BYTES

Supporting Resiliency

Microsoft Secure Infrastructure Assessment

Customers have had to move quickly to respond to new demands and new pressures over the past two months.

Customers are pivoting to remote work and putting the safety of their employees, customers, and communities first.

Implementing technology and revised ways of working whilst moving at pace is tough. Combine this with maintaining security and it’s easy to see how vigilance could slip.

The **Secure Infrastructure Assessment** will provide practical quick wins to help ensure you maintain control.

How It Works

- The Secure Infrastructure Assessment utilises the **Cyber Security Assessment Tool (CSAT)** for collecting and analysing data.
- Office 365, SharePoint and Fileshares are included in the scope. All endpoints, fileservers, configurations, security rights and roles are scanned and analysed.
- CSAT collects information about accounts, firewall settings, installed applications, the OS/Service Pack and Fileshares. CSAT also exports users and groups from Active Directory and Azure AD.
- Based on these scans the Secure Infrastructure Assessment surfaces potential cyber threats and vulnerabilities.
- The resulting reports and workbook will provide practical recommendations and quick wins plus a high-level roadmap to help you regain vigilance and control.

Deliverables

- ✓ Action Plan to improve Cyber Security
- ✓ Urgent priority actions & quick wins
- ✓ Technical Data and Analysis
  - Endpoint details & risks
  - Inventory & version data
  - Suspicious applications
  - Admin privileges
  - Bad password attempts & suspicious logons
  - Data protection: Potential PII data
  - Externally shared Sharepoint data
  - Microsoft Secure Score
  - End of Life products
- ✓ Overall CIS (Center for Internet Security) Company Rating
  - Mapped to Basic, Foundational & Organisational controls

Microsoft