity from the management centres to the managed devices is agreed on a per-customer basis, but in most cases a dedicated management VLAN is provisioned at the customer site to facilitate signature and sensor software updates. All communications between the management centres and the customer is secured using IPsec tunnels. The IP addressing for this network is assigned either by Essant or the customer; suitable Network Address Translations (NAT) are applied to the EMMC and customer firewalls to ensure correct working of polling, syslog, traps and alarm notifications.

- Security and Network Audit with Security Policy design (where required).
- Configure, install, manage, backup and maintain all equipment.
- Real-time intrusion monitoring, detection, alerting, blocking, response & escalation.
- 24x7 activity and availability monitoring.
- Automated signature pack management, distribution, updating and retuning.
- Global correlation of vulnerability data to prevent the spread of attacks via Cisco SIO (see below)
- Comprehensive executive, technical and compliance reporting.
- Secure online service management via the Essant Secure Portal.

Cisco Security Intelligence Operations



Cisco Security Intelligence Operations (Cisco ISO) is a sophisticated security ecosystem consisting of three components:

1. Cisco SensorBase: The world's largest threat monitoring network that captures global threat telemetry data from an exhaustive footprint of Cisco devices and services.
2. Cisco Threat Operations Center: A global team of security analysts and automated systems that extract actionable intelligence.
3. Dynamic updates: Real-time updates automatically delivered to security devices, along with best practice

recommendations and other content dedicated to helping customers track threats, analyze intelligence, and ultimately improve their organization's overall security posture.

Global Correlation

Cisco Global Correlation is a sophisticated, automated security capability that gives IPS devices unprecedented threat management efficacy. Global Correlation automatically correlates SensorBase threat information, including reputation, known exploits, anomalous behaviors, and vulnerability information, to detect blended, widespread, and targeted attacks.

Essant Managed IDS/IPS & Global Correlation

Combining the SensorBase Global Correlation of threat information with real time intrusion detection and prevention activities of the Essant Managed IDS/IPS service provide customers with unrivalled protection against ever increasing new and emerging threats .

