Cybersecurity Solutions
Trustwave Offshore Managed Security Services

Improving Security Outcomes

Information security has never been higher on the corporate agenda, with CEOs, Boards of Directors and Trustees now realising how fatal cybersecurity failures can really be. In reality, a major data breach will ruin not only an organisation's reputation, damage its brand and future prospects or plans, but also have serious consequences on the bottom line.

Against this backdrop, organisations are faced with the challenge of hiring, training and retaining in-house security experts, as well as efficiently using their costly skill sets. In many cases, moving to a hybrid or fully Managed Security Services Provider (MSSP) model may be the only viable way to effectively expand its security coverage to acceptable levels.

Sure has partnered with Trustwave, the leading cybersecurity service provider to exclusively offer Trustwave's full suite of security services, from network protection to SIEM and consultancy in the Channel Islands and Isle of Man, making Sure a one-stop-shop for network and information security. In combination with Sure's other security products this makes us the biggest provider of Managed Security in the islands.
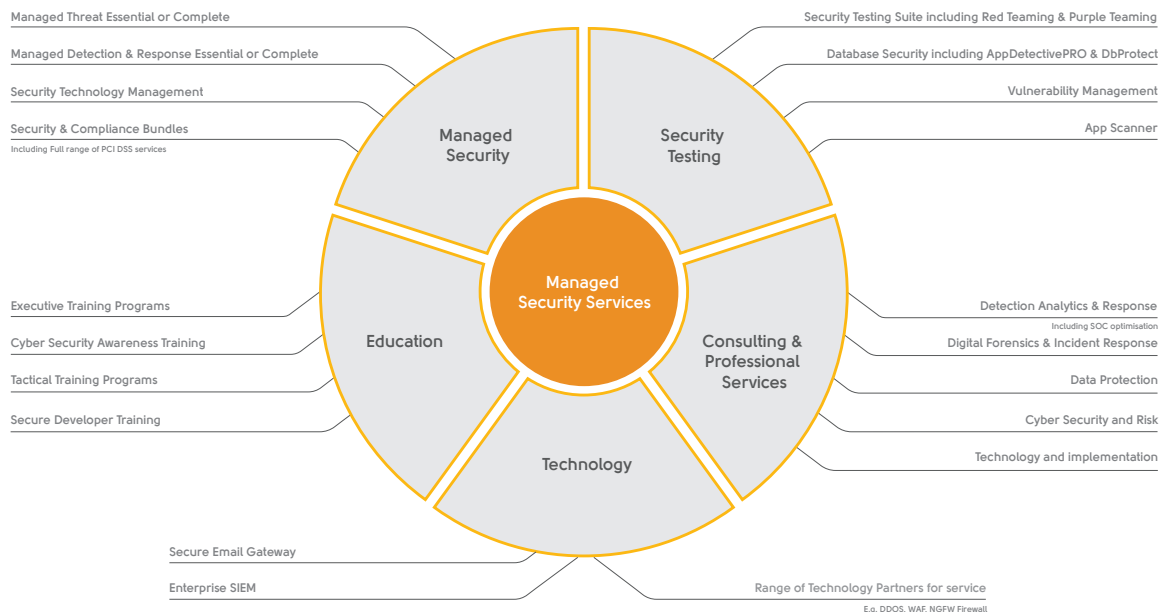
Securely Hosted in the Channel Islands

Security Information and Event Management (SIEM) is an approach to security management that combines SIM (Security Information Management) and SEM (Security Event Management) functions into one security management system.

Although Network Appliances and system software are good at catching and logging attacks, an SIEM system aggregates the data from multiple sources, identifies deviations from the norm and takes appropriate action.

Sure and Trustwave have created an offshore variant of their SIEM Security and Compliance Monitoring stack. The servers are hosted in Sure's highly secure Tier III data centres in the Channel Islands meaning data residency is guaranteed.

Sure & Trustwave - A Range of Products

Managed Threat Essential or Complete

Managed Detection & Response Essential or Complete

Security Technology Management

Security & Compliance Bundles
Including Full range of PCI DSS services

Security Testing Suite including Red Teaming & Purple Teaming

Database Security including AppDetectivePRO & DbProtect

Vulnerability Management

App Scanner

Managed Security

Security Testing

Managed Security Services

Executive Training Programs

Cyber Security Awareness Training

Tactical Training Programs

Secure Developer Training

Education

Consulting & Professional Services

Detection Analytics & Response
Including SOC optimisation

Digital Forensics & Incident Response

Data Protection

Cyber Security and Risk

Technology and implementation

Technology

Secure Email Gateway

Enterprise SIEM

Range of Technology Partners for service
E.g. DDOS, WAF, NGFW Firewall

Why you need a Security Information Management System

There are several drivers behind the requirement for security services.

Devices

Applications and data are now disparate: Meaning much of the intellectual property within a business now is contained in mobile devices, or across many geographically dispersed platforms owned by several service providers. However businesses are forced through regulation and compliance to protect data, both from a technical and process perspective.

Vectors

Threat vectors have moved significantly where assessment now covers users, access channels and disparate applications and platforms.

When Not If

Cyber-attacks are so frequent that it is now generally considered a "when" rather than "if" topic. Because of this, businesses are looking for the capability to monitor for and detect attacks when they happen. Then be prepared to act quickly in response.
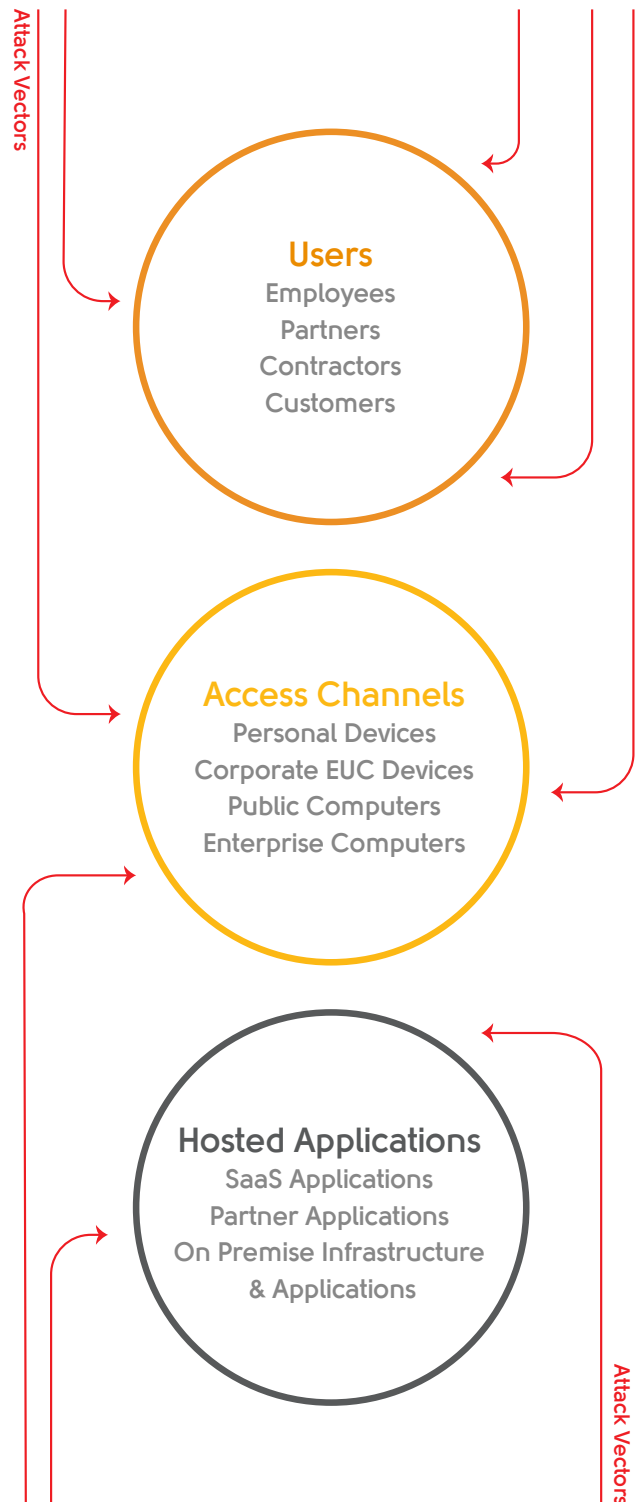
Disclosure

High profile breaches have driven awareness: Should there be a requirement to disclose an incident publicly, having a full understanding what occurred allows for an informed response rather than speculation in the media and the subsequent brand damage if the story changes.

Regulation & Compliance

General data regulations, and sector specific data regulations carry significant fines, where businesses are not meeting legislative requirements: New regulations such as the GDPR (General Data Protection Regulation) and the NIS (Network and Information Systems) Directive enforce a 72-hour reporting window.

Trustwave's Security and Compliance Monitoring services are designed to help security professionals monitor for and detect threats, by using the Trustwave platform to submit Log Data from supported Log Source devices for collection, correlation, storage, analysis, investigation and reporting.

Attack Vectors

Users
Employees
Partners
Contractors
Customers

Access Channels
Personal Devices
Corporate EUC Devices
Public Computers
Enterprise Computers

Hosted Applications
SaaS Applications
Partner Applications
On Premise Infrastructure
& Applications

Attack Vectors

We take security seriously

At Sure we host client data in our Data Centres, and carry sensitive data for Businesses, Government and Emergency Services. We believe in the products we sell and have implemented Trustwave internally to improve our own level of protection.