Insight | Connected Workforce

Solution Brief

Insight Security Configuration Maintenance Service

Background and business challenge

Transitioning to new ways of working has caused organisations to adjust their processes and methods of collaboration rapidly. With dispersed teams, new business challenges, and complex security issues, the needs of the agile workforce are evolving at lightning speed. As a result, IT organisations are having to deal with a series of challenges such as maintaining employee productivity, securely managing different working environments (onsite and remote) and staying innovative while remaining compliant.

"The threat landscape is becoming extremely difficult to map. Not only attackers are developing new techniques to evade security systems, but threats are growing in complexity and precision in targeted attacks."

(ENISA Threat Landscape Report 2020)

Security vulnerabilities can compromise both an organisation's current financial situation and endanger its future.

The damage cyberattacks do to organisations ranges from unauthorised access via a relatively simple hack to large-scale theft of sensitive data, resulting in prolonged downtime. Effective recovery is expensive and damages the confidence of customers and investors. If clients, vendors and suppliers can prove that a company did not take reasonable care with their data, it can suffer legal damages that can shut it down.

Related services

- Managed Detection and Response Service
- Security Awareness Program
- Microsoft Security + Azure Sentinel Workshop
- Microsoft Security Assessment Service
- Microsoft Compliance Assessment Service

Microsoft

Our solution

To keep up with the level of evolving cyberattacks, we have created a monthly Security Configuration Maintenance Service.

This service will help to secure end-user devices more effectively based on Insight and Microsoft Security best practices.

Incoming traffic, device protection and lateral movement – this last term refers to the techniques that a cyber attacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets.

Insight will provide the client with a monthly update of 3 sets of rules based on:

- Compliance policies to ensure only properly updated and configured devices can access company data and apps
- Configuration Profiles for the configuration settings of devices ensuring encryption, monitoring and protection on the end user device.
- App Protection Policies to protect company data.

Insight will document these new security configuration settings via a monthly change document for the client to review.
The client's IT department will assign the changes to end-users after testing the changes in their environment.

Business outcomes

By ensuring end-user devices maintain a proper security configuration we provide a significant barrier against malware, ransomware, and other cybersecurity threats before any damage occurs to an organisation. This allows organisations to reemain in control of their data and prevent potential loss of existing business. Maintaining regulatory compliance will allow an organisation to stay competitive in its market.

With the move to more flexible ways of working this service can help increase the cyber awareness of end-users and ensure optimal user experience, allowing the IT department to focus on strategic initiatives.

Why Insight?

Today, technology isn't just supporting the business; it's becoming the business. At Insight, we help you navigate complex challenges to develop new solutions and processes. We will help you manage today's priorities and prepare for tomorrow's needs.

Global scale & coverage	Operational excellence & systems	Software DNA	Services Solutions	Data centre transformation	Next-generation tech skills	App dev & IoT expertise	Insight Digital Workspace™	Partner alignment

Insight Connected Workforce

To know more about Insight ISCMS programme, contact your Account Manager.

0344 846 3333 | uk.insight.com