Brochure

Cyber Security

mother
technologies

About Mother

Established in 2002, Mother Technologies is a Scotland-based MSP (Managed Service Provider) with offices located in Aberdeen, Edinburgh, and Glasgow. The company has three distinct Service lines: IT, Telecom and Connectivity, providing customers with extensive experience and unified support across all three areas.

At Mother, we recognise the critical role that cybersecurity plays in modern business operations, and we are committed to delivering top-notch services to keep your organisation secure. Our team of experts takes the time to understand your requirements and develop tailored solutions that help you keep your business safe. Our objective is to eliminate the stress associated with the ever-evolving threat of cyber security. We have the expertise and resources to provide you with reliable solutions that meet your needs.

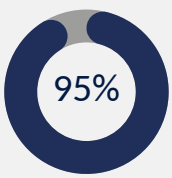
Contents

Why Mother?

Our engineers have a vast amount of combined experience across all our service lines. Their skill set is continuously growing through ongoing training, enabling us to deliver high-quality service.

Selecting the appropriate IT service provider can be a challenging endeavour. At Mother, we hold multiple industry certifications that you can rely on to guarantee that your IT support is in capable hands.

We know that every company operates differently. That's why we provide flexible solutions that can be made to fit your needs.



With a 95% customer retention rate, we consistently deliver excellent IT services to all our customers.

In 2023, Mother was Highly Commended as MSP of the Year at the Comms Business Awards. This award recognises outstanding Managed Service Providers in the UK for delivering exceptional customer service, innovative solutions, and measurable business benefits.

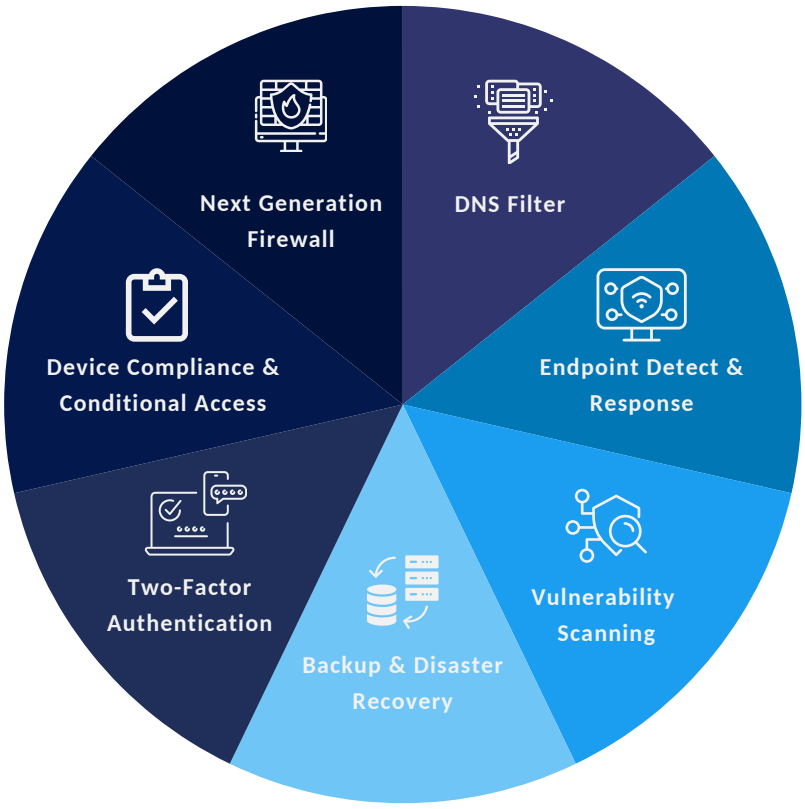
Introducing RoundClock Security Suite

7 Fundamental Components of Cybersecurity

Protect your business from evolving cyber threats with Roundclock, a collection of cyber security services designed to safeguard your systems and prevent disruption.

There is no silver bullet that will protect your organisation from today's cyber threats. Organisations must consider all areas of vulnerability and take action to mitigate against current and emerging threats.

To provide a concentrated security focus, Mother incorporates 7 security fundamentals in its RoundClock Security Suite that will fortify your defences, mitigate risk, protect your business from cyber threats and satisfy your security compliance requirements.



Next Generation Firewall

Powered by Cisco Meraki

A Next Generation Firewall (NGFW) goes beyond the legacy protection capabilities of traditional firewalls. Traditional firewalls allow or block traffic based on state, port, protocol or other rules defined by your network administrator. Today, your firewall needs to perform far greater in-depth traffic analysis to protect your organisation from the advanced cyber-attacks prevalent in modern day society.

Gartner stipulates that Next Generation Firewalls must include:

Stateful Inspection

Also known as Dynamic Packet Filtering, NGFWs must provide Stateful Inspection which is technology common to all traditional firewalls.

Deep Packet Inspection

Deep Packet Inspection provides firewalls with application and user-awareness allowing granular control of traffic from unauthorised or high-risk applications.

Cloud Implementation

In addition to ensuring NGFW prerequisites, Mother recommends that organisations keep NGFW functionality off-box. Simply put, this involves pushing your front-line defences into the cloud as far away from your front door as possible. It destresses your firewall and ensures internet traffic is being screened long before it reaches you.

Threat Intelligence

Threat Intelligence arms firewalls with the ability to act on threat intelligence feeds from external sources. NGFWs must include upgrade paths to cater for future as well as current information feeds.

Integrated Intrusion Prevention

Integrated Intrusion Prevention continuously monitors your network to provide security against unauthorised access and malicious activities.

Evolving Threat Defence

NGFWs must employ techniques to address evolving security threats in addition to those that are recognised and understood.

Why do you need a Next Generation Firewall?

Mother promotes Cisco Meraki MX Next Generation Firewalls for Ironclad security.

The Cisco Meraki MX series are advanced security appliances that go well beyond NGFW prerequisites. They possess a comprehensive suite of secure network and assurance capabilities and are 100% cloud-managed which simplifies their installation and remote management.

- Cisco Talos Threat Intelligence – one of the largest commercial threat intelligence teams in the world.
- World #1 SNORT-based Intrusion Detection & Prevention (IDS & IPS) – a fundamental requirement for PCI compliance.
- Cisco Advanced Malware Protection (AMP) – comprehensive security before, during and after a malware attack.
- High Performance for modern, bandwidth-intensive networks.
- WAN & Cellular Failover to protect against ISP connection outages.
- Site-To-Site AutoVPN.
- Application-Based Firewalling.
- Content Filtering.
- Web Search Filtering.
- Client VPN.

DNS Filter

Powered by Cisco Umbrella

In today's evolving IT landscape where the cloud has enabled an online, work-anywhere culture, organisations are finding it much harder to secure their networks.

Loading your organisation's firewall with every defence feature available has been the traditional method of protecting your on-site assets from malicious internet content. But if half of the assets (e.g. your laptops) are off-site in a satellite office or user's home, then they're not protected by your organisation's firewall. These endpoints are at high risk of malicious infection and are a major threat to your organisation when they return or remotely connect to your network. Your organisation requires On-Net Internet security for your main office devices and Off-Net Internet Security for your roaming devices.

What is it?

DNS Filtering is the process of using the 'Domain Name System' to block malicious websites and filter out harmful or inappropriate content.

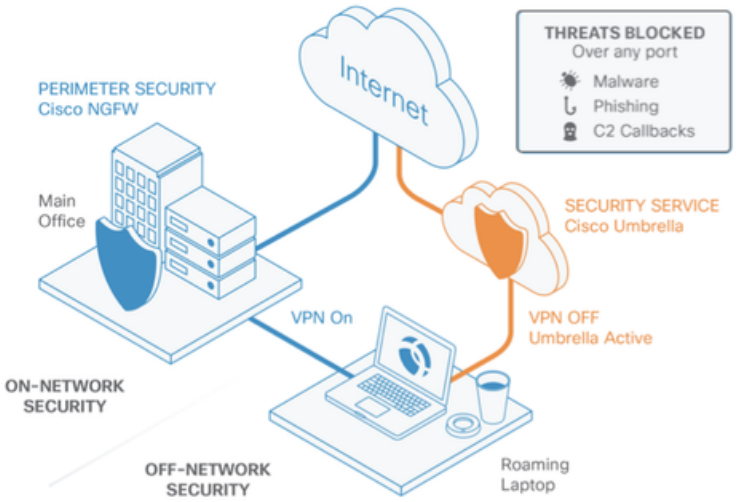
How does it work?

When a user requests a website, say mothertech.co.uk, the request is sent to a web service known as a DNS resolver. A DNS resolver determines the actual IP address of mothertech.co.uk. It then returns the IP address to the user's machine which in turn opens a connection to the given IP address and the content is loaded.

With a DNS Filter, when a user requests a website, a specially configured DNS Resolver performs a security check against the website. If the website is a safe site, then the IP address will return to the user's machine and the website will be presented to the user. If, on the other hand, the website is not safe, the DNS Resolver will not return the IP address of the website but will instead return an alternative address which displays a denial message.

Why RoundClock DNS Filter?

RoundClock DNS Filter is powered by Cisco Umbrella, **the world's #1 DNS Filtering Engine.** It is an off-box cloud service that filters all Internet traffic for your main office as well as your roaming users. It is a fundamental security requirement for your network today.



Key Features

Endpoint Coverage
Protects Windows, Macs, Chromebooks, and Apple smart devices.

On-Net and Off-Net Protection
Safeguards endpoints irrespective of location (Directly connected or roaming outside of the corporate network).

Shadow IT Detection
Identifies and blocks unauthorised cloud applications.

Granular Policy Control
Allows tailored protection with granular policies for individuals or groups.

Proxy and Deep Inspection
Enables deep inspection of risky domains, providing comprehensive protection against emerging threats.

Advanced Threat Intelligence
Leverages a global network of sensors and security intelligence for accurate prediction and proactive protection against cyber threats.

Comprehensive Web Security
Ensures safe and secure internet access by blocking domains associated with phishing attacks, malware, ransomware, botnets, and other high-risk or inappropriate categories before they reach the network.

Endpoint Detect & Response

Powered by Sentinel One

Standard Anti-virus software is no longer a satisfactory defence mechanism for combatting today's advanced security threats. To provide the high level of endpoint security required to protect your devices and to satisfy the prerequisites of Cyber Essentials, organisations need to upgrade their endpoint protection to Endpoint Detect & Response, commonly referred to as EDR.

We used to identify viruses from signatures (digital fingerprints) that identified a malicious object. Most of the latest and evolving threats today can't be caught by signature-based protection making it easy for them to sneak past your company's defences undetected.

Zero Day Attacks

Network vulnerabilities that attackers exploit before vendors or developers have even learned of the hole in their product.

Weaponised Documents

Seemingly harmless PDF email attachments that execute attacks once they have entered your network.

Fileless Threats

Many malware threats are difficult to detect because they live only in the memory of an infected machine.

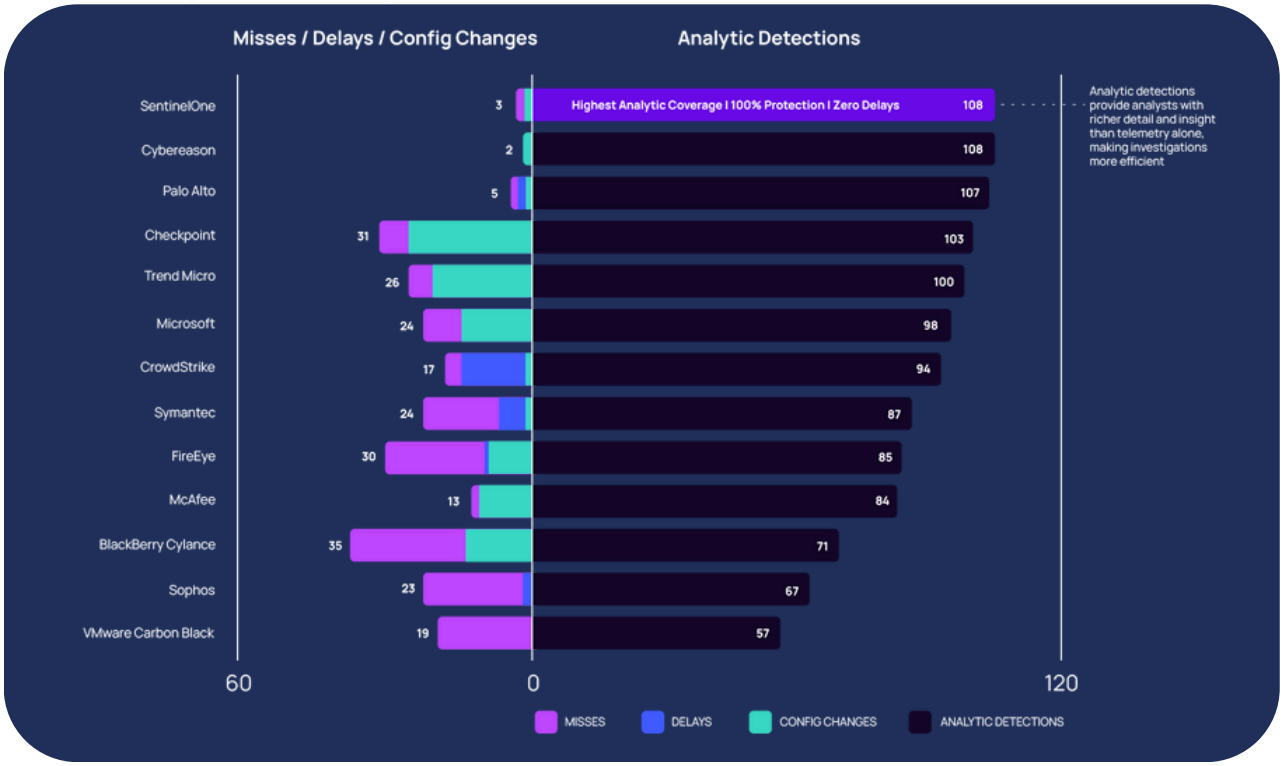
Ransomeware Attacks

Cyber-attackers disable your network and demand huge ransoms in order for services and data to be restored.

Why RoundClock EDR?

RoundClock EDR doesn't rely on legacy malware signatures. It uses artificial intelligence (AI) techniques to detect and prevent both current and emerging threats in real-time.

RoundClock EDR is powered by **SentinelOne**, recognised by Gartner, MITRE Engenuity and SE Labs as the a leader in the enterprise security market.



Traditional Antivirus ✗	RoundClock EDR ✓
Can't roll back to a pre-infection state, increasing your ransomware risks.	Help prevent ransomware by rolling back devices to their pre-infection state.
Use signatures to identify threats, meaning capabilities lag behind cyberattackers' latest strategies.	Use artificial intelligence (AI) to detect and prevent both current and emerging threats.
Fly blind during execution, creating an entry point for new threats from savvy attackers.	Monitor processes before, during, and after execution, to prevent new threats from executing.
Rely on daily or weekly scans, increasing your risks due to a time lag.	Monitor your systems in real-time.
Can slow down your device performance with long scans.	Keep device performance fast with continual monitoring.

Vulnerability Scanning

Dynamic threats call for a Dynamic approach. Mother has incorporated Network Vulnerability Scanning into its RoundClock Security Suite to report on network security vulnerabilities so action can be taken to mitigate against cyber attacks and fill compliance gaps.

Asset Discovery

RCVS uses multiple protocols to discover and probe your network for a complete and comprehensive inventory of your network assets. This includes your network endpoints (e.g. desktop and laptop devices), servers, virtual machines, routers, switches, access points, firewalls, printers and more.

Asset Vulnerability Detection

RCVS probes all your assets for vulnerabilities on a continual or snapshot basis. RCVS leverages multiple vulnerability sources including the NIST's National Vulnerability Database (NVD) and OEM sources in its detection phase.

Domain Vulnerability Detection

Active Directory is the cornerstone of almost every network and, whether local or cloud based, RCVS will perform an Active Directory Assessment to identify misconfigurations, weak policies, and privileged user-access.

External IP Scans

RCVS provides external scans to highlight weaknesses that could be exploited. External scans detect open ports, protocols, and named vulnerabilities in public-facing network equipment such as web servers and firewalls.

Compliance Scans

RCVS supports scanning of your network for common cybersecurity compliance standards that make up the foundation of a strong cybersecurity strategy. RCVS currently supports compliance standards for PCI DSS, HIPAA, GDPR IV, NIST 800-53, NIST 800-171, CIS, CIS 8.0, ISO 27002, Cyber Essentials, and Essential Eight.

Application Anomalies

Network vulnerabilities are often exploited by cyber criminals through weak network control and the presence of unauthorised applications installed by its users. RCVS will detect anomalies from a given application baseline enabling focused remedial action to be taken.

Reporting

Effective vulnerability scanning goes beyond detection; it provides actionable insights through comprehensive reporting. Our reporting process at Mother ensures that you receive clear and detailed information about the security posture of your systems.

Managed Service

In 2023 Mother Technologies was a finalist in the MSP of the Year Comms Business Awards so it'll come as no surprise that Mother can perform the remedial action necessary to secure your network and provide RCVS on a Managed Service basis to ensure network security isn't a one-off process but a continual assessment to ensure your security standards do not derail.

Backup & Disaster Recovery

Powered by Acronis

Maintaining reliable backups is critical. The shape of disasters goes well beyond hardware failure. Malware attacks are a far greater threat and moving your data to the cloud does not protect it.

Why RoundClock BDR?

Mother's RoundClock BDR utilises Acronis Cyber Protect to centrally manage the secure backup of corporate data and critical systems.

Microsoft 365
Microsoft doesn't backup your data. Cloud-to-cloud backup protects your data by securely transferring Exchange, OneDrive and Sharepoint data from 365 to a private cloud.

Google Workspace
Cloud-to-Cloud backup protects your data by securely transferring your Gmail, Drive, Contacts and Calendar from Workspace to a private cloud.

Spin up DR
For critical assets that require an instant-on in the event of a disaster, RoundClock's Spin-Up DR will launch a live hosted-replica whilst you're waiting for the restoration of the failed asset to be completed.

Endpoints
Centrally managed backup agents are installed on all your Endpoints to ensure critical data is backed up to the cloud and available for instant recovery.

Virtual Machines
RoundClock BDR will protect your Azure VMs or Amazon instances with the option to utilise Azure, local or private cloud storage for your backups.

Local Servers & Critical Assets
Local Servers and other critical assets incorporate a staged backup process where primary backups are sent to a local Network Attached Storage (NAS) and secondary backups are sent to the cloud. The local storage entertains fast recovery in the event of a system failure and the secondary cloud copies are reserved for catastrophic disaster recovery purposes.

Two-Factor Authentication

Ensuring comprehensive protection for your business against cyber threats is critical. Two-factor authentication (2FA) offers an additional layer of security that significantly heightens your defences, making it more challenging for cyber criminals to gain access to your sensitive data and systems. Despite initial reluctance by many due to perceived hassle, implementing 2FA is not just an option, it is an essential in today's digital environment.

Why do you need 2FA?

Consider the severe effects of a ransomware attack or the compromise of your passwords. Ransomware can have devasting effects including financial losses, operational disruptions, reputational damage, legal consequences and more. 2FA mitigates these risks by requiring users to provide two forms of authentication before accessing accounts or systems. Therefore, even if passwords are compromised or devices are stolen, hackers still face a barrier to entry.

Two-factor authentication sends a code to a device or portal that the user exclusively owns, adding an additional layer of security beyond passwords alone. Without access to the user's personal device, cyber attackers are unable to breach accounts.

Heightened Security
Improves defences against unauthorised access and data breaches.

Risk Reduction
Mitigates risks associated with password attacks and stolen credentials.

Enhanced Protection
Ensures account and data security across devices, mitigating the risk of compromise on one device and bolstering overall security.

Peace of Mind
The added security layer of 2FA offers peace of mind to businesses and users, protecting accounts and sensitive information.

Types of 2FA

There are various methods of 2FA, including:

Authenticator App

Code sent to mobile via SMS

Code sent to email

We recommend using either the authenticator app or SMS for 2FA authentication. Email platforms are high-risk due to their vulnerabilities and, moreover, you don't want to send security codes the very system that's potentially being breached. Authenticating via external off-net devices (i.e. a mobile phone) is safer.

Implementing 2FA

You may already have eligibility for 2FA within your existing 365 license subscription. If not, you can upgrade your subscription or reach for a 3rd party solution such as Cisco's 2FA solution, Duo. Duo has extensive customisable security features and is very easy to use.

Many businesses don't want to enable 2FA because it complicates their logins. Unfortunately, today's landscape is so cyber-crime abound that you must. Think of it this way, "If it's easy for you, it's easy for them." Whatever your preferred product, switch it on!

Device Compliance & Conditional Access

Your organisation is not safe if unrecognised endpoint devices can access your network. You have taken all the necessary steps to ensure your endpoints are secured with EDR and DNS filtering but that's of little comfort if somebody takes an old laptop out of a drawer and uses it to log-on to your network. The laptop is unlikely to comply with your security policies and consequently presents a significant threat. The same threat is prevalent from a user's personal home-computer.

The Risk of Unsecured Devices

When a device connects to your network, it effectively becomes a gateway to your entire system. If not responsibly managed, these devices introduce significant network vulnerabilities. Cyber criminals exploit these vulnerabilities to gain unauthorised access to your network.

The Solution: Enforcing Device Compliance and Conditional Access Policies

To mitigate the risk of unmanaged devices accessing your network, it is essential to enforce strict device compliance and conditional access policies. Conditional Access uses a compliance status to determine whether to grant or block access to a device.

By ensuring devices comply with the criteria set within your security policies, you safeguard your network by preventing unmanaged and non-compliant devices from connecting.

Your Conditional Access Policy might include up-to-date Operating System compliance, and confirmation that EDR and the DNS Filter is present and running. Upon satisfying the compliance criteria, device access is granted following successful user authentication.

Key Considerations

Here are the key considerations to take into account when implementing conditional access and device compliance:

Device Authentication
Verify the identity and compliance status of every device attempting to connect to your network.

Security Configuration
Ensure that devices adhere to your security standards.

Continuous Monitoring
Regularly monitor devices for compliance and take immediate action if a device falls out of compliance.

By focusing on these key areas, you create a safer network environment, ensuring only trusted devices are allowed in.

Service Portfolio

IT Support

At Mother, we understand the vital role IT plays in organisations. By comprehending your unique business requirements, our flexible support team delivers tailored managed services to ensure your IT remains aligned with your needs. With our Bronze, Silver, Gold, and Platinum packages, you can choose the level of support that suits you best. Our objective is to alleviate the stress of IT, allowing you to focus on your business goals.

Telecom

Mother's flagship cloud communications platform, Liberty, can be found in hundreds of businesses across Scotland and boasts extensive functionality to satisfy the most demanding client requirements.

Connectivity Solutions

Mother is an ISP and bona fide communications provider. We have wholesale agreements with all of the major carriers and can deliver anything and everything in the array of available broadband services right up to high-capacity, low-latency fibre circuits in a private or public arrangement.

Private Cloud

Mother has 4 datacentres across Scotland. We can provide private connections to the datacentres allowing you to secure your voice and data services with a level of resilience that is almost impossible to achieve with any on-premise arrangement.

Excellent Customer Service

Overall, from my experience with Mother Technologies, I would have no hesitation in recommending them to any educational institute or commercial organisation due to the exceptional work the team has carried out”

Mhairi Miller
Head of Operations
St Margaret's School for Girls

Contact Us

Aberdeen
Davidson House
Campus 1
Aberdeen Innovation Park
Balgownie Road
Aberdeen
AB22 8GT
+44 (0) 1224 350000

Edinburgh
Bonnington Bond
2 Anderson Place
Edinburgh
EH6 5NP
+44 (0) 131 603 4650

Glasgow
20-23 Woodside Place
Glasgow
G3 7QF
+44 (0) 141 212 6600