iomart

Managed Security Services

Managed Security Services – An Overview

In an age of ever-evolving cyber threats it is important to take a multi-layered approach to security to protect your business critical assets.

Security is a key component of every service that iomart delivers. Whether it's a SaaS product or a managed platform, security is built in from the start to everything we do.

iomart's portfolio of security services offers unparalleled protection to secure your business critical environment.

We build secure managed platforms to meet the most demanding compliance and governance regimes, and in a rapidly evolving threat environment, iomart's security experts can monitor and manage the platform to ensure it remains secure and that, in the event of an attack, prompt and appropriate mitigation action is taken.

iomart is the most accredited managed cloud service provider in the UK. Our security consultants can assess and manage your strategic approach to cyber security and help you to meet your compliance and regulatory obligations.

Accredited ISO 9001:2015 Quality Management System	CYBER ESSENTIALS	Accredited ISO 27001:2013 Information Security Management System	National Cyber Security Centre	Accredited ISO 22301:2012 Business Continuity Management System
PCI DSS COMPLIANT	Accredited ISO 20000:2011 IT Service Management System	AICPA SOC	Accredited ISO 14001:2015 Environmental Management System	PSN Public Services Network CONNECTION CERTIFIED
iomart SECURE DATA ico. Information Commissioner's Office	iomart QUALITY ASSURED Incorporated ISO 27017:2015 Information security controls on cloud service Code of practice	Accredited ISO 50001:2011 Energy Management System	PSN Public Services Network SERVICE CERTIFIED	N3 Connecting Healthcare
iomart QUALITY ASSURED Incorporated ISO 27018:2014 Protection of Personal Identifiable Information Code of practice	iomart QUALITY ASSURED Incorporated ISO 27032:2012 Cybersecurity Guidelines	iomart QUALITY ASSURED Incorporated ISO 27040:2015 Storage Security Guidelines	iomart QUALITY ASSURED Incorporated ISO 17789:2014 Cloud Computing Reference Architecture	iomart QUALITY ASSURED Incorporated OHSAS 18001:2007 Occupational Health & Safety Management System

Managed Secure Platforms

iomart's Managed Secure Platforms service offers multi-layered protection to address the key security threats facing organisations and businesses today.

We deliver secure, robust and customised platforms to meet your compliance requirements and, as threats evolve, we make sure that not only do those platforms remain compliant, you can prove they have.

Platform Hardening

As part of the discovery and deployment process iomart works with you to assess the most secure configuration for your platform. This process takes into account industry best practice, the existing threat landscape, your security policies and your governance and system performance requirements, to ensure that on go-live your platform presents the minimum possible exposure to threats.

As the platform evolves, its profile is continually reviewed, with changes recommended and actioned where appropriate, to ensure that a minimal acceptable threat exposure is maintained.

Endpoint Protection

Endpoint Protection is deployed to prevent malware, exploits and zero-day threats from compromising the host. This prevents the malware from loading into memory and the exploit from comprising a running process.

Memory is monitored to identify compromised processes or applications and behavioural analysis ensures unusual user behaviour is reported.

Network Security

Securing a network 24x7 is a multi-layered task encompassing physical and logical design, access controls, monitoring and response.

The specific design and control mechanisms deployed will depend on many factors including the sensitivity of the data, internet requirements, compliance requirements and application requirements. These requirements will be implemented using a combination of: physical and logical segregation; port and protocol management; traffic management; access control; and a range of tools such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS) and Distributed Denial of Service.

Managed Secure Platforms

Access Monitoring

Access Monitoring ensures that the appropriate Security Information Policy is applied to the platform and that the approved use of this policy is monitored and can be reported on. It allows only authorised users or processes to have access to the platform and ensures any deviations are reported for remedial action.

Log Management

Effective Log Management is the key to a secure platform. Key components to be monitored are identified, based on the specific platform design. These components can include: firewalls, routers, applications, Operating Systems, authentication systems, endpoint agents etc. These log entries give a view into the activities taking place on the platform and are captured and forwarded to a central system for analysis. This data is processed and combined with other information to alert to threats to the platform or highlight activity that could lead to a threat.

Content Integrity Management

Content Integrity Management ensures that key pieces of data within the platform have not been compromised or changed. This protection extends across files, binaries, registry entries and user and system permissions.

Vulnerability Scanning

Threats and compliance requirements constantly evolve, so a platform that was perfectly secure when it was deployed can quickly become vulnerable. To address this iomart offers an internal and external scanning service that can be scheduled as frequently as is necessary, to ensure the platform continues to be as secure as possible and remains demonstrably compliant.

For further details email info@iomart.com or call 0800 040 7228