ThreatDefence - Security Incident and Event Management Data Analysis

Background

ThreatDefence is SoftGen's latest offering in the fight against the growing number of cyber-attacks.

It is now widely recognized and accepted that Prevention is no longer sufficient – a strong security strategy needs to be Proactive and Multi layered.

As the number of attacks and the sophistication grows, traditional security management systems don't address the challenges faced in today's dynamic business environments. The need to utilise virtualisation, cloud computing and mobile devices, including BYOD, is a critical factor for a business to remain competitive.

ThreatDefence provides real time threat analysis, and can detect emerging and previously documented threats, such as the Crypto Lockers Ransomware virus, using technology that goes beyond signature and anomaly based detection.

ThreatDefence report and block any suspicious traffic on compatible firewalls. Apart from monitoring all your internet traffic, ThreatDefence can also monitor log data from Windows event logs, Mail and Web servers, Routers and Firewalls, in short any type of file log.

The log analysis capability of ThreatDefence allows a security analyst to extensively audit historic logs in order to determine if major security incidents have occurred in the past and prevent future incidents.

SoftGen's Security analysts, will analyze the events and raise a ticket with the customer helpdesk if action needs to be taken (changes to firewall policy, patch system etc.)

How it works

The deployment model consists of a single appliance for small to medium organisations which scales to clusters of appliances for large organisations.

Typically in an SMB environment the appliance is deployed in the data centre attached to the SPAN port of the primary switch which allows ThreatDefence to analyse all data passing through the switch.

In large organisations, ThreatDefence is deployed as a cluster of appliances to handle the load with NetFlow Sensors attached to critical switches throughout the network environment.

Network Monitoring is constant with real time alerting and reporting.

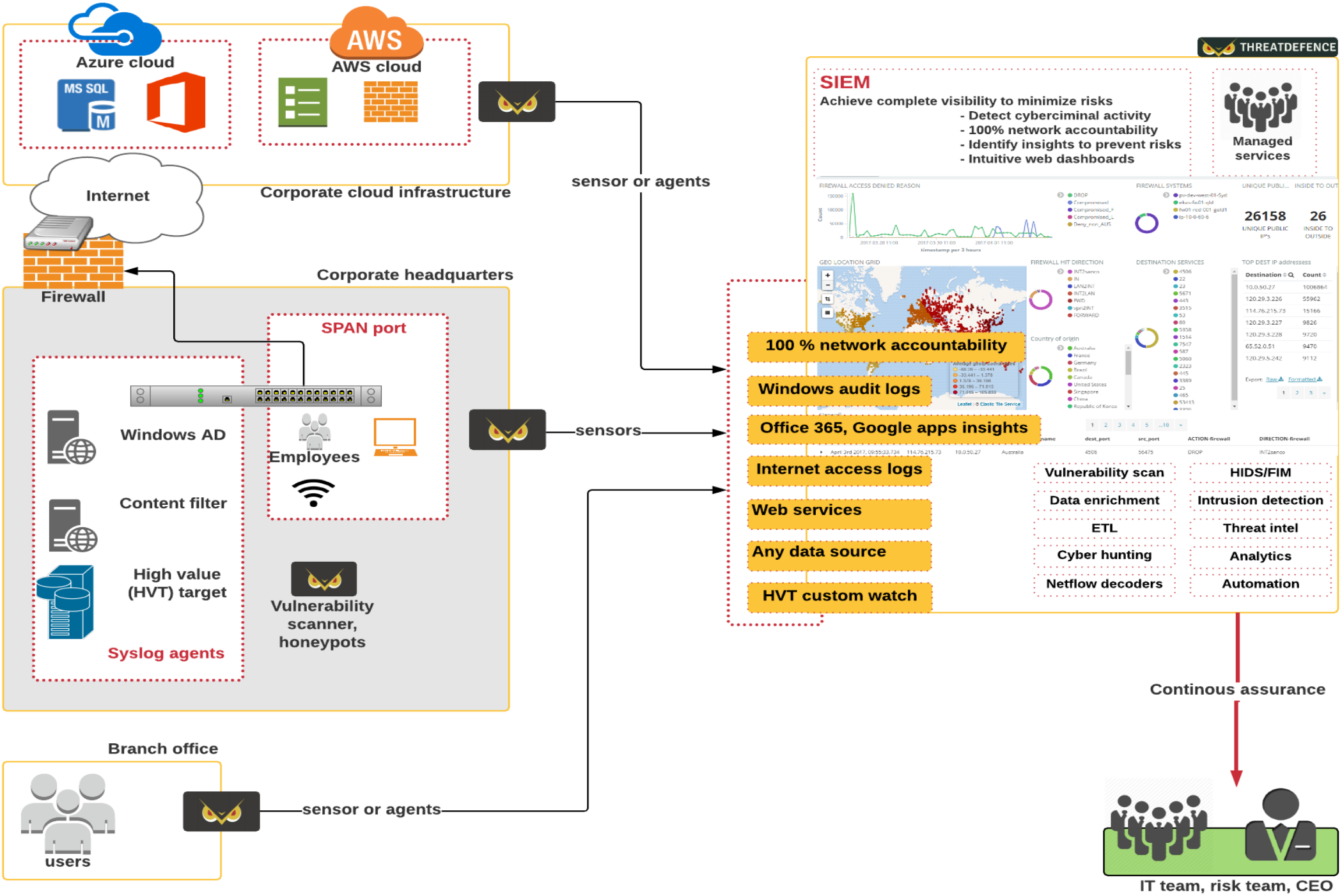
Customers typically set up multiple low cost large Flat Screen TV's to monitor events in real time. Critical alerts are both displayed on screen and emailed to the Network Operators.

Benefits:

- Rapid deployment. The system can be installed and reporting in ten (10) minutes.
- Operates in “Passive Mode”, with zero impact on production traffic.
- Seamless integration with current infrastructure – no changes to either hardware or software.
- Protects against emerging and undocumented threats such as Crypto Locker and Ransomware.
- It can receive log data from any type of audit file, for analysis and action.
- Detailed analytical reporting is available on a Daily, Weekly or Monthly basis, with customised reporting available as an option.
- We can assist in developing your security policies based on the data that enters your site from the Internet.
- Our Security Team will monitor, take action and report on all suspicious network traffic.
- Scalable – for organizations from 5 – 500+ users.
- Per user charge. Cost effective for organizations of all sizes, from SME to Enterprise.
- Cloud Orchestration + Rapid deployment = Fast ROI.
- API’S available for MSP platforms – currently Labtek, Enable, Maxfocus.

What’s makes us different:

- The service was developed locally, by security experts looking for a more comprehensive solution.
- The service is comprised of leading open source security and business intelligence (BI) tools, for example Suricata and Elastic Search – Vendor Independent.
- All logs from an organization’s entire infrastructure can be collected and stored in one location for convenient searching using business intelligence (BI) tools.
- The user interface is graphical and can be modified by the user in an intuitive and easily learnt manner.
- Daily and on-demand updates from live security intelligence feeds.
- The system has been tested and installed in a number of financial services companies in Australia, including a global financial corporation with 6000+ users.


Azure cloud
MS SQL
AWS
AWS cloud
Corporate cloud infrastructure
sensor or agents
Internet
Firewall
Corporate headquarters
SPAN port
Windows AD
Content filter
High value (HVT) target
Syslog agents
Employees
Vulnerability scanner, honeypots
sensors
Branch office
users
sensor or agents
THREATDEFENCE
SIEM
Achieve complete visibility to minimize risks
- Detect cyberciminal activity
- 100% network accountability
- Identify insights to prevent risks
- Intuitive web dashboards
Managed services
100 % network accountability
Windows audit logs
Office 365, Google apps insights
Internet access logs
Web services
Any data source
HVT custom watch
Vulnerability scan
HIDS/FIM
Data enrichment
Intrusion detection
ETL
Threat intel
Cyber hunting
Analytics
Netflow decoders
Automation
Continous assurance
IT team, risk team, CEO