

**Introduction:**

Thank you for choosing Echo Cloud Limited as your IT Support MSP provider. We hope to have a sustainable, strong and long lasting relationship with your company and we hope you will find our service second to none in regards to response times and vision for new products that will help your business.

We believe technology should empower your business, not hinder it.  
Our mission is to provide the most reliable and robust communication systems for your business, alleviating constant headaches so you can better focus on your day-to-day activities.

Below you will find a programmed description of the services you have opted in with us and details about those products and services.

**IT Support Unlimited Service:**

This is unlimited support 8.30 am to 5.00 pm Monday to Friday excl. Bank Holidays.

Email issues and troubleshooting  
Server & Break fix support  
Printer configuration  
New user setups  
PC & Laptop Break-fixes  
Active Directory & Azure troubleshooting and support  
Password changes  
Software installation and troubleshooting  
Technical contact for liaising with third-party systems  
Typically, most things that are required to maintain the status quo of your network.

At Echo we don't mark things with hours. This is a managed service in which we commit to being there as and when you need us for the small and big stuff.

We understand all businesses require help and technical support for a range of technology problems, from computers and printers to networks and software packages and we are there to help you with these needs.



## SLA's:

As a Echo client, we hope you enjoy a trouble free service with your IT Support service for many years. These days Cloud platforms & Hardware are built to the highest standards, however even the best engineered products can occasionally go wrong, lose updates and functions or get damaged or cause downtime.

That is why we offer all our customers a service and support agreement with completely unlimited cover for their IT systems. When you take out unlimited support you are not only getting a first class product, but also our commitment to provide a comprehensive after sales service. A system break down can be a real headache:

- PC or laptop shutdown lost productivity & Potential Major downtime
- Server Failure complete loss of productivity
- Out Of Date Firmware Loss of speed and Broadcast
- Total system failure stopping your business from working
- Repairs can be expensive as replacing faulty equipment could cost hundreds

## The Solution

For peace of mind your IT System will be protected by a service and support agreement providing you with:

- No call out charges which could be costly for multiple visits
- Response times \*\* 2 hour response for total system failure
- Hassle free help line will assist with all support and maintenance enquiries
- Comprehensive parts and labour cover with the majority of equipment easily available

With a dedicated support team we aim to provide you with peace of mind throughout the lifetime of the support. So if for any reason your system should develop a fault, simply contact us and help will be on the way. We have a dedicated team 9-5 Monday to Friday to assist you.

## What is covered?

If you suffer issues or change queries you are covered for all call outs, parts and labour. There is no limit to the number of call outs and additional system support.

## What is not covered?

The cover does not include damage caused by external influences such as power spikes, vandalism, theft, fire, flood, accidental damage etc. Please note also any hardware changes that require full upgrades will be chargeable ie new laptops, PC's and or Servers.

Therefore we present to you our standard SLA Times.

- System Failures & Outage/Disk Failures – 1–2-hour response time either on site or remotely.



- Urgent matters – 2–4-hour response time either on site or remotely.
- Basic queries or standard changes – 4–8-hour response time either on site or remotely.

### **RMM:**

We use an RMM product called SuperOps. Thi

offers a unified Remote Monitoring and Management (RMM) and Professional Services Automation (PSA) platform designed for modern Managed Service Providers (MSPs). It leverages AI and automation to streamline IT management, offering features like asset management, policy management, patch management, and more. This platform aims to provide a single pane of glass for MSPs, simplifying their operations and enhancing service delivery.

Here's a more detailed breakdown:

- **Unified Platform:**

SuperOps combines RMM and PSA capabilities into one integrated solution, eliminating the need for multiple tools and enhancing data flow between different functions.

- **RMM Features:**

The RMM component allows for remote monitoring and management of client networks, servers, workstations, and other endpoints. This includes real-time asset monitoring, granular information gathering, and proactive issue resolution.

- **PSA Features:**

The PSA component handles project management, ticketing, IT documentation, and other administrative tasks, helping MSPs manage their client interactions and projects effectively.

- **AI and Automation:**

SuperOps utilizes AI and automation to streamline workflows, automate tasks like patching and alerting, and improve overall efficiency.

- **Modern Design:**

The platform boasts a modern, user-friendly interface, aiming for intuitive navigation and ease of use for MSPs.

- **Focus on Customer Success:**

SuperOps emphasizes its commitment to customer success, providing tools and support to help MSPs grow their businesses.

- **Scalability:**

The platform is designed to support the needs of growing MSPs, providing tools for efficient resource management and scalable operations.

- **Intelligent Alerting:**

SuperOps offers intelligent alerting capabilities, allowing for proactive identification and resolution of potential issues based on configurable conditions and actions.

- **Runbooks:**

SuperOps provides runbooks to guide technicians through common tasks and procedures, ensuring consistency and efficiency in service delivery.



### **Backups & Disaster Recovery:**

You are covered for onsite and offsite backups.

We use two products to give you this desired effect.

From the servers we backup to an onsite local NAS box using software called Acronis.

Then from the NAS box we use a cloud based platform called AWS which sends that data from the NAS offsite into the cloud.

In the event of a disaster and the servers failed to operate we load up a temp server in our workshop, log into the AWS platform and restore a backup onto that server and bring it to your site.

A good restore with sensible data over a good broadband connection can take only 3-4 days. If it's multiple servers then the recommended allowance is 7 days.

We can offer an annual test restore to prove this works accordingly.

This is available on request.

Below is a description of both products used



AWS Backup is a fully managed service offered by [Amazon Web Services](#) that simplifies and centralizes data protection across various AWS services, including both cloud and on-premises workloads. It allows users to automate and consolidate backup tasks, monitor activity, and manage backups from a single console. This helps in safeguarding data, meeting compliance requirements, and recovering from ransomware attacks or other disasters.

Here's a more detailed breakdown:

Key Features and Capabilities:

- **Centralized Management:**

Provides a unified console, APIs, and the AWS CLI for managing backups across multiple AWS services.

- **Policy-Based Automation:**

Allows you to define backup policies that specify schedules, retention periods, and lifecycle rules for your backups.



### **Cross-Region and Cross-Account Backups:**

Supports backing up data to different AWS regions and accounts, enhancing disaster recovery and compliance.

- **Immutable Backups:**

Offers features like [vaults](#) and [restore testing](#) to protect against ransomware and accidental data loss.

- **Integration with Other AWS Services:**

Seamlessly integrates with services like Amazon CloudWatch, AWS CloudTrail, and AWS Organizations.

- **Compliance Support:**

Provides insights and analytics for data protection policies and operations, helping meet compliance requirements.

How it Works:

1. **1. Define Backup Policies:**

Create backup plans that specify backup schedules, retention periods, and other settings for your resources.

2. **2. Assign Resources:**

Associate your AWS resources (like EC2 instances, RDS databases, etc.) with the appropriate backup plans using tags or resource names.

3. **3. Automated Backups:**

AWS Backup automatically creates and manages backups according to your defined policies.

4. **4. Recovery:**

Restore data from backups when needed, either individual resources or entire applications.

Benefits:

- **Reduced Operational Overhead:** Automates and simplifies backup processes, freeing up time and resources.
- **Enhanced Data Protection:** Protects against data loss due to ransomware, accidental deletion, or other issues.
- **Improved Compliance:** Helps meet regulatory and business requirements for data protection.
- **Cost Optimization:** Provides granular control over backup storage and retention, helping manage costs.
- **Scalability:** Scales to handle large data volumes and complex environments.



# Acronis

Acronis offers a range of backup solutions designed to protect data across various environments, including physical servers, virtual machines, cloud workloads, endpoints like PCs and Macs, and mobile devices. Their core offerings integrate backup capabilities with cybersecurity features, aiming to provide a holistic approach to data protection and disaster recovery.

Here's a breakdown of the key aspects of Acronis backup solutions:

## 1. Integrated cyber protection

- Unified solution: Acronis Cyber Protect, for example, combines data protection (backup and disaster recovery) with cybersecurity (anti-malware, anti-ransomware, URL filtering) and endpoint management (patching, vulnerability assessments) in a single platform, eliminating the need for multiple disparate tools.
- Advanced threat detection: Acronis solutions employ AI-based behavioral detection and real-time monitoring to identify and proactively prevent cyberattacks, including ransomware and zero-day threats.
- Ransomware protection: Acronis Active Protection guards files, backups, and the backup agent against ransomware, automatically restoring impacted files if an attack is detected.
- Secure backups: Backups are protected with AES-256 encryption both during transfer and at rest, and optional password protection can be added for enhanced security



### **ESET Security:**

Echo will provide you with Eset Advanced Licenses for pure protection for each user and servers including Hyper V usage. Please see below a detailed description on this product.



ESET PROTECT Advanced is a business-focused security solution that offers multi-layered protection, including endpoint, server, and data security features. It builds upon the capabilities of ESET PROTECT Entry by adding Full Disk Encryption and Advanced Threat Defense. This comprehensive approach helps businesses protect against ransomware, zero-day threats, and other advanced attacks, while also ensuring compliance with data regulations.

Here's a more detailed breakdown:

#### Core Features:

- [Endpoint Protection:](#)

Protects computers, smartphones, and virtual machines with advanced, multilayered security.

- [Server Security:](#)

Provides real-time protection for company data passing through file servers.

- [Full Disk Encryption:](#)

Offers a robust encryption solution for system disks, partitions, or entire devices, helping businesses comply with data protection regulations.

- [Advanced Threat Defense \(ESET LiveGuard Advanced\):](#)

Analyzes suspicious files in a cloud sandbox environment to identify and neutralize zero-day threats and other new, unknown attacks.

Benefits:



- **Comprehensive Protection:**

ESET PROTECT Advanced provides a broad range of security features, including ransomware and zero-day attack protection.

- **Data Security:**

Full Disk Encryption helps safeguard sensitive data and ensures compliance with data protection regulations.

- **Ease of Management:**

Offers a unified management console for easy visibility and control across the network.

- **Proactive Security:**

Advanced Threat Defense helps mitigate risks from emerging and unknown threats.

- **Multi-Platform Support:**

Compatible with Windows, macOS, iOS, and Android devices, as well as Linux servers.

### **Mimecast:**

Echo will provide you with a product called Mimecast. A package that protects and blocks out any potential email threats across your business.

# **mimecast™**

Mimecast licenses are subscriptions to a cloud-based email security, archiving, and continuity service. They provide protection against various email threats, including phishing, malware, and spam, while also ensuring email continuity during outages and facilitating secure messaging and archiving. Licenses are typically purchased for a specific number of users or seats and can be tailored to meet an organization's specific needs.

Here's a more detailed breakdown:

Key Features & Benefits:

- **Email Security:**

Mimecast licenses offer robust email security solutions, including protection against phishing, malware, spam, and advanced attacks like spear-phishing and impersonation.

- **Cyber Resilience:**

They ensure business continuity by providing access to email during outages, keeping employees productive and minimizing downtime.

- **Secure Messaging:**





Mimecast facilitates secure and compliant communication with features like encrypted messaging and large file sending.

- **Archiving:**

They offer long-term email archiving for compliance, e-discovery, and data retention purposes.

- **Integration:**

Mimecast integrates with various platforms like Microsoft 365, providing a seamless user experience.

- **Scalability:**

Mimecast licenses can be scaled up or down based on an organization's needs, allowing for flexibility and cost-effectiveness.

- **Simplified Management:**

Mimecast's platform is designed for easy management, with a single administration console for all services.

Licensing Models:

- **Subscription-based:**

Mimecast licenses are typically subscription-based, with varying durations (e.g., annual or multi-year).

- **Seat-based or User-based:**

Licenses are often purchased based on the number of users or active mailboxes, [according to a Reddit thread](#).

- **Bundled Services:**

Mimecast offers different bundles of services, such as Email Security, Archiving, and Continuity, allowing organizations to choose the best fit for their requirements.

- **Add-ons:**

Organizations can also add specific features, like [Secure Messaging](#), to their existing Mimecast license.

## **Terms & Conditions:**

A full list of our terms and conditions can be found on our webpage [here](#).