Customer Security Discovery

Network & Security Discovery collects detailed information on every asset, including those not physically connected to the network and Identifies all risks from misconfigurations, network vulnerabilities and user threats. **Network & Security Detective**, ensures accurate detailed auditing your infrastructure networks & security and Supports all environments, from on-prem, to remote, to cloud, to work-from-home
This simple checklist outlines some of the detail documentation, misconfigurations and vulnerabilities we collect when we review your IT assessments

- Missing critical patches
- Missing or out-of-date antivirus and spyware
- On-prem synch failures
- Computers with open listening ports
- Unsupported operating systems in o
- Enabled logins for former employees/vendors
- Weak/insufficient password requirements
- Systems with weak local passwords
- Multi-factor authentication not
- Non-administrators with Admin or Admin privileges
- Improper network share permissions
- Credit card/PII stored on unauthorized systems
- Excessive inactive SharePoint sites
- Firewall has open ports with known issues
- Lack of outbound (egress) filtering firewall
- Lack of content filtering
- Systems inside the network with anti-exploitable ports/protocols
- Application vulnerabilities
- TLS Deprecation
- Auto screen lock disabled use Account lock out disabled
- Incorrect and/or inconsistent application of security settings
- Confirm domain policies and local security policies match best practices
- Confirm recommended Microsoft enabled security controls implemented
- Large number of failed logins Domain
- Anomalous user logins
- Untested or missing backup/business continuity
- Improper physical security for server room
- Physical threats in server room exploitable
- Rogue or unauthorized devices and computers by the