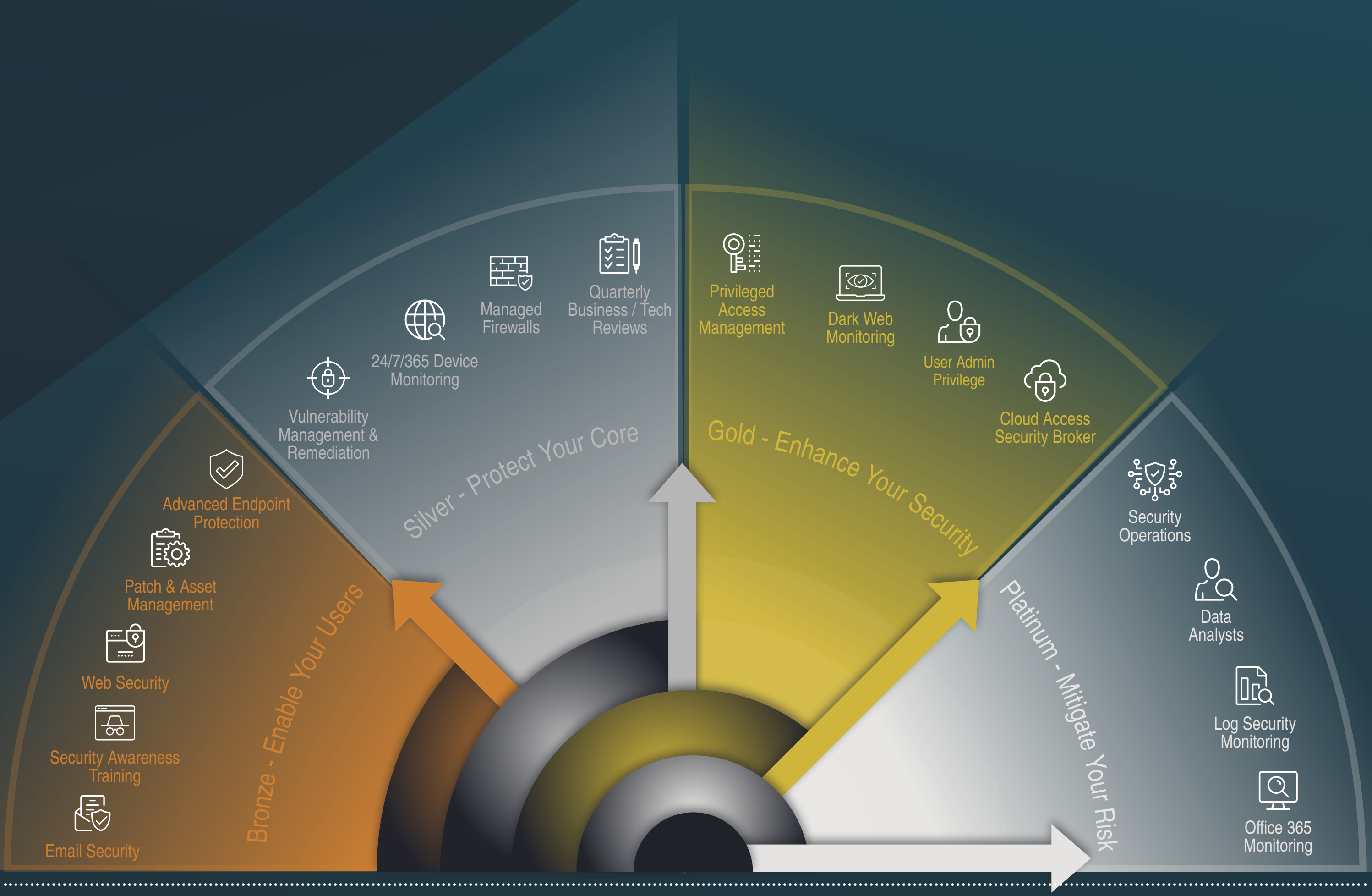
netutils

Managed Cyber Security Platform

Your Entire Security Posture-as-a-Service



Advanced Endpoint Protection
Patch & Asset Management
Web Security
Security Awareness Training
Email Security
Bronze - Enable Your Users
Vulnerability Management & Remediation
24/7/365 Device Monitoring
Managed Firewalls
Quarterly Business / Tech Reviews
Silver - Protect Your Core
Privileged Access Management
Dark Web Monitoring
User Admin Privilege
Cloud Access Security Broker
Gold - Enhance Your Security
Security Operations
Data Analysts
Log Security Monitoring
Office 365 Monitoring
Platinum - Mitigate Your Risk

Enable | Protect | Enhance | Mitigate

CYBER ESSENTIALS CERTIFIED PLUS

QMS ISO 9001 REGISTERED

QMS ISO 27001 REGISTERED

Crown Commercial Service *Supplier*

t: 020 8783 3800 | **e:** info@netutils.com | **w:** netutils.com | **b:** netutilsblog.com

Managed Services to Suit Your Business Needs

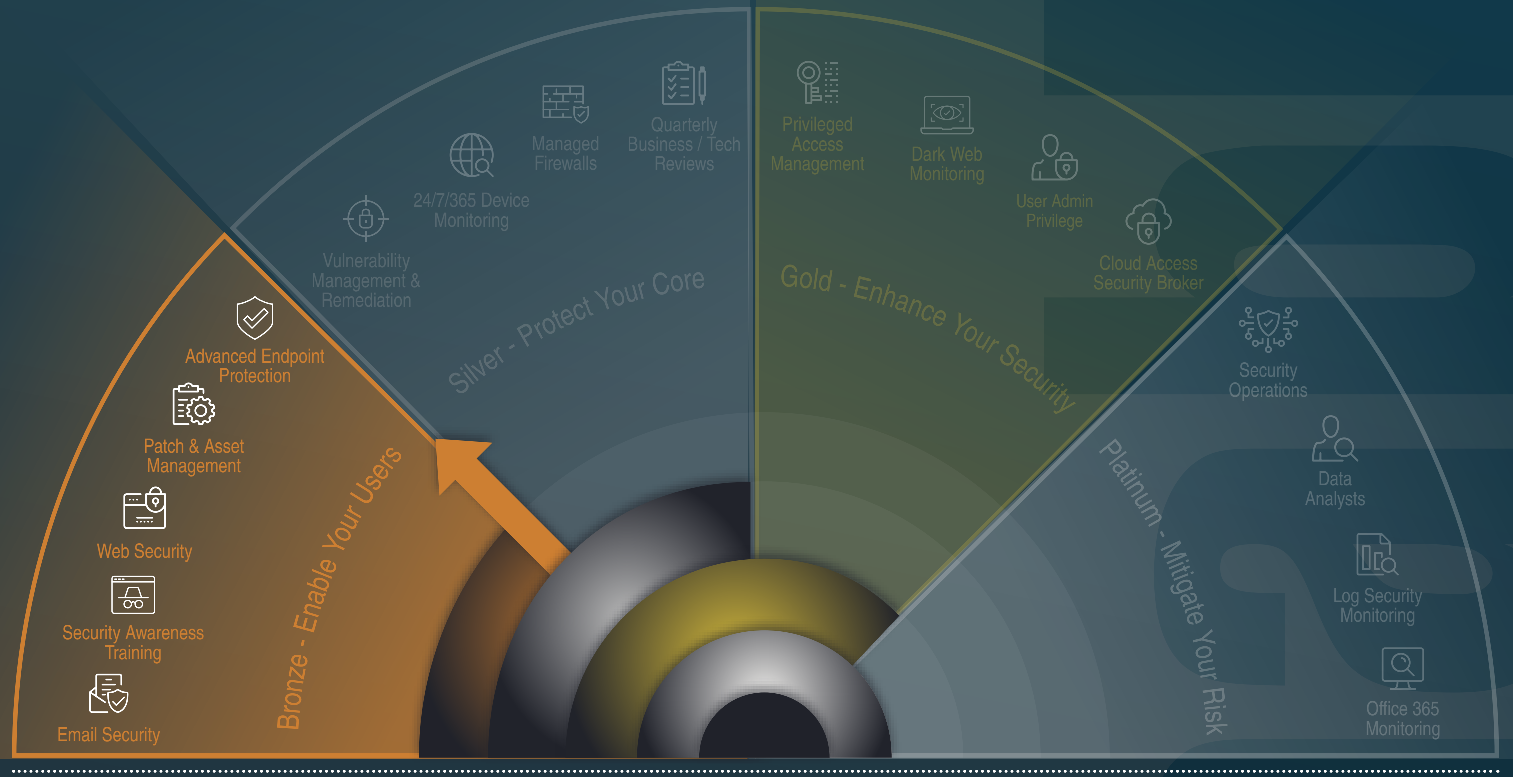
Save time, money and resource with our cost-effective managed cyber security platform; keep your users safe, protect your core infrastructure, enhance your security and mitigate risk against cyber crime.

By utilising our expertise and experience you're leveraging an enhanced team who are constantly trained and certified in all specialist areas.

We work alongside industry leading vendor partners and invest the time and resource, so you don't have to.

Services Matrix	Bronze	Silver	Gold	Platinum
Email Security	☑	☑	☑	☑
Security Awareness Training	☑	☑	☑	☑
Web Security	☑	☑	☑	☑
Patch & Asset Management	☑	☑	☑	☑
Advanced Endpoint Protection	☑	☑	☑	☑
Vulnerability Management & Remediation		☑	☑	☑
24/7/365 Device Monitoring		☑	☑	☑
Managed Firewalls		☑	☑	☑
Quarterly Business / Tech Reviews		☑	☑	☑
Privileged Access Management			☑	☑
Dark Web Monitoring			☑	☑
User Admin Privilege			☑	☑
Cloud Access Security Broker			☑	☑
Security Operations				☑
Data Analysts				☑
Log Security Monitoring				☑
Office 365 Monitoring				☑

Bronze


Advanced Endpoint Protection
Patch & Asset Management
Web Security
Security Awareness Training
Email Security
Bronze - Enable Your Users
Vulnerability Management & Remediation
24/7/365 Device Monitoring
Managed Firewalls
Quarterly Business / Tech Reviews
Silver - Protect Your Core
Privileged Access Management
Dark Web Monitoring
User Admin Privilege
Cloud Access Security Broker
Gold - Enhance Your Security
Security Operations
Data Analysts
Log Security Monitoring
Office 365 Monitoring
Platinum - Mitigate Your Risk

Enable Your Users

Bronze - Enable Your Users

Email Security | Security Awareness Training | Web Security | Patch & Asset Management | Advanced Endpoint Protection

Secure and empower your users with our comprehensive endpoint security services including email and web security, patch and asset management, advanced end-point protection and security awareness training. The NetUtils Bronze managed service represents all the fundamentals needed to establish a robust security posture and protect your business, delivering enterprise grade, class leading managed security services for smaller businesses budgets.

Email Security

Our solution provides a multi-layered email security solution for your entire organisation from known, unknown and emerging email security threats. Stop large-scale phishing, targeted attacks, CEO fraud and malware in their tracks with a comprehensive, cloud email security solution.

Protection from Traditional Threats
Including spam, viruses, large-scale phishing attacks and malicious URLs.

Prevent Impersonation Attacks
Modern, targeted and sophisticated email threats including Business Email Compromise (BEC) and CEO fraud.

Multi-Layered Threat Protection
A unique combination of technologies.

Unique Time-Of-Click Protection from Malicious URLS
Unique time-of-click protection from malicious URLs.

Security Awareness Training

Security awareness training is a form of education that seeks to equip members of your organisation with the information they need to protect themselves and their organisations' assets from loss or harm.

Our security awareness training platform helps employees confront the fact that bad guys are trying to trick them. Once they confront that, they become aware and able to detect these scam emails and can take appropriate action like reporting suspicious emails, deleting emails, or not clicking a link.

Our fully managed security awareness programme removes all the burden of delivery and maintenance and equips you with everything needed to cultivate a security aware culture within your organisation.

Prevent Data Breaches and Attacks
Equipping your users with the tools needed to help prevent attacks is the core reason for undertaking security awareness training.

Culture Of Security
Build security into the fabric of your business. Advanced training platforms help monitor and develop a culture of security, making people your first line of defence.

Reinforce Your Technological Defences
Attackers rarely attack businesses through technological means only. Instead typically targeting people, seen as an easy way into protected networks.

Gain Customer Confidence
A business that invests in measures (both technological and educational) to improve cyber security is better able to generate consumer trust.

Compliance
For many organisations compliance is the driving force behind a security awareness training initiative, often beginning as a box ticking exercise to becoming a core element of the organisation's security posture.

Social Responsibility
Attacks spread from business to business and across networks. It's all of our responsibilities to do everything we can to prevent this, with security awareness training being one tool available.

More than 90% of successful hacks and data breaches **start with phishing scams.**

Phishing is a threat to every organisation across the globe.

Patch and Asset Management

View and manage your software inventory and, at the same time, achieve pre-emptive vulnerability management. This scalable, flexible and intuitive solution can handle both Microsoft and 3rd party software.

Software Management
Manage software across your organisation from a unified, secure interface.

Rapid Deployment
Rapid deployment of security-critical patches and updates, for essential resilience against cyber threats.

Automated Processes
Allow granular control over your organisation's software environment.

End User Empowerment
Install and update automatically or grant privileges to users to manage their own software securely, according to custom-built policies.

Automating your patch management routine helps you **save valuable time and resources.**

Web Security

Protect your organisation from web-borne malware, offensive or inappropriate content and manage time spent on websites that impact productivity with our web security platform. Powered by a unique architecture that ensures lightning fast response times for all users no matter where they are in the world.

Threat Protection
Protection via a powerful combination of real-time traffic inspection, URL reputation, advanced anti-malware and threat intelligence.

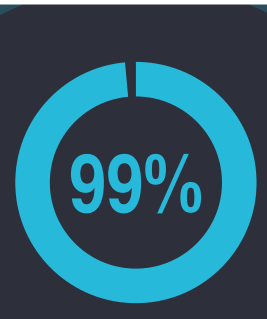
Encrypted Sites
With over 70% of the web encrypted deep inspection of SSL/TLS traffic is essential.

Automatic Unknown URL Classification
Automatic real-time analysis of previously unseen pages.

Guest And Captive Portals
Create and apply separate policies to personal and guest devices.

Powerful Policies
Block/allow or apply time quotas based on users, groups, devices by category or keyword lists.

Page Level Categorisation
Every page within a site is categorised – not just the domain or sub-domain.



"99% of the **vulnerabilities exploited will be the ones known to security and IT professionals** for at least a year."

Gartner

Bronze - Enable Your Users

The **WannaCry ransomware attack** was the worst cyber incident in history, with **over 200,000 endpoints encrypted, across 150 countries,** and damages of up to $5 billion.

Next-Gen Antivirus

Using real-time low-impact in-memory file and signature scanning, alongside active registry change scanning, our next-gen endpoint antivirus provides the leading edge, code-based detection and mitigation. The solution combines the techniques known by both traditional and next-gen antivirus to detect and remediate viruses, APTs, financial fraud, ransomware and data leaks.

Local File/Signature & Registry Scanning
Real-time low-impact in-memory file and signature scanning, alongside active registry change scanning.

Real-time Cloud Scanning
Unknown file and potential threat found will be sent to our cloud for extra scanning.

Sandbox and Backdoor Inspection
Malicious activity will be stopped at its roots to provide unparalleled endpoint threat remediation.

Process and Behaviour-Based Scanning
Monitor processes and process changes with Heuristic, behaviour-based engines.

Advanced Threat Prevention

Provides a unique 2-way traffic filtering engine that supports fully customisable white/black listing.

Track device-to-infrastructure communication, able to detect malware strains that other solutions struggle to see.

Malware is blocked at a traffic level, stopping its communications with criminal infrastructure.

By leveraging the unique intelligence gained through blocking threats at the DNS, HTTP and HTTPS level, the threat prevention system not only gives you the power to stop active attacks, but they also accelerate any investigation process. Vulnerable endpoints can be pinpointed and reinforced against future threats, ensuring a proactive approach to security.

Spot Hidden Threats Using Machine Learning
Neutralise threats that would otherwise bypass traditional firewall or antivirus solutions.

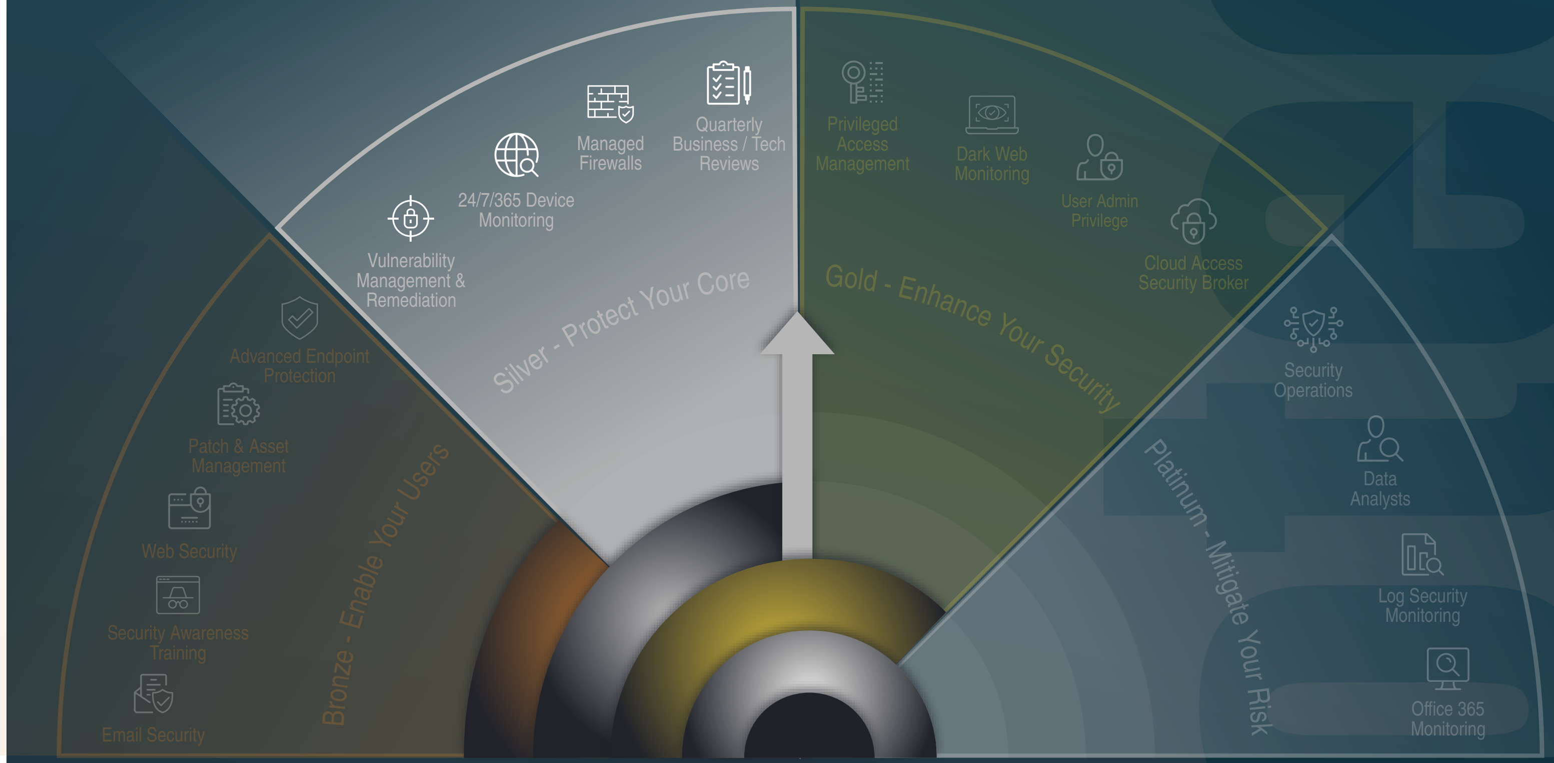
Detect DNS-Hijacking
Prevent, detect, and block threats and proactively hunt for DNS-based threats.

Prevent Exploits, Ransomware and Data Leakage at DNS Level
Move beyond signature-based detection and block attacks that antivirus will never recognise.

Hunt, Detect, And Respond to Threats Faster
Leverage a Host-Based Intrusion Prevention System (HIPS), augmented by our highly intelligent threat detection technology.

In an ever-changing threat landscape, **impeccable detection and powerful mitigation is the fundamental** security layer.

Silver


Bronze - Enable Your Users
Advanced Endpoint Protection
Patch & Asset Management
Web Security
Security Awareness Training
Email Security
Silver - Protect Your Core
Vulnerability Management & Remediation
24/7/365 Device Monitoring
Managed Firewalls
Quarterly Business / Tech Reviews
Gold - Enhance Your Security
Privileged Access Management
Dark Web Monitoring
User Admin Privilege
Cloud Access Security Broker
Platinum - Mitigate Your Risk
Security Operations
Data Analysts
Log Security Monitoring
Office 365 Monitoring

Protect Your Core

Silver – Protect Your Core

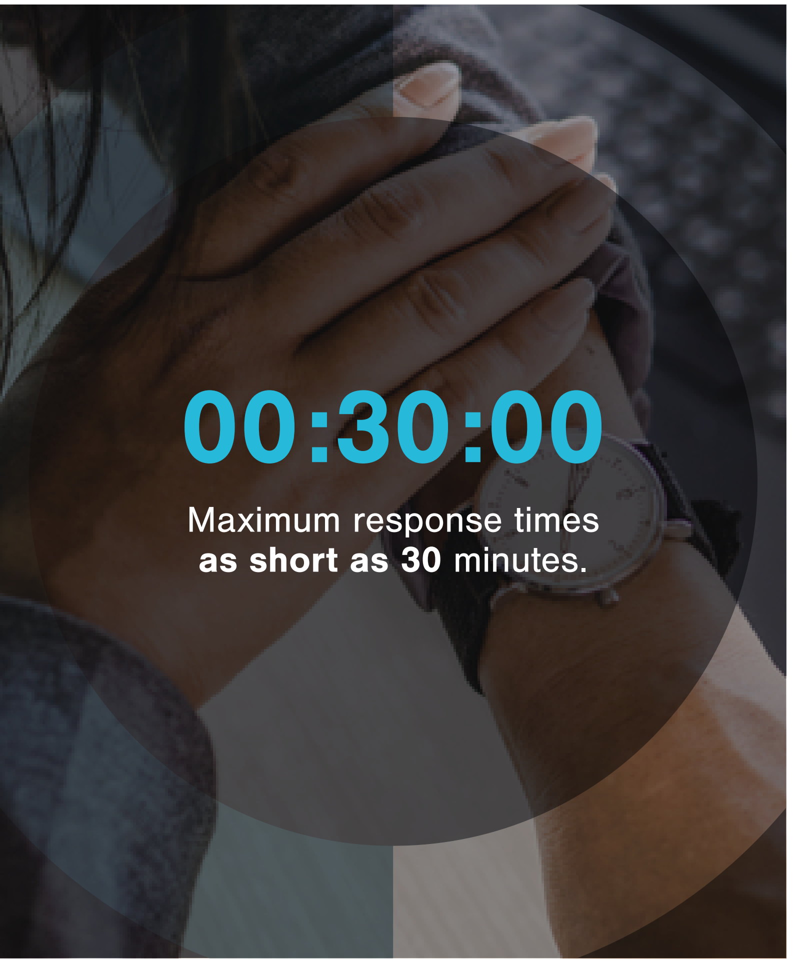
Vulnerability Management & Remediation

24/7/365 Device Monitoring

Managed Firewalls

Quarterly Business Tech Reviews

Focus on what matters to your business and let us manage the burden of your day-to-day IT infrastructure. With the NetUtils Silver managed service you gain access to our highly trained, certified and experienced technical team who will manage, review and maintain your critical infrastructure so you don't have to. We will become an extension to your existing team and work alongside you to ensure you extract the most from your security investments.



00:30:00

Maximum response times **as short as 30** minutes.

> **"Four in ten businesses report having cyber security breaches** or attacks in the last 12 months **with medium-sized businesses the most vulnerable."**
>
> UK Government Cyber Security Breaches Survey of 2021

Managed Infrastructure (Firewalls)

The NetUtils Managed Infrastructure and specifically Managed Firewall service enables you to extract the maximum value from your security purchases while ensuring that you protect your network from unauthorised access and malicious attacks. Firewalls are the critical gateway into a network, and those managed by NetUtils come with the highest degree of attention and expertise with the sole purpose of protecting your critical assets and securing your perimeter.

A fully managed contract gives you access to expert configuration, management, and monitoring with an efficient response to any identified issues, ultimately lowering the risk of disruption while allowing you to concentrate on your core business. The engineering team within NetUtils will work alongside your organisation providing a dedicated team of experts to manage some of your most critical infrastructure.

Day To Day Maintenance

Our experienced engineers will maintain your infrastructure on a day-to-day basis, applying rule and policy changes as needed, troubleshooting issues as they arise and generally managing your equipment to maintain the levels of service your business requires.

Continual Improvement Process

A set of realistic and meaningful targets against the continual improvement of your network's health and security posture will be agreed. By regularly reviewing the status of your equipment in line with best practice, we ensure that your security risk is mitigated as much as possible. Included in the continual improvement programme are reviews of rules, policy, configuration, known vulnerabilities and firmware updates. Our experienced engineers will always ensure that your equipment is in an optimal state and fully updated and secure.

Vulnerability Management & Remediation

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. Effective remediation entails continuous processes and is a critical element in the securing of your network. Vulnerabilities should be identified and remedied in good time to prevent weaknesses being exploited. Any of the equipment included within a managed infrastructure contract will be regularly audited and updated to confirm no known vulnerabilities go unaddressed.

24/7/365 Device Monitoring & Proactive Support

Our Network Operations Centre (NOC) provides device and network availability monitoring and alerting 24/7/365 via our technical support team. The status of key performance metrics such as uptime, CPU usage, memory usage and storage space are actively monitored. Our support team is notified when an issue is detected and you are notified as agreed, based on the priority level of a monitored device. Notifications are normally provided via telephone or email within 30 minutes of a critical alert.

The platform can monitor a variety of network equipment, such as routers, firewalls, switches, services, storage devices and other network devices. Each monitored device is allocated 10 monitored performance metrics, this can be increased subject to requirement.

Industry Leading SLAs

We pride ourselves with having some of the most robust SLAs in the business. With maximum response times as short as 30 minutes you can always rest assured there will be an experienced engineer available to assist.

Quarterly Business / Tech Reviews

Quarterly service reviews will be undertaken where case history and platform performance can be discussed. This gives you the opportunity to feedback on our performance and for us to advise on future direction, industry trends etc.

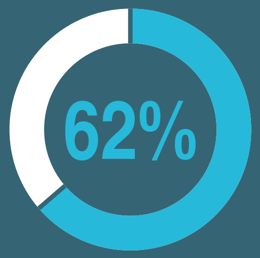
> **Let us shoulder your burden.**
>
> "There's no mystery here, this is about **highly trained staff** dedicated to **keeping your IT systems maintained and secure."**
>
> NetUtils CEO, Ashok Thomas

> **"The cyber security skills shortage is not just a problem confined to the UK.**
>
> Even though an additional 700,000 skilled workers joined the talent pool last year, **the study indicates a global shortfall of 3.21 million** and a **UK deficit of 27,000 vacancies** as of April 2020."
>
> 2020 Cyber Security Workforce Study

Silver – Protect Your Core

Access To Experts in Their Field

The managed firewall service addresses the cyber security skills gap head on. You no longer have to burden your staff with having to continually keep abreast of the ever-changing threat landscape, we've invested in our team so we can do this for you. If Cyber security is not your core business, then why invest in making your staff experts in it, instead deploy their valuable skills elsewhere in growing your organisation. Cyber security is our core business and with over 20+ years' experience and a workforce dedicated to protecting you now is the time to let us shoulder your burden and keep you safe.



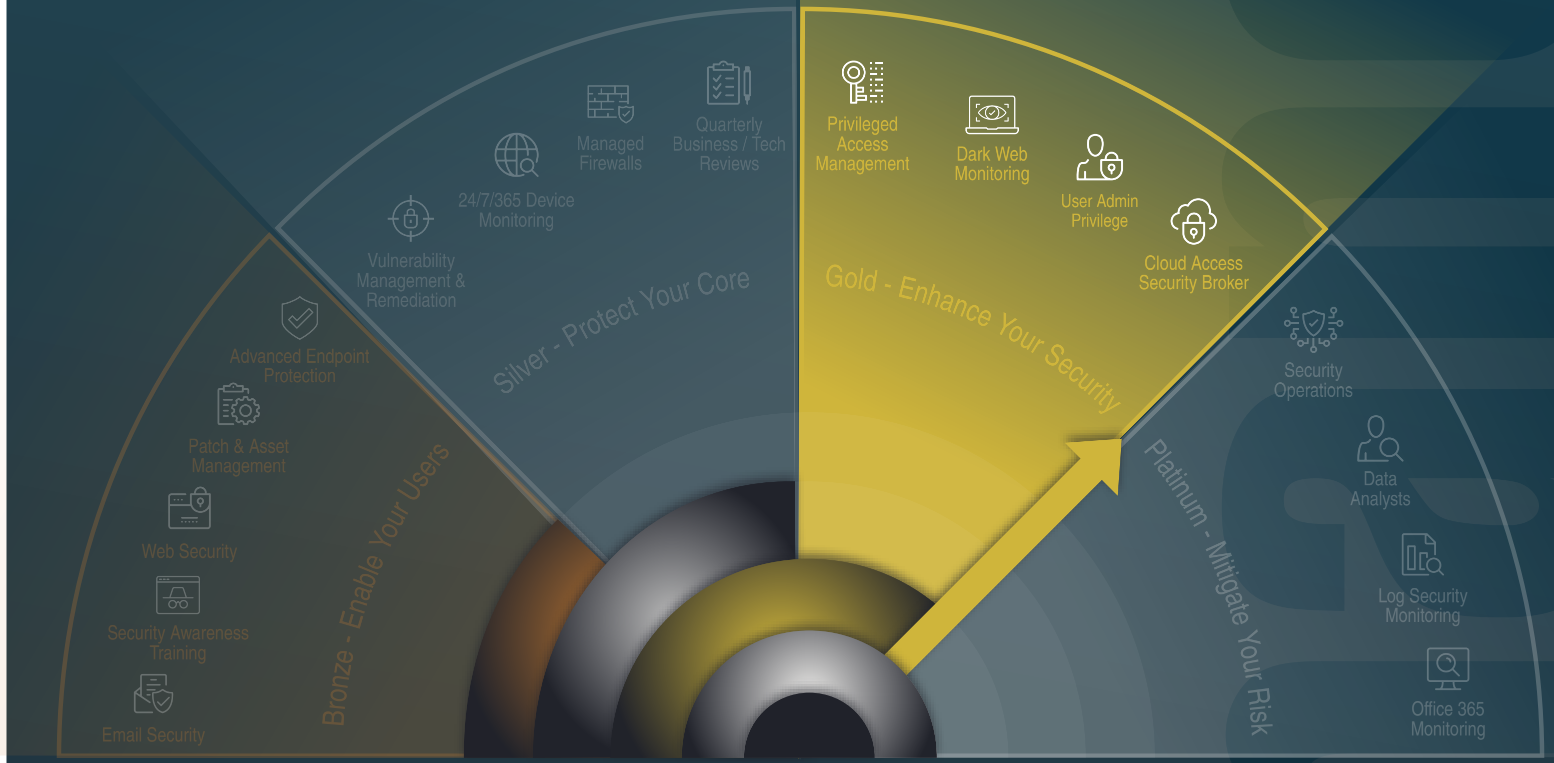
"62% of respondents indicate that **their organisation's cyber security team is** either somewhat or **significantly understaffed.**"

ISACA's Global State of Cyber Security – 2020

Below is a snapshot of some of the certifications we hold within our Technical Team, for further information or full engineer bios please get back in touch.

Juniper Networks JNCIS-SEC **JNCIS-ENT** JNCIP-ENT **JNCSP-SEC** JNCIS-SEC **JNCIP-SEC** JNCIS-ENT **JNCIS-SEC** JNCIA-Junos **JNCIA-SEC** JNCIA-Cloud **JNCDA-Design** **Fortinet** NSE 1 **NSE 2** NSE 3 **NSE 4** NSE 5 **NSE 6** NSE 7 **Palo Alto Networks** PSE Foundation **PSE Associate** Accredited Configuration Engineer (ACE) **Accredited Sales Executive (ASE)** Certified Network Security Engineer (PCNSE) **Accredited Configuration Engineer (ACE)** **Pulse Secure** Connect Secure Associate **Policy Secure Associate** Pulse One Associate **Connect Secure Associate** Policy Secure Associate **Pulse One Associate** **Personal Certs** CISSP **CISM** Member of the BCS, MBCS **PRINCE2 Practitioner** ITIL

Gold


Bronze - Enable Your Users
Advanced Endpoint Protection
Patch & Asset Management
Web Security
Security Awareness Training
Email Security
Silver - Protect Your Core
Vulnerability Management & Remediation
24/7/365 Device Monitoring
Managed Firewalls
Quarterly Business / Tech Reviews
Gold - Enhance Your Security
Privileged Access Management
Dark Web Monitoring
User Admin Privilege
Cloud Access Security Broker
Platinum - Mitigate Your Risk
Security Operations
Data Analysts
Log Security Monitoring
Office 365 Monitoring

Enhance Your Security

Gold - Enhance Your Security

Privileged Access Management

Dark Web Monitoring

User Admin Privilege

Cloud Access Security Broker

Elevate your security posture to the next level with a comprehensive end to end security platform dedicated to protecting your business. The NetUtils Gold managed service addresses internal and external threats posed from credential theft, shadow IT, data breaches and ransomware attacks and represents a robust and comprehensive set of security solutions, backed with the expertise of NetUtils' Technical Team managing them on your behalf.

"Users primarily access the dark web using the TOR browser.

2 Million

active users connect to the dark web through the TOR browser every day."

Privileged Access Management (PAM)

Effective and agile Privileged Account Management (PAM) has become mission-critical for organisations of every size. With our managed PAM service, it's now possible for even the smallest of organisations to adopt a robust privileged account security posture. Our managed PAM service gives you access to an enterprise-grade PAM solution at a fraction of the cost of traditional on-prem products.

So, what benefits will a PAM solution bring to my business?

- A PAM solution effectively sets up a barrier to guard against attacks, both external and internal, becoming a fundamental layer in your security posture.
- While many security solutions draw on the resources of the IT team a PAM solution actually improves IT efficiency. Particularly for application and support teams by increasing efficiency and enabling seamless user workflows.
- It helps mitigate risk and ensures compliance and confirmation with integrity, putting users into enforced workflows with full audits.
- Our PAM solution plays well with other tools contributing to the enhancing of your cyber security posture, adding additional layers of security, audit and enforcement.

Improve Security
Protect privileged accounts to tighten your attack surface and resilience.

Unburden IT Teams
Control PAM easily with a simplified interface and streamlined design or let us manage it on your behalf.

Audit And Report
Auditing, reporting, and alerts scheduled, or custom help proactively meet compliance obligations. Granular policy control applies across all devices and teams.

Detect Suspicious Activity
Real-time session monitoring & control includes proxying, session recording, and keystroke logging.

"An estimated **90% of posts on dark web forums** are from buyers looking **to contract someone for cyber crime."**

Dark Web Monitoring

Dark web activity has increased over 300% in the last 3 years with thousands of email addresses, passwords and other sensitive data being exposed on the dark web every day, the risks to your business are considerable. It is often the case that organisations have no idea that these vulnerabilities exist and therefore do nothing to address them.

While the information on the dark web is there to stay, having visibility of it and ensuring you know the types of compromises you have suffered is key in ensuring your defences are in place and your vulnerabilities addressed.

Our Dark Web Monitoring service ensures the greatest amount of protection with 24/7/365 human and machine-powered monitoring of business and personal credentials, including domains, IPs and email addresses. The service uncovers your compromised credentials in dark web markets, data dumps and other sources, and alerts you so you can take action. Having this information allows you to act before cyber criminals do.

Comprehensive, Validated Data
Delves into the dark web, including hidden chat rooms, unindexed sites, private websites, P2P (peer-to-peer) networks, IRC (internet relay chat) channels, social media platforms, Black market sites, 640,000+ botnets.

Deploy In Minutes
The service takes just minutes to set up via a secure SaaS platform and will start showing compromised results right away.

Supply Chain Monitoring
Monitor your third-party suppliers to determine if they are a potential risk to your organisation.

Real-Time Alerting
Receive real-time alerts the moment your data is found on the dark web.

User Admin Management

Admin rights management is not only a burden on the IT team but doing it poorly can also pose a significant risk to the business. It is no longer an option to allow admin access to users across the business, doing so not only introduces the risks of users installing malicious applications to their machines, but also allows cyber criminals when they do breach your defences to freely navigate the network.

Our next-gen user rights management tool is vital for scalability and efficiency. It's not just about managing user rights, but also about the fast flow of software installs, logs and audits, data protection, compliance and more.

The auditing functionality is granular and essential for data protection and compliance, supporting a full audit trail of allowed executions, blocked executions and passive mode monitored executions, with a 90-day retention for all logs.

Easy Escalation of Rights and Files
Fast-track management of local admin rights with grant and removal processes.

Full Control of The Escalation
View all user requests and grant (or deny) them for a selected time period.

Auto-Approval Mode to Avoid User Support Time
Eliminate manual escalation of rights from your networks.

Full Audit Trail
Check the endpoint's history of requests.

"88% of organisations surveyed say that **insider threat is a cause for alarm."**

ENISA Report for Insider Threat in 2020

netutils

Managed Cyber Security Services Platform

Gold - Enhance Your Security

Cloud Access Security Broker (CASB)

According to Gartner, the cloud access security broker (CASB) market can be defined as “products and services that address security gaps in an organisation’s use of cloud services... They deliver differentiated, cloud-specific capabilities generally not available as features in other security controls such as web application firewalls (WAFs), secure web gateways (SWGs) and enterprise firewalls.”

Our CASB enables your business to discover, analyse, secure and manage user interaction with cloud applications. Achieve complete visibility and control with a full-featured CASB solution and protect your modern mobile workforce. Integrated with web security for visibility and protection at every stage of an attack.

Cloud Data Security (DLP)
Analyse files uploaded to cloud apps. Use templates for personal data, confidential content, PCI DSS, HIPAA (etc.)

Visibility or Control
Reveal applications that are in use (sanctioned and non-sanctioned) or block access to features and actions within apps.

Flexible Deployment
Agents, gateways, or both, with centralised policy management to protect office and mobile users.

Extensive App Catalogue
Automated, continuous updates to a catalogue of hundreds of business applications and thousands of actions.

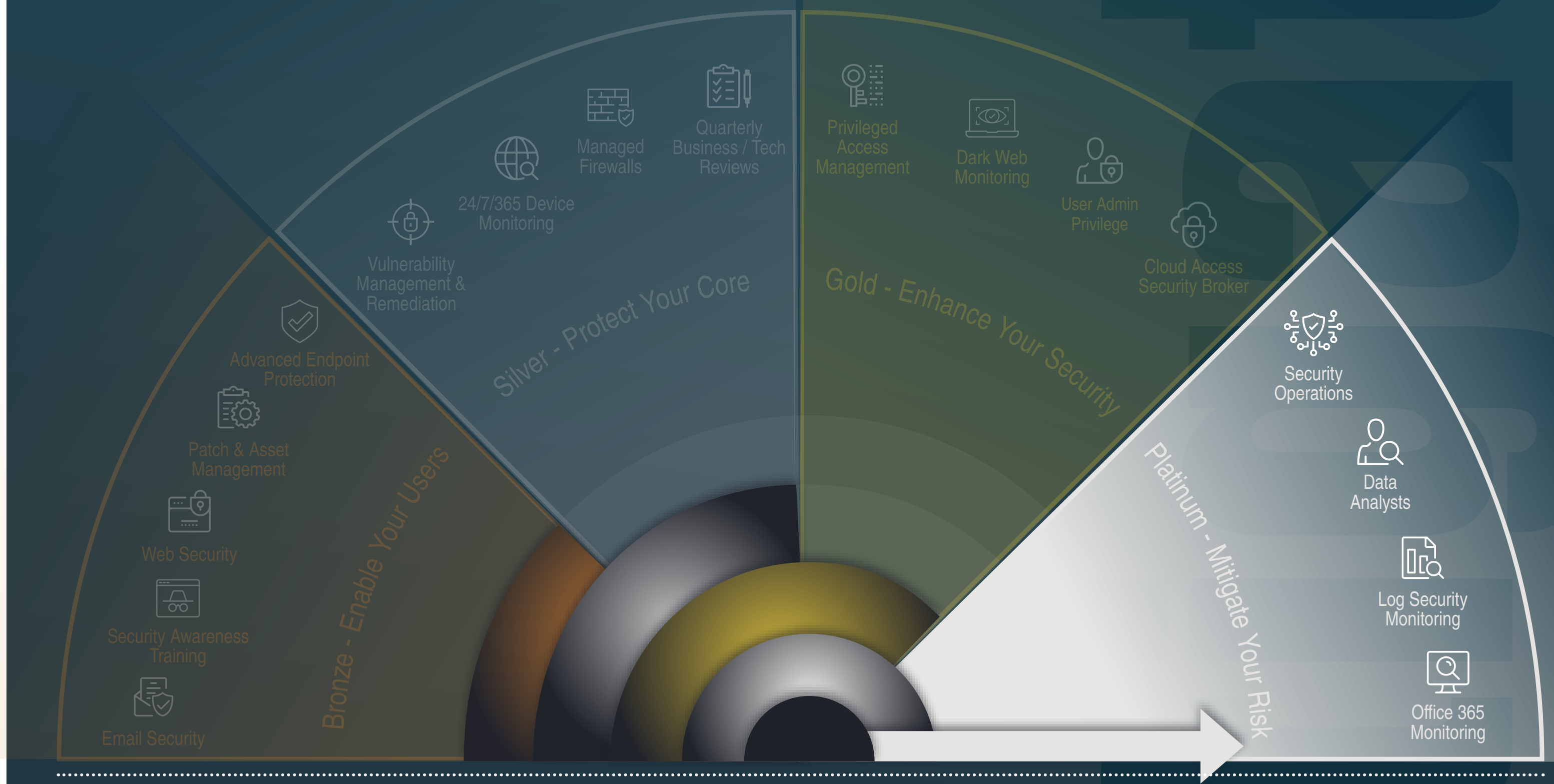
Integrate with Web Security
Integrates seamlessly with our existing web security solution and can be enabled with a single click.

> **“Shadow IT refers to information technology used by employees without the knowledge of the company’s IT department.**
>
> E.g. personal messengers, video conferencing, collaboration tools or file transfer or sharing services.”

“42 percent of respondents state that they **are using personal email accounts for work without the approval of their employers’ IT team.”**

Statista Report 2020

Platinum



Bronze - Enable Your Users
Advanced Endpoint Protection
Patch & Asset Management
Web Security
Security Awareness Training
Email Security
Silver - Protect Your Core
Vulnerability Management & Remediation
24/7/365 Device Monitoring
Managed Firewalls
Quarterly Business / Tech Reviews
Gold - Enhance Your Security
Privileged Access Management
Dark Web Monitoring
User Admin Privilege
Cloud Access Security Broker
Platinum - Mitigate Your Risk
Security Operations
Data Analysts
Log Security Monitoring
Office 365 Monitoring

Mitigate Your Risk

Platinum - Mitigate Your Risk

Security Operations

Data Analysts

Log Security Monitoring

Office 365 Monitoring

The ultimate eyes on protection needed in every organisation’s cyber security arsenal. The NetUtils Platinum managed service is a set of security products that collect, aggregates and normalises data from your network across hundreds of sources including O365 to facilitate AI enabled analysis using our analytics platform, SIEM, threat intelligence, and 24/7/365 Security Operations Centre.

Log Security Monitoring

The NetUtils SOC provides you with access to a fully managed 24/7/365 security operations centre. The service uses leading edge technology paired with human talent, with just a single objective, to monitor your network, protect your assets and keep your business safe.

The SOC collects, aggregates, and normalises log data from hundreds of sources for AI enabled analysis using an analytics platform, SIEM, threat intelligence, and of course the individuals manning the 24/7/365 operations centre. Our service identifies threat-like behaviour in your systems such as impossible logins, multi-factor bypass, coordinated attacks, and rogue agents.

Key Features

- Hundreds of Support Integrations
- SIEM Analysis
- AI Analytics Engine
- Self-service Reporting
- Deployment of physical or virtual appliance for on-prem logs (like syslog)
- Supports key industry and regulatory compliance standards such as continuous monitoring and log retention
- ROI on existing investments – Merge data from your existing security tools with multiple sources to provide greater visibility and re-use existing investment

> “As organisations continue to move to the cloud, encrypt communications, adopt IoT, and manage third-party vendors, the **complexity of the network increases.**
>
> This in turn, **impedes visibility, slows operations, and impacts security.”**
>
> www.csoonline.com

Typically Log Security Monitoring will protect you against activities like:

3rd Party Violation

Monitors activity by external vendors and partners who have access to organisational systems, to identify anomalous behaviour or escalation of privileges.

Unauthorised Access

Monitoring who is accessing devices and where they connect to, and alert when source or target is unknown or suspicious.

Compromised User Credentials

Uses behavioural analysis to detect anomalous behaviour by users, indicating a compromise. For example, logins at unusual hours or at unusual frequency.

Cloud Infrastructure Attack

Alerts on threat-like behaviour in AWS services.

Anomalous Privilege Escalation

Detects users changing or escalating privileges for critical systems.

Multi Vector Attack

Correlates data from multiple sources to get consolidated visibility of multiple attacks.

O365 Security Monitoring

The NetUtils SOC monitors Office 365 activity using an analytics platform, SIEM, threat intelligence and 24/7/365 Security Operations Centre to identify threat-like behaviour such as unauthorised access to cloud mailboxes, admin changes in the environment, impossible logins, and brute force attacks.

Key Features

- SIEM Correlation & SOC Analysis
- Support for custom alerting and reports
- Visibility to login activity in the dashboard
- Detects potential threats of suspicious activity in Office 365
- Supports industry & regulatory compliance requirements

Typically O365 Security Monitoring will protect you against activities like:

Malicious Admin Changes

Tracks admin activity and changes to the O365 tenant.

Foreign Login

Monitors geolocation access with IP location sourcing and login from suspicious or unusual countries.

Impossible Login

Detects logins from different geolocations within a short period of time.

Unauthorised Delegate Access

Tracks when emails delegates are added.

Failed or Unauthorised Access

Detects failed or suspicious login attempt.

Suspicious Email Forward

Alerts when email forwarding rules have been created outside of the domain.

> “A high proportion of UK businesses continue to **lack staff with the technical skills, incident response skills and governance skills needed** to manage their cyber security.”
>
> Cyber Security Skills In The UK Labour Market 2021 Report

Platinum - Mitigate Your Risk

The Human Element – The SOC Team

Fully managed Security Monitoring means our automated advanced search & detection technology is backed by a team of certified security analysts. These experts in the Security Operations Centre (SOC) manage, tune and monitor our systems and your business's data 24/7/365 to ensure you are protected. The SOC Team protects your business with the combination of machine and human analysis. We use some terms and processes in our service delivery that hopefully give you some context into the workings behind the scenes.

Definition

- **Alert** - An observable occurrence in a protected server, application, or, more broadly, the internet that may imply a potential threat to an information system or a potential compliance issue.
- **Alarm** - A pattern of potentially malicious activity that implies an identified threat to an information system, violates acceptable use policies, or circumvents standard security practices. We classify incidents into three threat severity ratings: High, Medium, and Low.

Expert SOC Research, Escalation, and Response - Identified incidents are reviewed and researched by security certified professionals who:

- Proactively research threats
- Our SOC experts are skilled in threat research and the art of the identification of suspicious activity known in the industry as "Threat Hunting."
- Escalate priority incidents

Ready 24/7/365, our team of experts are trained in straightforward explanations of security findings. Priority Incidents / Alarms are escalated to you according to your designated escalation path.

- **Respond for Remediation**

  When an escalated incident requires remediation, our SOC experts are available to provide remote remediation assistance and advice.

Get **more visibility** into your systems.

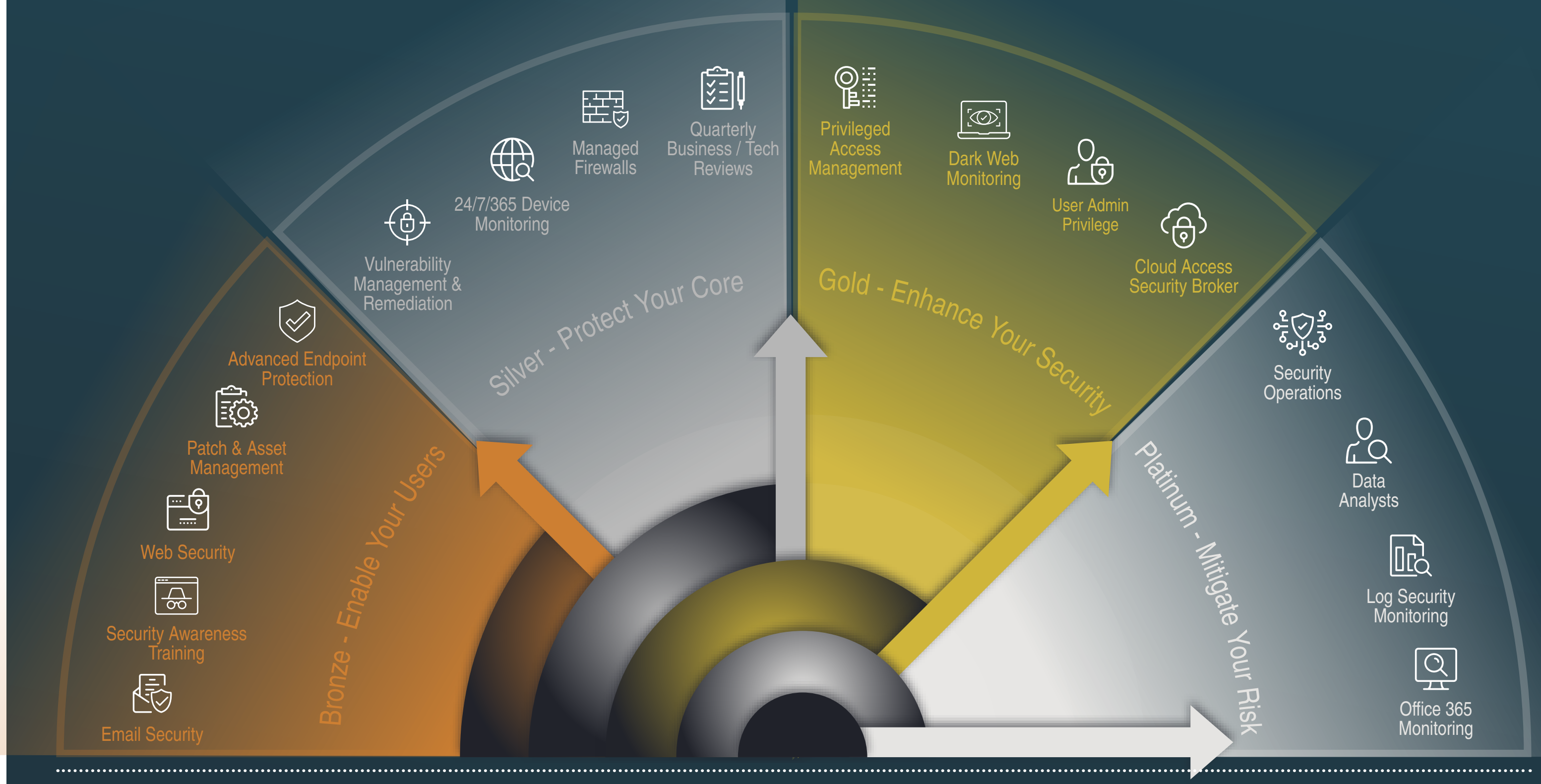
"59% of respondents believe that **lack of network visibility poses a high or very high risk to their operations.**"

2020 SANS Network Visibility & Threat Detection Survey

netutils

Managed Cyber Security Platform

Your Entire Security Posture-as-a-Service


Bronze - Enable Your Users
Advanced Endpoint Protection
Patch & Asset Management
Web Security
Security Awareness Training
Email Security
Silver - Protect Your Core
Vulnerability Management & Remediation
24/7/365 Device Monitoring
Managed Firewalls
Quarterly Business / Tech Reviews
Gold - Enhance Your Security
Privileged Access Management
Dark Web Monitoring
User Admin Privilege
Cloud Access Security Broker
Platinum - Mitigate Your Risk
Security Operations
Data Analysts
Log Security Monitoring
Office 365 Monitoring

Enable | Protect | Enhance | Mitigate

netutils

t: 020 8783 3800
e: info@netutils.com

w: netutils.com | b: netutilsblog.com

About NetUtils

We are a leading UK specialist integrator of network, security and data solutions for enterprise, telco, MSPs and ISPs. With more than 27-years history and over 400 enterprise and service provider clients including many listed within the FTSE 100, NetUtils brings its customers the depth and breadth of people, technologies and services to improve business performance in this ever-changing digital world.

CYBER ESSENTIALS CERTIFIED PLUS

QMS ISO 9001 REGISTERED

QMS ISO 27001 REGISTERED

Crown
Commercial
Service
Supplier