Service description

Summary

Daisy Protect MDR is a comprehensive, managed cybersecurity solution designed to protect businesses from advanced threats. It combines cutting-edge endpoint protection with 24/7 monitoring, detection, and response by a team of expert security professionals. The service includes proactive threat hunting, automated threat remediation, and detailed reporting. It integrates seamlessly with existing IT infrastructure and provides end-to-end protection for hybrid environments, ensuring businesses stay secure from emerging risks. Daisy Protect MDR offers scalable, expert-driven defence to minimise downtime and mitigate threats quickly.

What is protected

Daisy Protect MDR offers a comprehensive set of protections and services for businesses. Here's a list of what's typically covered with the service:

FEATURE / SERVICE	DAISY PROTECT MDR
ENDPOINT PROTECTION	☑
ADVANCED THREAT DETECTION	☑
NETWORK PROTECTION	☑
CLOUD APPLICATION PROTECTION	☑
MOBILE THREAT DEFENCE	☑
CONTINUAL EXPERT-LED THREAT HUNTING	☑
DIGITAL FORENSIC INCIDENT RESPONSE (DFIR) ASSISTANCE	☑
MALWARE DETECTION SUPPORT AND ANALYSIS	☑
ADVANCED EMAIL SECURITY	☑
WEB AND APPLICATION CONTROL	☑
FIREWALL & DEVICE CONTROL	☑
CLOUD SANDBOX	☑
CUSTOMISED RULES AND EXCLUSIONS OPTIMISATION	☑
INTEGRATION WITH SIEM & OTHER SECURITY TOOLS	☑
24/7 EXPERT-LED CONTINUOUS MONITORING, HUNTING TRIAGE AND RESPONSE	☑
VULNERABILITY & PATCH MANAGEMENT	☑
EXPERT ASSISTANCE FOR MDR ALERTS WITH MORE CONTEXT	☑
REMOTE MANAGEMENT CONTROLS	☑
DAISY BACKUP	☑

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Service description

Endpoint protection

Endpoint protection is a comprehensive cybersecurity solution designed to protect you from a wide range of threats, including malware, ransomware, viruses, and phishing attacks. It provides real-time antivirus, antispyware, firewall and web control, alongside specialised features like ransomware protection, email security and device control.

Advanced threat detection

Advanced threat protection is a cybersecurity solution designed to detect, analyse and respond to sophisticated threats. It combines multiple layers of security, including real-time malware detection, behavioural analysis, machine learning and sandboxing, to identify and block advanced threats like zero-day attacks, ransomware and targeted intrusions.

Network protection

Network protection is a security solution designed to safeguard your network infrastructure from a variety of cyber threats. It includes advanced firewall protection, intrusion detection and intrusion prevention systems (IDS/IPS), along with secure VPN and web filtering to prevent unauthorised access and malicious activity. By monitoring network traffic and blocking harmful connections, network protection helps prevent attacks such as hacking, data breaches, and malware manipulation.

Cloud application protection

Cloud app protection primarily supports security for popular cloud applications like Microsoft 365 and Google Workspace. It offers comprehensive protection for services within these ecosystems, including Outlook, Teams, OneDrive, SharePoint, Exchange and Google Drive. Our solution is designed to secure emails, documents and collaborative tools by detecting and blocking threats such as phishing, malware and ransomware. This protection helps safeguard sensitive data and ensures that cloud-based communication and collaboration are secure from cyber threats.

Mobile threat defence

Mobile threat defence will protect your smartphones and tablets from malware, phishing, and data breaches. It offers real-time threat detection, app scanning, anti-theft tools, and remote device management for both Android and iOS devices. It ensures mobile security and safeguards sensitive data from various cyber threats.

Continual expert-led threat hunting

Continual expert-led threat hunting is a proactive service where security professionals actively search for hidden threats within your network. By using advanced tools and threat intelligence, experts identify and mitigate sophisticated attacks, such as zero-day exploits and insider threats, before they cause damage.

Digital Forensic Incident Response (DFIR) assistance

We offer online investigations and technical cybersecurity consultations, focusing on malware and cybersecurity attacks. PR issues are not included.

Malware detection support

Malware detection support and analysis offers expert assistance in identifying, analysing and mitigating malware threats. This service helps detect malware that may evade standard security measures, providing in-depth analysis to understand the threat's behaviour, origin and impact. The team uses advanced tools and techniques to deliver detailed reports, recommend remediation steps and enhance overall security to prevent future infections.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Advanced email security

Advanced email security is a robust solution designed to protect you from email-based threats, including phishing, malware, spam, and ransomware. It uses advanced filtering techniques to block malicious attachments, links, and suspicious emails before they reach the inbox.

Web and application control

Web and application control is a security feature that helps manage and control access to websites and applications on the network. It allows administrators to block access to malicious or inappropriate websites, limit the use of certain applications and prevent the execution of unauthorised software.

Firewall and device control

Firewall and device control provides robust protection against unauthorised network access and external threats. The firewall monitors incoming and outgoing network traffic to block potential attacks, ensuring secure communication.

Cloud Sandbox

Cloud Sandbox is an advanced security feature that isolates and analyses suspicious files or programs in a controlled, virtual environment. When a potentially malicious file is detected, it is executed in the cloud-based sandbox to observe its behaviour and identify any harmful actions, such as malware or ransomware.

Customised rules and exclusions optimisation

We start by analysing your environment for optimisation. We check for false positives like files, URLs, domains, or IPs, create exclusions, and provide information on any potential threats or weaknesses. The rules and exclusions are tailored to your environment.

Integration with SIEM and other security tools

Daisy Protect MDR integrates with SIEM (Security Information and Event Management) and other security tools to share real-time security event data, enabling more effective monitoring, correlation of alerts, and faster incident response.

24/7 expert-led monitoring, hunting, triage, and response

Our round-the-clock service combines internal and external feeds, advanced monitoring, and detection techniques to protect your environment. This service identifies hidden malicious activity, containing and removing threats to prevent significant damage.

Vulnerability & Patch Management

Vulnerability & Patch Management will help identify and fix security vulnerabilities in your software and systems. It automates patch deployment, ensuring critical updates are applied promptly to protect against potential exploits. This tool provides real-time monitoring and reporting, helping you maintain a secure environment by reducing the risk of cyber attacks targeting unpatched vulnerabilities.

Expert assistance for MDR alerts

Our security experts provide ongoing guidance and support for managing MDR alerts, offering in-depth context and assistance.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Key functions of MDR

Daisy Protect MDR offers significant advantages for organisations looking to reduce cyber risk but which lack the internal resources to effectively address skill gaps, cut costs, and improve detection and response. A top-tier solution should empower organisations to:

Monitor - Experienced threat hunters continuously monitor your IT environment, actively tracking malware and APT groups to ensure the highest level of situational awareness.

Detect - Threat actors have numerous methods to bypass perimeter defences, but by utilising behavioural analytics, they can be identified quickly for swift remediation.

Triage - An initial assessment and alert categorisation help filter out false positives while gathering the essential information.

Prioritise - Intelligent analytics prioritise these alerts based on severity, ensuring that the most critical threats are addressed first. This phase is crucial in the MDR workflow, especially considering how many IT teams struggle with alert overload.

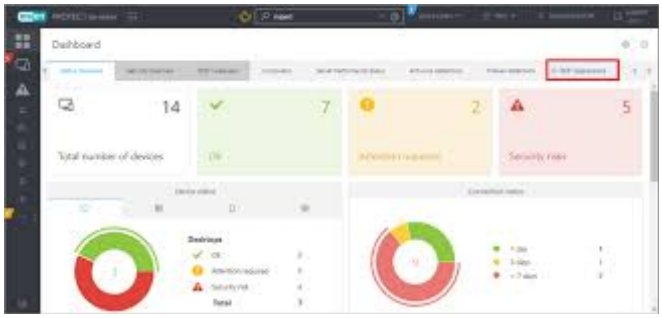
Investigate - Automated tools, combined with human expertise, dive deeper into alerts by analysing data and logs to determine their nature and scope. They assess whether an alert is a true positive and identify the necessary steps to resolve it.

Respond - An effective MDR service will either deliver basic response actions to block and contain the threat or provide full containment and remediation of compromised systems. The latter may include actions such as password resets, patching specific endpoints, or even reimaging affected computers.

Deployment of Daisy Protect MDR

Daisy Protect MDR is deployed on endpoints through several methods, depending on the organisation's infrastructure, size, and preferences. The preferred method of installation is as follows:

Deployment of Remote Management Console: For centralised management of security products across your network.



Configuration of deployment policies: We will create deployment policies based on your requirements (e.g., security settings, update schedules). We will liaise with you to identify permitted access for threat, triage and remediation work.

Installation on devices: We will remotely push out the installation package to all endpoints, such as computers, servers, and other devices, without the need for physical intervention on each individual endpoint. This process is fully automated, ensuring a seamless deployment across the network. It's important to note that the licences used on mobile devices are included in the total number of licences. For instance, a 100-seat licence can cover 100 computers and up to 100 Mobile Device Management (MDM) instances, providing comprehensive coverage for both desktop and mobile devices within the same licence allocation.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Network optimisation: Involves fine-tuning the network security configuration to ensure maximum efficiency and performance post-deployment. This process includes:

- **Performance tuning** - Customising settings to optimise system and network performance, ensuring that the solution doesn't negatively impact the speed and responsiveness of devices or applications.
- **Traffic analysis** - Monitoring network traffic to ensure that the security features, such as firewall and intrusion prevention, are working effectively without creating unnecessary bottlenecks.
- **Policy adjustment** - Fine-tuning security policies, such as web and application control, to align with needs while maintaining robust protection against cyber threats.
- **Regular updates and patching** - Ensuring that the latest security patches and updates are applied to both our product and the underlying network infrastructure.
- **Automated updates:** Once deployed, the management console will perform auto updates without the need of user interaction. An active internet connection is required.

System requirements

Your system should meet the following hardware and software requirements for Daisy Protect MDR to perform optimally:

Processors supported:

Windows:

- Intel or AMD processors (32-bit or 64-bit) are typically supported
- x86 architecture (32-bit)
- x64 architecture (64-bit)

MacOS:

- Intel processors (32-bit or 64-bit) for older macOS versions
- Apple Silicon (M1, M2) processors are supported, offering compatibility for both Intel-based Macs and newer Apple M-series Macs

Linux:

- Intel and AMD processors are supported, typically those with a 64-bit architecture.

Operating systems supported:

The following operating systems are supported by Daisy Protect MDR:

MacOS operating systems supported:

- MacOS Sierra (10.12)
- MacOS High Sierra (10.13)
- MacOS Mojave (10.14)
- MacOS Catalina (10.15)
- MacOS Big Sur (11.0)
- MacOS Monterey (12.0)
- MacOS Ventura (13.0)

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Service description

Windows operating systems supported:

- Microsoft SBS 2011 Standard x64
- Microsoft SBS 2011 Essentials x64
- Windows Server 2012 x64
- Windows Server 2012 CORE x64
- Windows Server 2012 R2 x64
- Windows Server 2012 R2 CORE x64
- Windows Storage Server 2012 R2 x64
- Windows Server 2016 x64
- Windows Storage Server 2016 x64
- Windows Server 2019 x64
- Windows Server 2022 x64
- Windows 10 x86
- Windows 10 x64 (all official releases)
- Windows 10 on ARM
- Windows 11 x64 (21H2 and 22H2)

Linux operating systems supported:

- Ubuntu 16.04.1 LTS x64 Desktop
- Ubuntu 16.04.1 LTS x64 Server
- Ubuntu 18.x4.1 LTS x64 Desktop
- Ubuntu 18.x4.1 LTS x64 Server
- Ubuntu 20.04 LTS x64
- Ubuntu 22.04 LTS x64
- Linux Mint 20
- RHEL Server 7 x64
- RHEL Server 8 x64
- RHEL Server 9 x64
- CentOS 7 x64
- SLED 15 x64
- SLES 12 x64
- SLES 15 x64
- Debian 9 x64
- Debian 10 x64
- Debian 11 x64
- Oracle Linux 8
- Amazon Linux 2

Smartphones and tablets supported:

- Android 5 (Lollipop) and later
- iOS 9 and later

Remote deployment via Microsoft Intune and VMware One

To use the Daisy Protect MDR, you must:

A) Obtain a list of the number of endpoints in its IT environment and must be compatible with the installation of the management console.

B) Compatible endpoint products (endpoint/server security/mail security products and Management Agent and connectors) for its endpoint devices.

C) Have those endpoint devices managed by the management console product.

When using this MDR service, you shall not change any rules, exclusions, or settings without prior approval or knowledge. The breach of this obligation may negatively impact the functioning of the Service and/or the console, and Daisy shall not be liable for any damages incurred thereof.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Service description

Remediation on Daisy Protect MDR

Remediation work focuses on identifying, mitigating, and recovering from security incidents such as malware infections, network breaches, or other forms of cyber attack. It involves a series of steps that help restore the security of your environment while reducing the risk of future attacks. Here's an overview of what remediation typically involves:

- **IT Support –** Prevent issues before they arise. Our cutting-edge monitoring solution keeps a watchful eye on the clients' devices, allowing for early detection and prevention of potential problems before they escalate into major problems.

  As a centralised help desk, we act as the single point of contact for all IT issues, including those involving third-party vendors. We manage communications and ensure seamless resolutions.
- **Network Equipment** - Remote monitoring of equipment such as routers, switches, firewalls, and Access Points (AP) for health management, to allow the IT Support to troubleshoot software issues, configure settings, download applications, and perform maintenance updates including software upgrades.
- **Cybersecurity** - Implementing security measures to protect your data, systems, and networks from cyber threats, breaches, and vulnerabilities.
- **Continuous Improvement** - Reviewing and assisting on best practice, but also helping clients to change their businesses ready for the future and to make them more efficient.
- **Device Coverage** - We'll offer assistance for devices allocated to your employees, encompassing desktop computers, laptops, tablets, and mobile devices.
- **Remote Management** - Remote access to endpoints and servers to allow IT Support to troubleshoot issues, configure settings, perform maintenance updates, and install security patches on software.
- **Reporting and Documentation** – We will use advanced reporting capabilities to monitor and analyse cyber attacks, providing detailed insights into the nature and impact of each incident. We will offer actionable recommendations to strengthen security measures and prevent future attacks.

Daisy backup

Award-winning cloud backup: Experience military-grade encryption and seamless granular recovery for effortless data restoration.

Key features for backup

Backup frequency: Backups are set to run once a day at a random time by default. For more flexibility the optional Advanced pack allows you to schedule multiple backups per day at specific times. (Available upon request through your Account Manager, additional charges apply.)

Granular recovery: Individual items or entire mailboxes can be restored, making it convenient to recover specific files or folders without restoring the entire backup.

Data retention policies: Cloud backup allows you to define data retention policies, enabling you to comply with regulatory requirements and manage storage space effectively.

Military-grade encryption: M365 data is secured with robust AES-256-bit protection.

Data retention policies: Cloud backup allows you to define data retention policies, enabling you to comply with regulatory requirements and manage storage space effectively.

Backup method: Starts with an initial full backup followed by incremental backups for all subsequent backups.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Service description

Daisy's backup provides complete backup solutions and restoration for your M365 estate, ensuring that any necessary recovery can be performed quickly and efficiently, reducing the impact on your business operations. If you require backups of files, applications, or systems, these are available upon request through your Account Manager and additional charges apply.

Protected areas:

- **Exchange Online:** Mailboxes, archives folders, calendar events, tasks, contacts, journal entries, and notes.
- **SharePoint**: Secure site collections, group sites, team and communication sites, attachments, documents, libraries, Google Titles pages, and Wiki pages.
- **OneDrive**: Entire storage area.
- **Teams**: Chats, files, and channel conversations.

Review process for key areas

Reporting review

Every six months we will review security event and activity reports that are generated on Daisy Protect MDR to identify any anomalies, trends, or recurring threats. We will evaluate the effectiveness of incident response actions taken based on the previous month's findings and analyse key areas such as malware detection and system alerts.

Patch management review

Every six months we will assess and ensure critical security patches are applied across all systems, including operating systems, applications, and third-party software.

Threat hunting review

Every six months we will perform a proactive threat-hunting review, scanning logs, network traffic, and endpoint activities for signs of undetected threats. We will focus on identifying unusual patterns that may indicate a breach or emerging threats.

Device count review

Every six months we will review the total number of licences purchased against the total number of endpoints and 0365 mailboxes devices currently in use, identifying any discrepancies.

Daisy backup review

Every six months we will review the amount of user's backups and ensure that all critical data is being backed up when scheduled.

Limitations and assumptions of the service

The following limitations are not unique to Daisy Protect MDR but are common in many security solutions. However, understanding these constraints can help organisations make informed decisions when selecting the right MDR solution.

Operating systems – Daisy Protect performs optimally with Windows 10 and Windows 11. Outdated Windows operating systems will display an error upon installation and will require an older version of software to be installed. Support for the older operating system isn't guaranteed due to fixes and module updates not being supported by Microsoft.

0365 - 0365 mailbox licenses are limited to the number of licenses purchased. To accommodate any unforeseen needs, we will offer a 20% concession on the total purchased license amount. This ensures flexibility and supports your organisation in managing license requirements efficiently while staying within budget. For instance, if you purchase 100 licenses but have a total of 115 mailboxes, we will allow you to continue using the additional 15 mailboxes at no extra charge. This arrangement will be reviewed every six months.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Service description

Cloud application protection – Whilst cloud application protection focuses on securing Microsoft 365 and Google Workspace, it does not directly protect cloud applications outside of these ecosystems, such as Salesforce, Dropbox, Zoom, and Amazon Web Services.

IT Support - The IT Support element in remediation is exclusively available to customers who have included IT Support services as part of their agreement with us. These services are provided as a value-added component for those who have paid for and opted to integrate IT Support within their service package. This ensures that our customers receive comprehensive assistance and resolution for any technical issues encountered during the remediation process, streamlining their experience and maintaining the highest standards of service.

Customisation limitations - Customisation for detection rules and exclusions is available but may not meet the needs of highly complex environments. However, ongoing optimisation will effectively align rules with the customer's needs.

Third-party integration – Integrates with SIEM and other tools, but some integrations may require additional setup or are not fully automated.

Response times - 24/7 monitoring is provided, but response times may vary based on incident severity and resource availability.

False positives or negatives - False positives or negatives can occur, requiring a balance between detection accuracy and minimising disruption.

Limited coverage for certain devices - Daisy Protect MDR supports many endpoints, but may have limitations for certain devices or older platforms.

Here are some examples of devices and platforms that may not be supported or have limited functionality:

Older Windows versions:

- Windows XP (especially versions older than Service Pack 3)
- Windows Vista (especially pre-Service Pack 2 versions)
- Windows 7 (though it may still be supported, it may not be compatible with updates)

Mac OS versions:

- Older versions of macOS, such as macOS 10.9 (Mavericks) or earlier, may not be supported by the latest products.

Older Android devices:

- Older Android versions (such as Android 4.x and below) may not be supported, or if they are, they may have limited protection features.

Older devices with limited resources:

- Some older hardware, especially devices with low RAM or CPU power, might not meet the requirements for the latest version of Daisy Protect MDR.

Other

- An internet connection is required for activation and updates to function properly.
- Two antivirus programs running simultaneously on a single device causes inevitable system resource conflicts, including slowing down the system to make it inoperable.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk

Company Reg. No: 04145329 | VAT Reg. No: 422 5118 33 | Registered in England and Wales

Service Level Agreement

Priority levels 1, 2, and 3

INCIDENTS / SERVICE REQUESTS				
PRIORITY LEVEL	INITIAL RESPONSE	UPDATE (INTERNAL)	MAXIMUM TARGET TIME TO RESOLUTION	TARGET RESOLUTION TIME
1	1 hour	1 hour	4 hours	2 hours
2	4 hours	4 hours	2 business days	1 business day
3	4 hours	8 hours	5 business days	2 business days

P1

- Incidents where a total site outage affects all users, or the primary line of business, or where the productivity suite (e.g., Microsoft 365) is unavailable to all staff.

P2

- Incidents that reduce the level of functionality or performance of the services across one or more sites or teams.

P3

- Incidents that affect a single user or component that has limited impact on the rest of the system (low disruption to service).

Raising a request or issue

If you need to raise a request or escalate an issue, please contact our service team using the methods below. For more information, please contact your Account Manager.

General Support

- Email: **mspsupport@daisycomms.co.uk**
- Telephone: **03330 434 000**

Escalation Contact

- Email: **itserviceescalations@daisycomms.co.uk**

When raising **P1** requests we encourage you to call our help desk to ensure immediate escalation.

P3 incidents can be reported via email. You'll promptly receive a response confirming the incident has been logged, along with an incident reference.

Daisy Communications Ltd.
Lindred House
20 Lindred Road
Brierfield, Nelson
Lancashire, BB9 5SR

Contact us:
T: 0800 040 8888
E: info@daisycomms.co.uk