# VITG Managed Security as a Service

| Managed Security as a Service (MSaaS) Features* | Essentials Bundle | Advanced Bundle | Resilience Bundle |
|---|---|---|---|
| **Endpoint Security**<br>• Next Gen Anti-Virus/Anti-Ransomware with EDR | ✓ | ✓ | ✓ |
| **Email Security**<br>• Advanced Email Filtering | ✓ | ✓ | ✓ |
| **Backups & Disaster Recovery**<br>• Microsoft 365 (M365) Cloud Backups | ✓ | ✓ | ✓ |
| **Security Awareness Training**<br>• Cyber Security Staff Training Platform | ✓ | ✓ | ✓ |
| **Application Hardening I**<br>• 3rd Party Patching | ✓ | ✓ | ✓ |
| **Identify Protection**<br>• Multi-Factor Authentication (MFA) | ✓ | ✓ | ✓ |
| **M365 Alerting and Monitoring**<br>• Automated SaaS Security | ✓ | ✓ | ✓ |
| **Email Security II**<br>• DKIM/SPF Records Review | | ✓ | ✓ |
| **Identity Protection II**<br>• Dark Web Monitoring | | ✓ | ✓ |
| **24/7 Security Operations Center**<br>• Monitoring, Alerting & Remediation | | ✓ | ✓ |
| **Application Hardening II**<br>• Application Whitelisting | | ✓ | ✓ |
| **Backups & Disaster Recovery II**<br>• M365 Backup Integrity Check (Annual) | | ✓ | ✓ |
| **Email Security III**<br>• DMARC Records Review | | | ✓ |
| **Penetration Testing**<br>• Real-Time & Automated Penetration Testing | | | ✓ |
| **Vulnerability Management**<br>• Vulnerability Reporting | | | ✓ |
| **Identity Protection II**<br>• Restrict and Review Admin Privileges<br>• Azure Active Directory Password Complexity | | | ✓ |
| **Data Security**<br>• Endpoint Management & Drive Encryption | | | ✓ |
| **Application Hardening III**<br>• Disable Macros | | | ✓ |
| **Backups & Disaster Recovery III**<br>• File Backup Integrity Test (Annual) | | | ✓ |

Bundles above require all users to have either a Microsoft Business Premium or Microsoft 365 E3 subscription and Windows Defender enabled to take advantage of the extra security features these licenses include.

# Endpoint Security

## What is it?

Endpoint Security (e.g. Anti-Virus/Anti-Ransomware Software) helps protect your computer against malicious tools and code used by cyber-criminals or aggressive marketing (Spyware). Next Generation Endpoint Security software is designed to monitor all facets of your computer software, ready to detect traditional viruses and suspicious behaviour that more advanced malware might use.

A system without Endpoint Security is just like a house with an open door.

## MSaaS Essentials/Advanced/Resilience Bundle Includes:

**Endpoint Security**

- Block potentially unwanted applications
- Real time endpoint security monitoring
- Behavioural-based ransomware detection and containment
- Device Isolation

# Email Security

## What is it?

Security to monitor emails that are being sent and received. Well designed and configured Email Security is required to filter unwanted email, such as spam, phishing attacks, embedded malware, and malicious web links, while continuing to deliver legitimate emails.

Email protection is critical in today's climate, as it's a very popular delivery mechanism for threats that target organisations and their staff, causing significant amounts of financial and reputational loss. For example, a phishing email is designed to trick users into giving up sensitive information, approving falsified bills, or downloading malware to infect the company network.

## MSaaS Essentials Bundle Includes:

**Email Security I**

- **Advanced Email Filtering** - Security to monitor emails that are being sent and received.

## MSaaS Advanced Bundle Includes:

**Email Security II**

- **DKIM/SPF Records Review** - A set of email authentication methods for proof that senders are truly authorized to send email from a particular domain.

## MSaaS Resilience Bundle Includes:

**Email Security III**

- **DMARC Records Review** - An open email authentication protocol that provides domain-level protection of the email channel.

# Backups & Disaster Recovery

## What is it?

Backing up critical data is essential. Backups protect you from disaster situations, both accidental and malicious. They protect against human errors, hardware failure, virus attacks, power failure, and natural disasters. Backups can help save time and money in recovery if these failures occur.

However, having a backup is not enough. They need to be regularly monitored, maintained, and tested to ensure their integrity. Restorations need to be planned and rehearsed in case of data loss or a disaster so the backups can be put to efficient use to save time and money when that comes.

## MSaaS Essentials Bundle Includes:

**Backups & Disaster Recovery I**

- **Microsoft 365 (M365 Cloud Backups) -** Daily, automated Microsoft Office 365 backup that auto-discovers new and/or altered content to back up.

## MSaaS Advanced Bundle Includes:

**Backups & Disaster Recovery II**

- **M365 Backup Integrity Check (Annual) - S**ervice to ensure proper operation of backup tasks and the consistency between the cloud backup data and local files until the complete restoration of backup data is needed.

## MSaaS Resilience Bundle Includes:

**Backups & Disaster Recovery III**

- **File Backup Integrity Test (Annual) -** An integrity test service to ensure continuity of the backed-up data in the event of a required data restore to the end point.

# Security Awareness Training

## What is it?

Security Awareness Training is the process of educating and testing employees to help protect your business against cyber-crimes including phishing and other social-engineering attacks. Within the three main building blocks of a layered IT security strategy: People and the Human element is an important one.

Security Awareness Training helps every employee in your organization recognize, avoid, and report potential threats that can compromise critical data and systems including phishing, malware, ransomware, and spyware. As part of the training, mock phishing and other attack simulations are typically used to test and reinforce good behaviour.

## MSaaS Essentials/Advanced/Resilience Bundle Includes:

**Cyber Security Staff Training Platform**

- Training for employees to identify and respond appropriately to information security threats by encouraging safe and secure use of computers. Information, email, and the internet.

# Application Hardening

## What is it?

Ensuring your software remains fully patched is critical. When vulnerabilities in software are found, vendors of the software release patches to fix the vulnerability. It is particularly important for these patches to be applied in a timely manner, before attackers have the chance to exploit them. This is one way of 'hardening' Applications on computers, as recommended by the ACSC's Essential 8 Mitigation Strategies.

VITG would like to ensure your organisation remains clean and secure by having a centrally managed platform that manages these updates, reporting on software that is not compliant and promptly patching them.

Additionally, having a centrally managed platform that will scan the entire corporate network for all network attached devices for vulnerabilities is key. Many organisations will monitor network attached devices, such as switches, printers and wireless access points for connectivity, but not their firmware update status. This proposal will cover vulnerability management reporting but not remediation. Due to the nature of vulnerability remediation, a separate scope will need to be provided on a case-by-case basis for remediation.

## MSaaS Essentials Bundle Includes:

**Application Hardening I**

- **3rd Party Patch Management -** The process of testing, acquiring and installing patches for commonly used third party applications that are specifically relevant for the end point. This ensures the device is running optimally.

## MSaaS Advanced Bundle Includes:

**Application Hardening II**

- **Application Whitelisting -** The practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system.

## MSaaS Resilience Bundle Includes:

**Application Hardening III**

- **Disable Macros -** Macros can pose vulnerabilities to end point devices via embedded scripted viruses in certain macros which the best defence is to block the macro before an exploit can occur.

# Identity Protection

## What is it?

Identity Protection refers to many security methods, but a general view can be described as the practice of making sure that company (and personal) information that makes up the online or real-life self is protected and not stolen. If attackers can steal parts or all your sensitive data related to your identity, the attacker may impersonate you and could gain access to your bank account, company email mailbox and online data.

## Why should I use MFA?

Risk reduction is critical for organizations, which is why MFA use is growing exponentially. In a world where credential harvesting is a constant threat and over 80% of hacking-related breaches are caused by stolen or weak passwords, this kind of comprehensive authentication solution is essential. With MFA, it's no longer about granting access based on traditional usernames and passwords; it's about granting access based on multiple weighted factors, reducing the risks of compromised passwords. It adds another layer of protection from the kinds of damaging attacks that cost organizations millions.

Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- **Something you know** - typically a password.
- **Something you have** - such as a trusted device that is not easily duplicated, like a mobile phone.
- **Something you are** - biometrics like a fingerprint or face scan.

Multi-Factor Authentication helps safeguard access to data and applications while maintaining simplicity.

## MSaaS Essentials Bundle Includes:

**Identity Protection I**

- **Multi-Factor Authentication (MFA)** - An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.

## MSaaS Advanced Bundle Includes:

**Identity Protection II**

- **Dark Web Monitoring** - A service which regularly searches places on the dark web where information is traded and sold, looking for your information.

## MSaaS Resilience Bundle Includes:

**Identity Protection III**

- **Restrict Admin Privileges** - Privileges determine the admin's controls, information they can access, and tasks they can perform on the end point device. Restrict Admin Privileges ensures no unnecessary privileges are provided to users.
- **Annual Admin Review** - Admin privileges are reviewed from time to time to ensure the right users have the correct levels of access.
- **Azure Active Directory Password Complexity** - Ensures all users create a complex and secure password.

# M365 Alerting and Monitoring

## What is it?

When it comes to cybersecurity, organisations need to stay ahead of the game to detect and stop unauthorized activity in client applications by immediately locking the account when a breach occurs.

The technology landscape for many organisations has evolved and unfortunately so have cybersecurity threats. These threats come from external and internal sources, they find holes in networks and also infiltrate through the Software as a Service applications that many clients use every day to run their businesses. Constant but unintrusive, real-time monitoring facilitates application hygiene necessary for proper end user protection in an evolving landscape.

## MSaaS Essentials Bundle Includes:

### M365 Alerting and Monitoring

- **Automated SaaS Security –** Providing valuable time to properly act before a bad actor can inflict additional damage. The solution provides unified, real-time monitoring to protect the endpoint against data theft, data-at-risk and bad actors.

# 24/7 Security Operations Center

## What is it?

A Security Operations Center (SOC) is a managed detection and response service that leverages a threat monitoring platform to detect malicious and suspicious activity across three critical attack vectors: Endpoint, Network and Cloud. Trained and certified Cybersecurity Analysts then hunt, triage and escalate when actionable threats are discovered.

## MSaaS Advanced Bundle Includes:

### Monitoring, Alerting & Remediation

- **Continuous Monitoring –** Around the clock protection with real-time advanced threat detection.
- **Advanced Security Stack –** 100% purpose-built platform backed by more than 50 years security experience.
- **Breach Detection –** Catching sophisticated and advanced threats that bypass traditional AV and perimeter security solutions.
- **Threat Hunting –** An elite cybersecurity team proactively hunts for malicious activities.

# Penetration Testing

## What is it?

Penetration testing is an automated network penetration test platform that allows organizations to conduct a full-scale automated network penetration test at any time to assess their infrastructure. In a time where news of data breaches is becoming "the new normal," the need for organizations to evaluate their overall risk and avoid becoming the next victim has become critical. Organizations simply can't protect themselves from risks they're unaware of and require a simplified process of identifying new threats within their environment on an on-going basis, at any time.

## MSaaS Resilience Bundle Includes:

### Penetration Testing

- **Real-Time & Automated Penetration Testing -** Automated and full-scale penetration test platform that makes network penetration testing more scalable, accurate, faster, consistent, and not prone to human error.

# Vulnerability Management

## What is it?

Vulnerability management is a continuous, proactive, and often automated process that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program. By identifying, assessing, and addressing potential security weaknesses, organizations can help prevent attacks and minimize damage if one does occur.

The goal of vulnerability management is to reduce the organization's overall risk exposure by mitigating as many vulnerabilities as possible. This can be a challenging task, given the number of potential vulnerabilities and the limited resources available for remediation. Vulnerability management should be a continuous process to keep up with new and emerging threats and changing environments.

## MSaaS Resilience Bundle Includes:

### Vulnerability Management

- **Vulnerability Reporting -** The process of identifying, assessing, and reporting on security vulnerabilities across all devices that are attached to your network. A vulnerability management report documents the findings and recommendations to remediate whatever security vulnerabilities the assessment found.

# Data Security

## What is it?

Data security is the practice of protecting digital information from unauthorised access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

When properly implemented, robust data security strategies will protect an organization's information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among the leading causes of data breaches today. Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used. Ideally, these tools should be able to apply protections like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements.

## MSaaS Resilience Bundle Includes:

**Data Security**

- **Endpoint Enrolment** - The process of setting up the endpoint device ready to align with your organisation's policies to provide management and safeguard data.
- **Device Encryption** - The security practice of protecting the contents of the device from unauthorised access by encrypting the data.