iomart
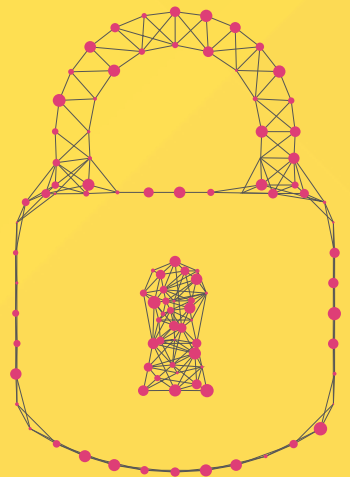
MANAGED SECURITY SERVICES

Make Your Business Cyber Secure

Cyber security is of critical concern to all of us. Criminals have turned their attention to the online world and are constantly evolving the methods they use to strike. Insider threats are also ever present. The results can be devastating.

Now is the time to take control. To protect your infrastructure and critical data, ensuring there are no security blind spots.

Many organisations use disparate security tools that issue threat alerts but require you to take the remedial action.

The Managed Security Service from iomart (iMSS) proactively defends, detects and responds. You can sleep easy knowing that our security and infrastructure experts are policing your systems every minute of the day.

iMSS protects against external and insider threats, exposes vulnerabilities and takes rapid action to overcome them.
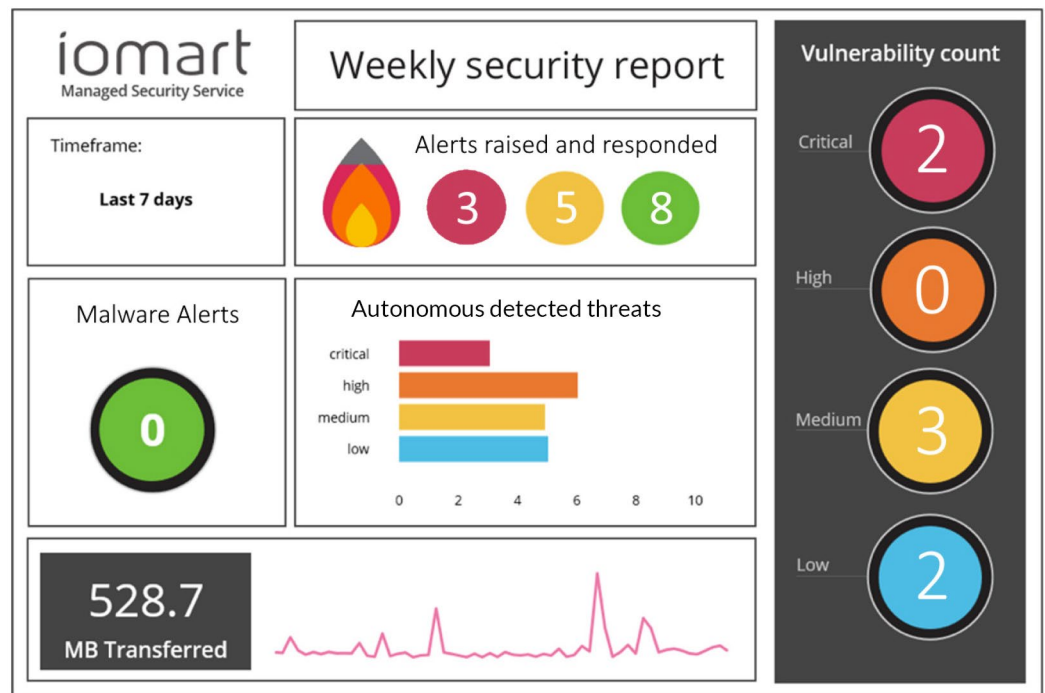
Protect	Protects from the perimeter to the desktop to stop attackers in their tracks
Detect	Uncovers evolving vulnerabilities and suspicious activity
Respond	Takes action to nulify the threat and update defences to prevent further compromise

The iMSS control panel gives a real-time view of the threat landscape and regular security reports are provided.

Example of executive security report

iMSS combines best-in-class technologies from the world's leading security companies with iomart's 20yrs+ of infrastructure provision and security expertise, to deliver complete peace of mind.

Get in touch to find out how our Managed Security Service can protect your business from current and emerging cyber-threats.

Learn more
www.iomart.com

Talk to us today
0800 040 7228 or info@iomart.com

The Threat Matrix

Global attacks are on the rise. From email compromise to traffic flood, from human error to deliberate malicious acts, there are many forms of attack and many ways to fall victim.

Man in the Middle

IP Theft

Phishing

Information Theft

Drive by Downloads

Personal Data Loss

Ransomware

Data Breach

Rogue Software

Document Theft

DDoS

Crypto Locker

Password Attacks

Detect Compromise

Detect Attacks

Reports/ Dashboards

iMSS
iomart

Detect Suspicious Activities

Detect Vulnerabilities
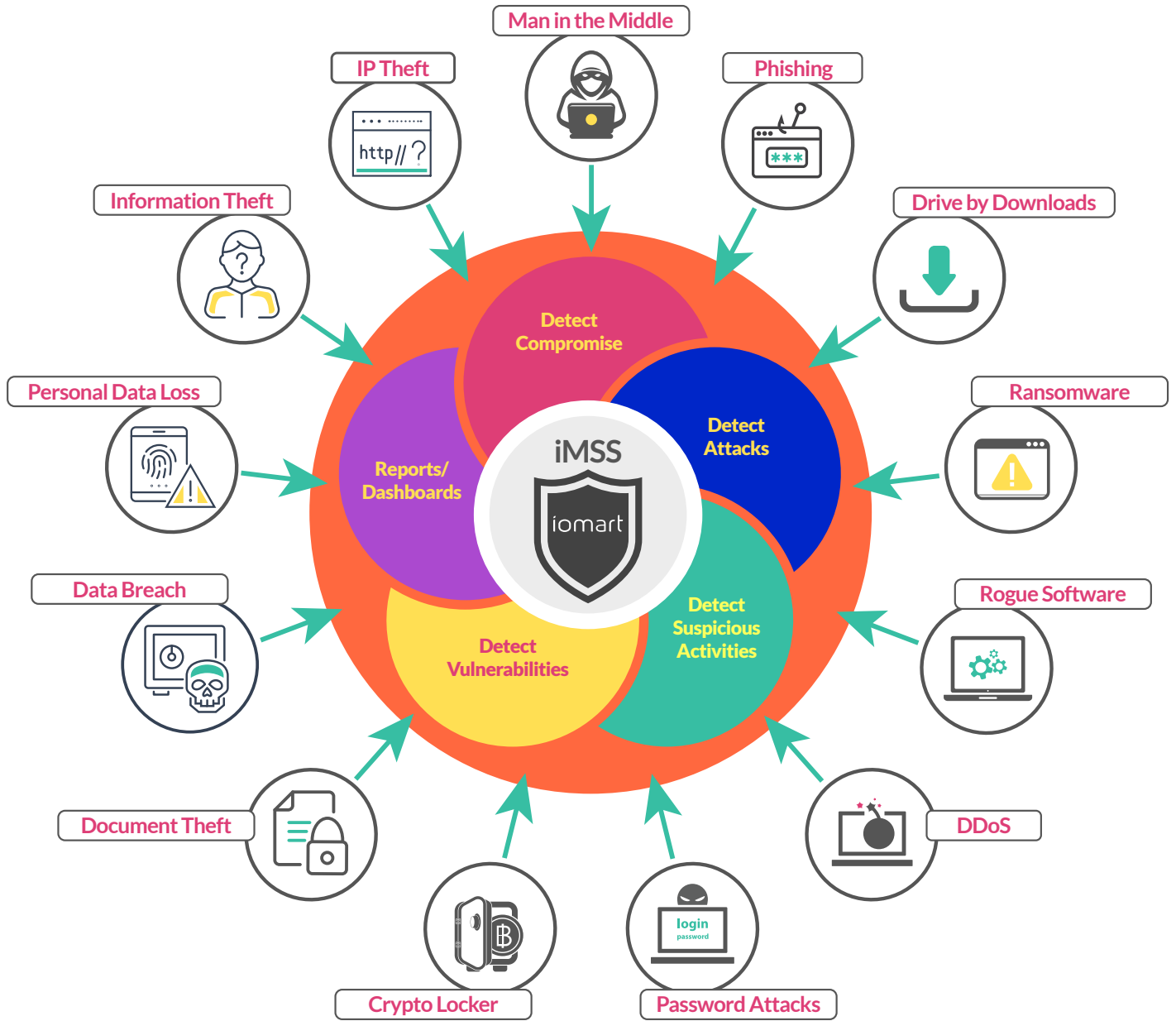
It is no longer a matter of if you will be hit. It is a matter of when.

Comprehensive defence-in-depth from iomart is the answer to this complex problem.

With over 20 years of experience managing secure infrastructure for our customers we understand how to protect you from, and react to, the growing threats you face.

We are proactive and vigilant on your behalf 24 hours a day, 7 days a week, 365 days a year.

Managed Security Service

Key Features

iMSS takes a data and business driven approach to cyber security, using best-in-class tools and a real-time dashboard to identify and protect you from all the threats you face.

The service is run from our Security Operations Centre which is located in the UK and staffed by certified security professionals. Security events are fed into our Security Information and Event Management System (SIEM) and acted upon by the iomart Security Analytics Team.

Protecting your organisation and your people from attack is a complicated business. This is why iMSS addresses so many different aspects of the threat landscape.

Defending Against Insider and External Threats

Intrusion Detection and Prevention

Service Capability
Ensures communication policies are being followed and IP systems are configured correctly. Analyses packets and protocols for known malware, flags variations to normal communications.

Benefits
Uses technologies ranging from next-generation firewalls to AI to detect and prevent intrusions.

Abnormal Access Protection

Service Capability
Builds on multi-factor authentication protection. Monitors normal account usage, including time and source of login and failed login attempts.

Benefits
Stops attacks before they can start or before payload can be delivered.

Malware and Ransomware Protection

Service Capability
In-depth protection through anti-virus monitoring, file and object monitoring, privileged user monitoring and systems, process and connection monitoring.

Benefits
Alerts on attempts to compromise a system so decisive action can be taken before malware is installed or fully delivers its payload.

Vulnerability Scanning

Service Capability
Monitors port policies, spots anomalous services and detects unpatched systems, applications and devices. Tests for latest known threats.

Benefits
Identifies the latest threats as they evolve and provides guidance on mitigation strategies.

AI Security

Service Capability
Learns what normal activity is for the environment being protected and alerts on activity that appears to be outside the usual patterns of behaviour.

Benefits
Complements traditional technologies by providing protection against unknown or rapidly evolving threats.

Data Loss Prevention

Service Capability
Monitors access to key resources and blocks unusual connections, ensuring access is restricted to authorised users.

Benefits
Detects unusual or unauthorised behaviour.

DDoS Prevention

Service Capability
Defends against three main categories of DDoS threats; volume-based attacks, application attacks and low-rate attacks.

Benefits
Active mitigation of a wide range of attacks that could take services offline.

Application Defence

Service Capability
Inspects and applies rules to online traffic and blocks attack. Checks if versions of applications and patch levels of Operating Systems are up-to-date. Monitors to measure performance and identify configuration change.

Benefits
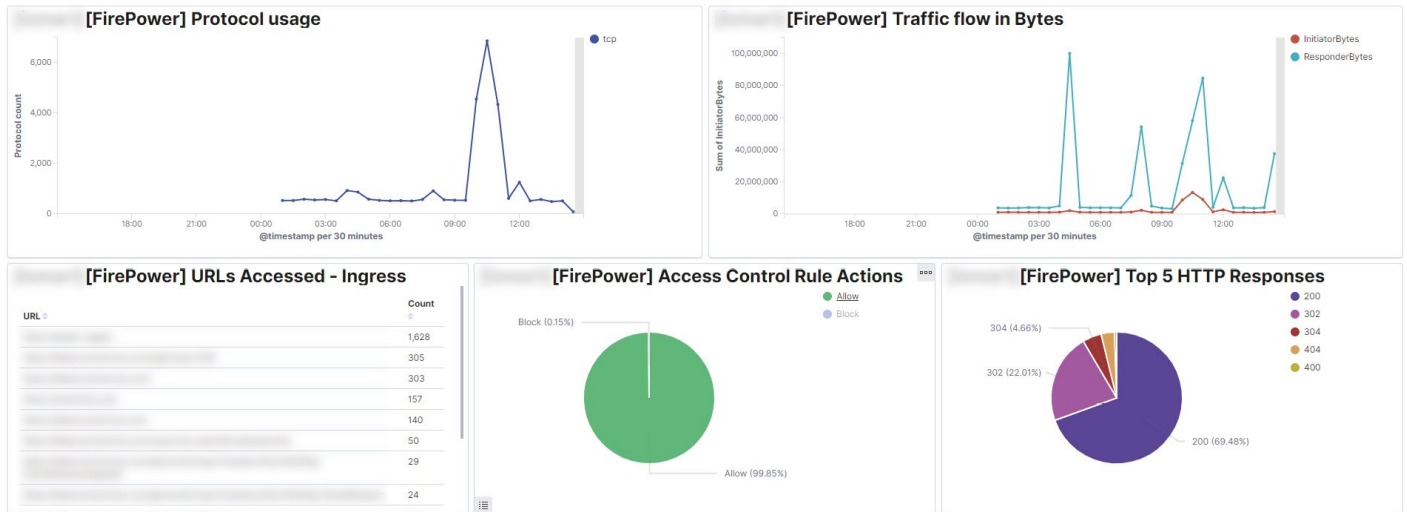Blocks threats and identifies version-related vulnerabilities.

Managed Security Service

Key Reports

Our Managed Security Service provides protection from BYOD through to the HyperCloud. Importantly, the reporting functions help demonstrate compliance with any relevant industry and regulatory standards.

As well as the dashboard, real-time live views are available of how each individual component of the service is performing.
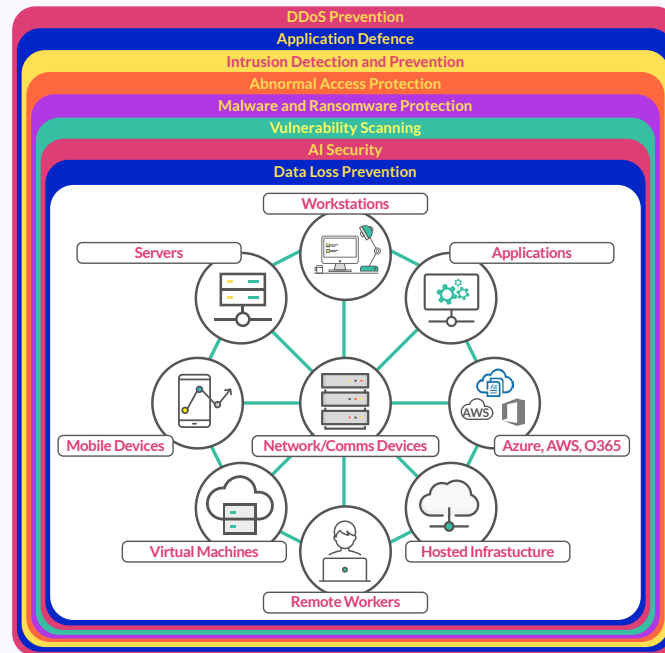
[FirePower] Protocol usage

[FirePower] Traffic flow in Bytes

[FirePower] URLs Accessed - Ingress

[FirePower] Access Control Rule Actions

[FirePower] Top 5 HTTP Responses

Sample dashboard view

Managed Security Service

Key Defences

Our comprehensive Managed Security Service monitors the behaviour of users, devices, applications, servers, infrastructure and networks. It has the power to ingest millions of log entries to search for intrusions and zero day threats and produce powerful custom reports which are then acted upon.

DDoS Prevention
Application Defence
Intrusion Detection and Prevention
Abnormal Access Protection
Malware and Ransomware Protection
Vulnerability Scanning
AI Security
Data Loss Prevention

Workstations
Servers
Applications
Mobile Devices
Network/Comms Devices
Azure, AWS, O365
Virtual Machines
Remote Workers
Hosted Infrastucture

With no hardware or licensing concerns, iMSS can scale according to your business requirements.

It offers comprehensive protection, ranging from the devices of remote workers, private cloud, through to the HyperClouds of Azure and AWS.

Using machine learning, integrated threat intelligence and expert analysis of the global threat landscape, iomart ensures you are protected and defended 24/7/365.

Get in touch to find out how our Managed Security Service can deliver next-generation cyber threat protection for your business.

Glasgow
Stockholm
Dublin
Amsterdam
Warsaw
Frankfurt
Vienna
Paris
Luxembourg
Madrid
Toronto
Chicago
Buffalo
Ashburn
Sacramento
Dallas & Garland
Los Angeles
Dubai
Tokyo
Hong Kong
Singapore
Jakarta
São Paulo
Sydney
Melbourne

Manchester
York
Nottingham
Leicester
St. Asaph
Maidenhead
London
Gosport

Why we're one of the World's Leading Cloud Companies

iomart provides globally supported managed services. Customers worldwide trust us to manage their critical infrastructure and work with them to overcome their technology challenges.

We are experts on all aspects of internet and cyber security, and our managed security service is at the forefront of current security provision.

Fully certified to supply secure managed services to both the public and private sector and with over 300 infrastructure and security experts on hand, we are ideally placed to deliver.

Secure from the internet, through our data centres, all the way to the device; whether you are under threat from a Denial of Service, Ransomware or any other type of cyber threat, we are here to help.

UKAS MANAGEMENT SYSTEMS 0026

Information Security

ISO 17789:2014 Cloud Computing Architecture

ISO 20000:9-2015 Service Management Guidance for Cloud Services

ISO 27005-2018 Information Security Risk Management

ISO 27017:2015 Cloud Service Information security controls

CYBER ESSENTIALS

PCI DSS COMPLIANT

ISO 27018-2019 Protection of Personally Identifiable Information in Public Cloud

ISO 27032:2012 Cybersecurity Techniques

ISO 27040:2015 IT Security Storage

ISO 27701-2019 Privacy Information Management

iomart

Learn more
www.iomart.com

Talk to us today
0800 040 7228 or info@iomart.com