# Armour Networks Managed IT Service (MITS)

Effective January 2023

armournetworks

## MAINTAINING & SECURING

Your infrastructure proactively

### DEDICATED NETWORK ADMINISTRATOR

- Technology Checklist
- Best Practices
- Scheduled & On-Demand Reporting

### PROACTIVE IT MANAGED SERVICES

- Patch Management
- Anti-Spyware Management
- Email Threats Management
- Desktop optimisation
- SOC-2 Compliant documentation
- State of art Backup

## SUPPORTING

Your business 24/7

### CUSTOMER SUPPORT TEAM

- Helpdesk Support
- On-site Support
- Problem Isolation & Resolution
- Incident Response & Management
- Service Desk Portal
- Remote Support Framework

### DEDICATED VCIO

- Technology Summary
- Design Desk Resources
- Budget Planning
- Business Impact on Technology Decisions

Our ArmourNet MITS Program is a comprehensive IT Managed Services solution which covers a  whole lot more than most other offerings seen in the industry and is what separates us from the crowd.

Shifting from a technical to a business relationship to address the business impact of technology in your organisation, our ArmourNet MITS Program assures you have your very own internal IT department focused on technology standards and alignment together with business impact and IT strategy.

## Simple Pricing, Best Value.

We don't believe in long-term contracts. Our SLAs terms are no longer than 3 months, as we are confident about your satisfaction with us.

Not only will you have unlimited access to our highly accredited technical team, you will also be assigned with a virtual Chief Information Officer (vCIO) performing scheduled proactive visits helping you understand the business impact of technology and who will be responsible for implementing a series of best practices for key technology areas to align your technology with high standards on a regular basis.

# Dedicated IT Management (vCIO)

## Understanding Your Business

A function of our engagement is to have a complete mastery of your business use of technology. This goes beyond basics including industry trends, business applications, or compliance requirements. This implies that we need to understand what your business does, how you do it, and what your technology does for you in order to provide you with the highest level of our service.

## Client Education

We will educate you in various technology topics ranging from security, compliance, and new technologies. This is not the opportunity to lecture you on what you do right or wrong. It is rather to keep you aware of trends. If a new service may benefit you, it is best to inform you in advance before the next budget period. When the time is right to adopt the new solution, you would already be aware of the benefits.

## Technology Business Reviews

Technology business reviews are for advocating improvements and alignment to defined standards. This is a regular monthly or quarterly face to face meeting where we will cover reactive support, ongoing projects, and recommendations for further improvements.

## Life Cycle Budgeting & Warranty

Out state-of-art Asset Life Cycle Management is not only capable of helping you with budgeting and device replacement due to warranty expiration. Unless your technology is very outdated, in most of the cases, we can extend the warranties of your 'in working order' devices perpetually, which can save your business thousands of dollars. It is our mission to keep your DMI (Digital Maturity Index) score high for as little expense as possible.

## New Technology Planning

When you contemplate new technology, we as your vCIO become your liaison. A successful project must consider expenses, infrastructure requirements, downtime, and scope of work. The need to see value early in the decision-making process prevents unforeseen issues. We will work with you to evaluate the options and implementation process.

## Modern Workplace Technology Training

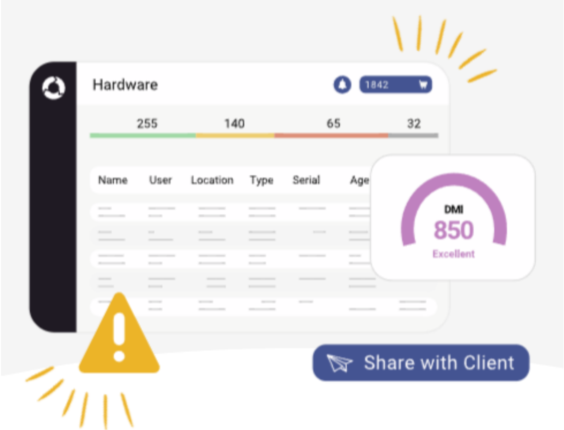
Modern workplace technologies represent a complete change in direction from what businesses are used to. Once these new technologies are introduced into your organisation, we will host focus group sessions with your staff showing them what's possible and how best to adapt their current processes and workflows with the technology.

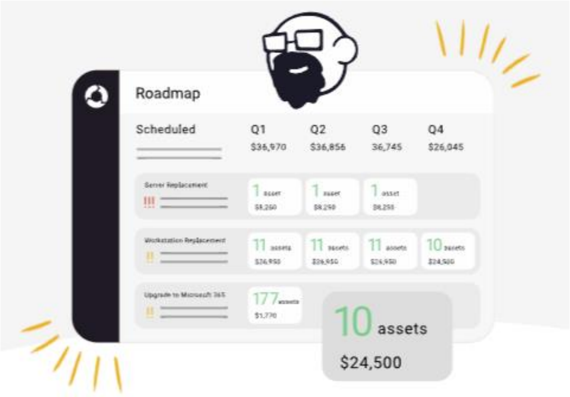
## Strategic Roadmap

We will keep up to date a 12-month strategic technology roadmap for your organisation. The plan will contain projects that enable you to align with a defined set of best practices and focuses on technical alignment and business goals.

## Budgeting

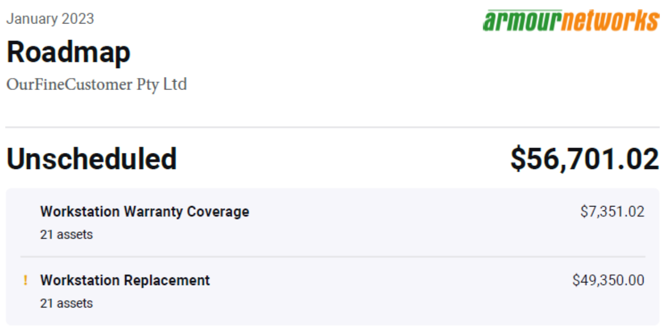
A budget is as equal in importance to recommendations and a strategic roadmap. Planning and allocating funds ahead of time prevents surprise expenditures. Broken down per month or quarter, granular budgets make planning for items more manageable and advanced awareness of projects and their costs puts will put you more at ease.




Roadmap

| Scheduled | Q1<br>$36,970 | Q2<br>$36,856 | Q3<br>36,745 | Q4<br>$26,045 |
|---|---|---|---|---|
| Server Replacement<br>!!! | 1 asset<br>$8,250 | 1 asset<br>$8,250 | 1 asset<br>$8,250 | |
| Workstation Replacement<br>!! | 11 assets<br>$26,950 | 11 assets<br>$26,950 | 11 assets<br>$26,950 | 10 assets<br>$24,500 |
| Upgrade to Microsoft 365<br>!! | 177 assets<br>$1,770 | | | |

10 assets
$24,500


January 2023

**Roadmap**

OurFineCustomer Pty Ltd

| Unscheduled | $56,701.02 |
|---|---|
| Workstation Warranty Coverage<br>21 assets | $7,351.02 |
| ! Workstation Replacement<br>21 assets | $49,350.00 |

*The difference between assets replacement and our premium business warranty extension service could mean **65%-85% savings** to your business. We offer 12, 24, 36 months coverage for qualified devices beyond regular (or extended) vendor warranty. Not applicable to MacOS and Microsoft Surface devices.*

# Proactive IT Managed Services

We have developed comprehensive checklists that we run through to keep all components of your network in excellent order. Our Network Monitoring System sends us alerts when any key variable on your network reaches a warning or critical state, so we can act upon the alert before you even know there's a problem.

## Network Monitoring

Network Monitoring is critical for the delivery of management services that keep your IT infrastructure up and running. Our system-monitoring program allows us to detect and respond to any critical issues before they reach a crisis level, as well as encouraging us to become more proactive and create improved infrastructure planning decisions based on historical trending and detailed usage analysis.

## Technical Documentation

We will keep up to date comprehensive technical documentation of your network to simplify and speed up future troubleshooting of any technical issues. We will also compile and send you a monthly top-level report which summarises key network indicators over the month. This will highlight any concerns which may come up from time to time.

## Software License Management

We will administer and maintain the currency of software licenses and subscriptions for your IT assets and users. Our comprehensive license management will ensure that you will maintain license compliance.

Whenever new licenses or subscriptions are purchased, installed, or upgraded, we will maintain and keep up to date this information as part of our Asset Management processes.

## IT Asset Management

Discovering and managing IT assets is a tough job especially when it comes to keeping track of IT inventory. Our Asset Management system automates a lot of this work and records any changes made on your IT Assets in real-time.

When a new IT device is installed, it will be issued with a unique Asset ID and all appropriate details such as the device name, serial number, and any warranty details together with renewal or expiration dates will be recorded and tracked.

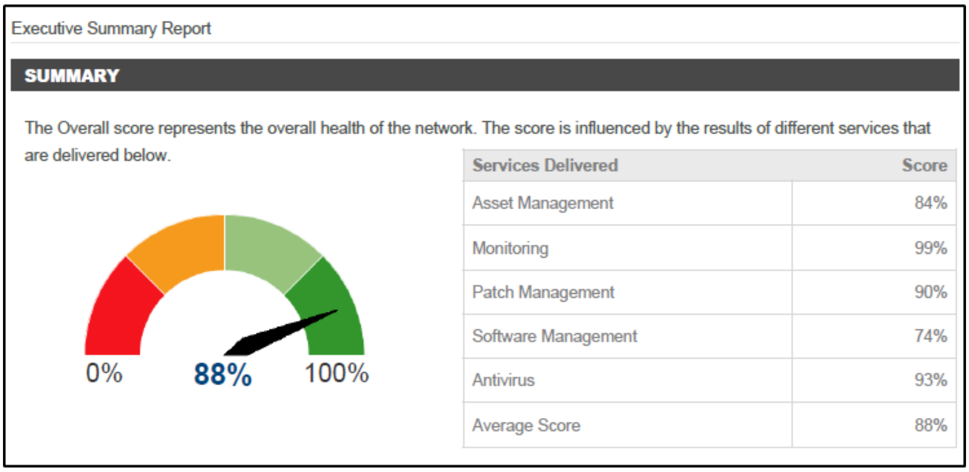
Technical work performed or related to any IT device will be logged against the Asset ID. When any warranty or license needs to be renewed a notification email will be sent at least one month prior so we can discuss options going forward.

With all your IT Asset information being recorded and tracked, we can provide high-level management reports such as providing a list of all your computer's hardware specifications.

## Reporting

The reporting tool as part of our Network Monitoring system allows us to gain insight into your IT infrastructure. Strategic operations are maintained through utilization, network assessment, capacity and event reporting. Providing "on-demand" reports also simplifies the process of troubleshooting issues and we can quickly demonstrate the need for more resources with capacity reports or highlight strategic improvements using our network assessment reports.

These reports cover such key areas as device inventory, pricing, antivirus protection, backup integrity, user audits, hardware and software check-ups, and more. That's data we can immediately use to improve your IT environment.



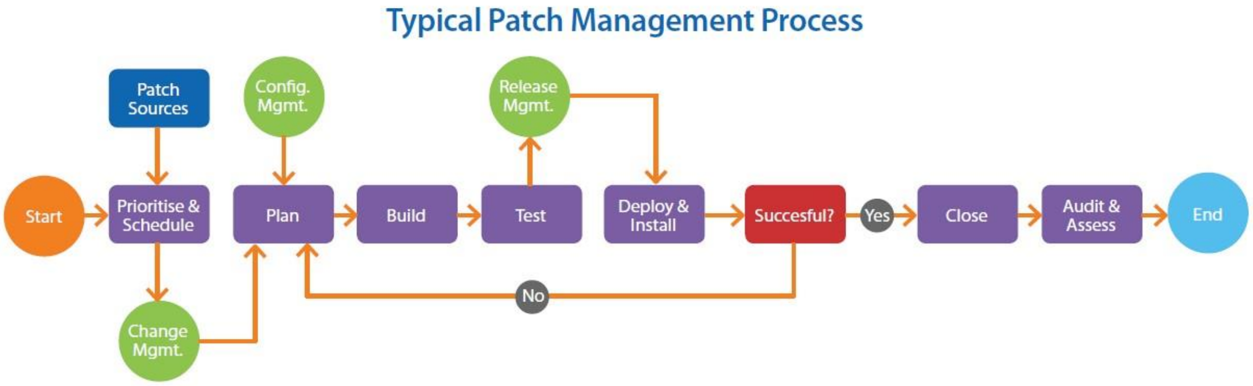
Executive Summary Report

SUMMARY

The Overall score represents the overall health of the network. The score is influenced by the results of different services that are delivered below.

| Services Delivered | Score |
|---|---|
| Asset Management | 84% |
| Monitoring | 99% |
| Patch Management | 90% |
| Software Management | 74% |
| Antivirus | 93% |
| Average Score | 88% |

## Patch Management



It all boils down to being proactive instead of reactive. Proactive management anticipates problems in advance and develops policies to deal with them; reactive management adds layer upon layer of hastily thought up solutions patched together using bits of string and glue. It's easy to see which approach will unravel in the event of a crisis.

Patch management is often seen as a trivial task. Simply click on 'update' and that's it. But, there is a lot more to it and a proper policy is certainly not overkill.

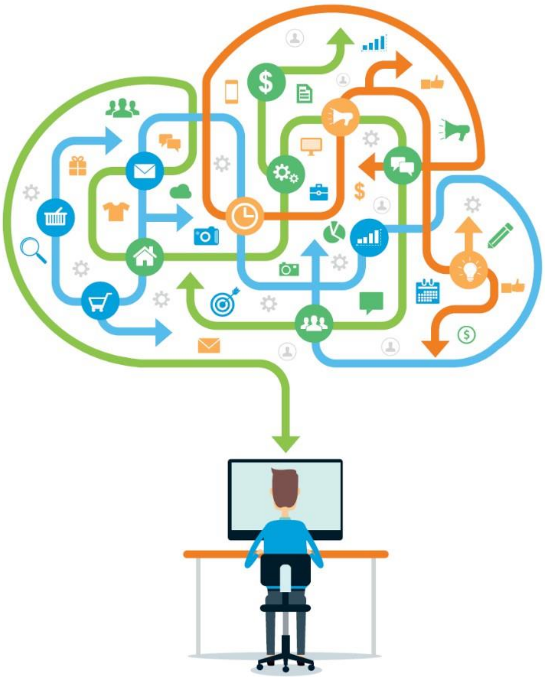
Effective patch management has become a necessity in today's information technology environments. Reasons for this necessity are:

- The ongoing discovery of vulnerabilities in existing operating systems and applications
- The continuing threat of attackers developing applications that exploit those vulnerabilities
- Vendor requirements to patch vulnerabilities via the release of patches and updates

One of the easiest ways for hackers to breach networks is by targeting the vulnerabilities of out-of-date software. In fact, without vigilant patching, you could be exposed to major attacks like WannaCry or Petya. That's why keeping software current with the latest security patches is essential for strong cybersecurity.

Our proactive patch management approach anticipates problems in advance, and we develop policies to deal with them in a tried and tested manner.

## Automation & Self-Healing



By automating checks and alerts, automatically approving critical patches, and taking care of routine tasks like system restarts and cleaning out temp files,  the system manages most behind the scenes potential issues on autopilot. We will also set up automatic fixes for problem scenarios such as an application failing. This allows us to fix problems quickly, often before your staff would even know about them.

Some common uses of automation scripts are:

- ✓ Automate software deployment
- ✓ Modify computer settings
- ✓ Modify registry settings
- ✓ Automate computer maintenance
- ✓ Automate the updating of third-party applications

Self-healing is a pre-configured response and action to specific types of service failures. When a failure occurs, our monitoring agent automatically restarts the service or executes a preconfigured script to try to resolve the issue. The system then verifies if the problem has been resolved and sends the appropriate notifications.

# Network Administration

Our team of IT experts will fully manage your organisation's network and keep your IT Systems operational constantly monitoring functions and operations within your network.

We are essentially responsible for installing, maintaining and upgrading any software or hardware required to efficiently run your Servers and computers.

## Infrastructure Management

- ✓ Manage the performance and availability of the LAN and WAN
- ✓ Maintenance and reconfiguration of existing settings
- ✓ Resolving outages and performance degradations
- ✓ Tracking usage bandwidth
- ✓ Managing capacity
- ✓ Managing 3rd party relationships

We will provide a proactive fault, performance, and availability management service for your LAN and WAN. Essentially this encompasses devices such as your network switches, routers, Wireless Access Points and UPS's etc.

A network audit will be performed during the transition stage and the results documented and used to form the baseline for future measurement purposes.

The results of the network audit may also identify a requirement to redesign aspects of the network and its components which we will advise accordingly.

We also manage and provide support for all your IT peripherals and will keep firmware up to date on devices when required as well as conducting necessary preventative checks. This includes your devices such as your Thin Client terminals, Printers, Scanners, Network Switches, Wireless Access Points and UPS's.

# IT Security

- ✓ Review all security configurations and update them in line with business needs
- ✓ Configuration and management of Firewalls and Network permissions
- ✓ Ensuring the integrity and currency of all LAN user ID's and passwords
- ✓ Regular Audits of logs to check for suspicious activities, unauthorised logon attempts
- ✓ Compliance Audits
- ✓ Manage workstation and server patching levels and provide ongoing vulnerability assessments as a business-as-usual function.
- ✓ Catch unauthorized login attempts to restricted computers and detect an unusual midnight log-in.
- ✓ Be alerted to unauthorized connections to the network.
- ✓ In the event of breach, data loss or ransomware attack, rapidly respond and provide a full suite of services including data recovery, server configuration, network reconfiguration, investigation and analysis.

Securing an organisation's data and systems is a continually evolving process. We take a holistic approach to security and assess your entire technology stack to ensure it complies with the Australian Cyber Security Centre (ACSC) standards.

We will assist with adopting appropriate technical and organisational measures in order to ensure the confidentiality, integrity, security and availability of your organisation's IT assets, information, data and IT services.

By integrating the leading best of breed security products with our highly trained technical team, we keep your network safe and secure and will maintain authorised access control and integrity of your network. All security change requests will only be actioned when provided in writing from authorised personnel only. All changes made will be logged and tracked as part of our IT governance policy.

## On premise Gateway Security (Firewall)

- ✓ 24x7 Connection monitoring
- ✓ Critical Event Alerting
- ✓ Firmware Updates
- ✓ Configuration backup
- ✓ Technical Support
- ✓ Comprehensive usage reporting (requires license)
- ✓ Emergency loan Firewall

We will keep your Firewall's firmware up to date and the configuration backed up. And for added peace of mind we will supply you with an emergency loan firewall to get you up and running quickly in case of any failure with your current firewall.

We will also provide monthly monitoring reports showing all security activity passing through the firewall and where possible will include granular reporting down to the user level (Subscription license required).

## Active Directory (AD) Security

- ✓ Manage users and groups (add, delete, edit)
- ✓ Manage access privileges to network resources
- ✓ Develop and maintain network group policies
- ✓ Implement Robust AD Administration Privileges and limit Domain User accounts

## Anti-Virus & Spam Filtering (licenses required)

- ✓ Identify and quarantine out of date or unpatched computers which have access to the network
- ✓ Ensure all Servers and Computers have up to date Antivirus and AntiSpam protection configured properly
- ✓ Alerts sent of unprotected computers
- ✓ Keep up to date black/white lists of accessible networks
- ✓ Control access to compact disk drives, usb and communication ports
- ✓ Control which applications can be installed

## Endpoint Detection & Recovery (licenses required)

We ensure that best of breed next generation Detection, Prevention, and Recovery Control software is installed on all Servers and computers at all times to protect against malicious code and that appropriate user awareness procedures are implemented and maintained.

Unlike traditional signature-based security products, next generation AV solutions are based on dynamic behavioural analysis techniques in combination with machine learning and intelligent automation. With this, even infections with unknown or stealthy malicious code can be identified and automatically blocked within a few seconds on the basis of its execution behaviour before damage occurs.

## Device Encryption

Bitlocker which is built into Windows 10 Pro will encrypt your hard drive thus protecting your data in the event a corporate owned laptop was stolen. The criminal would not be able to read any data off the hard drive due to the encryption.

## Office 365 Security (Add-on licenses required)

Our approach to securing your office 365 environment is to ensure you have the following protection mechanisms in place.

### ✓ Enabling Password Protection

To help users avoid choosing weak and vulnerable passwords, Azure AD Password Protection will block a wider range of easily guessable passwords.

### ✓ Enabling Multi Factor Authentication for all accounts requiring a username and password to log in

This is a method of confirming your identity before logging onto your Office365/Azure cloud environment by using a combination of two different factors: 1) something you know e.g. Password or PIN, 2) something you have e.g. Mobile, Apple watch, or 3) something you are e.g. FaceID, Windows Hello. With Azure Identity Protection and conditional access, machine learning, access location and risk assessment will be used to intelligently know when to challenge a user for MFA.

### ✓ Enabling Self Service Password Reset for all accounts requiring a username and password to log in

A more secure way for users to reset their passwords if forgotten. This method also ensures that the new password complies with the password protection policy mentioned above.

### ✓ Restricting Legacy apps that don't support modern authentication to Office365

Any application or service using old and unsecure protocols trying to access your Office365 environment will be blocked. E.g. Older versions of MS Office suite of products (Outlook 2013, 2010).

### ✓ Disabling persistent browser session when outside the office

A persistent browser session allows users to remain signed in after closing and reopening their browser window. This behavior when outside the office or on unmanaged devices can become a security risk. As a result, this is disabled when accessing from outside the office.

### ✓ User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource. We set timeout limit on browser and applications when accessed from outside the office. Note that these time limits are very reasonable and ensure that the user's experience is not degraded.

### ✓ Customizing Office 365 Sign In page

This involves customizing your Office 365 sign in page with your corporate logo and picture so that your users can easily recognize it and differentiate between a fake Office 365 sign in page and your legitimate one.

### ✓ Configuring Cloud App Security policies

With Office 365 Cloud App Security, we can set up notifications of triggered alerts for a typical or suspicious activities, see how your organisation's data in Office 365 is accessed and used, suspend user accounts exhibiting suspicious activity, and require users to log back in to Office 365 apps after an alert has been triggered. Cloud App security can also monitor and protect data hosted with other 3rd party cloud solutions such as Salesforce, Google, Dropbox, etc….

### ✓ Update DNS records (SPF, DMARC and DKIM records)

These records will be configured in your environment to further strengthen your Office 365 email security platform.

### ✓ Configuring Exchange Online Protection and Advanced Threat Protection (ATP) policies with Scheduled reporting

This will safeguard your organisation against malicious threats posed by email messages, links (URLs) and collaboration tools. The following policies will be configured and enabled: ATP Safe Attachments, ATP Safe Links, ATP anti-phishing and anti-spam protection, Attack Simulation (end-user training to becoming experts at identifying phishing emails). Scheduled reports will be configured to be emailed to you and any other person you nominate on a Monthly basis.

### ✓ Configuring and enabling Access reviews

We'll configure monthly and quarterly access reviews for you to review and take action to either remove or keep users from email groups, teams, SharePoint TeamSite and Office365 groups. This ensures that the users have the right access as they move to different departments or depart from your organisation.

### ✓ Intune MDM (Optional) - Addon license required

To protect your corporate data on corporate owned devices such as mobile devices and be able to manage them remotely, Intune MDM can be enabled, configured and have your corporate devices enrolled in it.

The Intune MDM profiles will get installed on the devices. The profile will carry settings for email, Wi-Fi, corporate sanctioned apps, device features and restrictions to help protect both devices and the data.

## Server Management

### Physical Server Hosts | VMware, Citrix, Hyper-V

- ✓ 24x7 System monitoring and Alerting
- ✓ Firmware updates
- ✓ Onsite & Remote Technical Support
- ✓ Emergency loan Server

We will monitor your Server hosts with e-mail alerts sent to our NOC team when any critical thresholds are reached. This includes monitoring the HDD, RAID Status, Memory and CPU and will arrange warranty replacements for any faulty hardware when required.  As we keep a history of all monitoring data, we will review the comprehensive reports which will highlight any trends for us to be aware of.

We will also ensure all the latest firmware updates are applied on a regular basis as well as any critical security patches and updates as they are released.

For added peace of mind we will provide you with an emergency loan Server to get you up and running quickly in case of any hardware failure with your current Server host.

### Servers | Operating System (physical or virtual)

- ✓ 24x7 System monitoring and alerting
- ✓ Realtime System Services monitoring (self-healing)
- ✓ Server Log Monitoring
- ✓ AV Software Updating
- ✓ Malware scanning
- ✓ Weekly System & Disk Optimisation
- ✓ Operating System Updates & Patching
- ✓ Onsite & Remote Technical Support
- ✓ Vendor liaison

We have developed a comprehensive checklist for server maintenance which is performed each month. This includes investigating error logs, which ensures your server remains free from corruption & unlikely to create disruptions to your business operations. We also conduct weekly disk defragmentation, perform system optimisation and ensure that the antivirus software is being updated regularly and that a weekly Malware scan is conducted.

Server Maintenance also includes the monthly patching of only prequalified Operating System and Security patches as well as Server restarts.  Furthermore our Server monitoring system performs self-healing on any failed critical services. This means that the system will automatically attempt 3 times to restart any failed services whereby providing rapid rectification of common issues. Any triggered self-healing attempts sends an alert to our NOC team for further investigation.

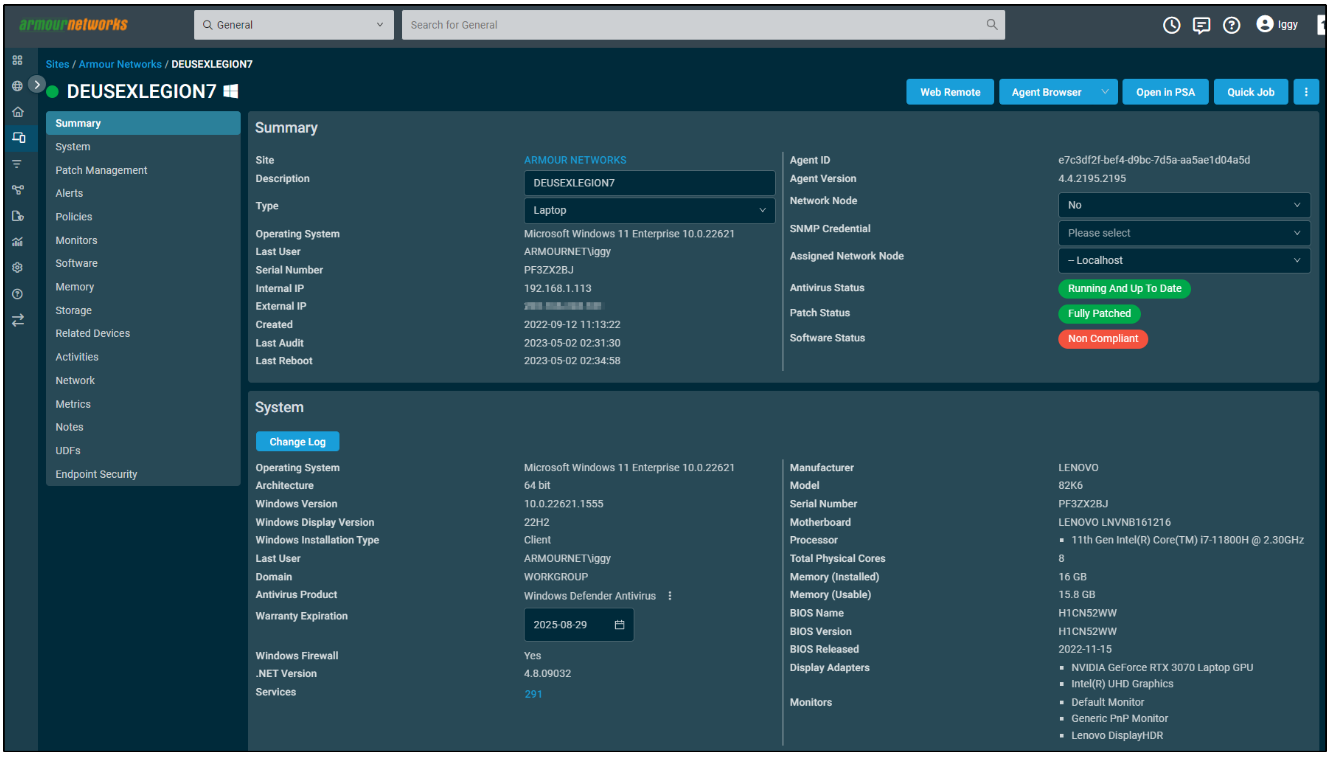
And lastly, where your Server is running bare metal on your physical host, for added peace of mind we will supply you with an emergency loan Server to get you up and running quickly in case of any hardware failure with your current Server.

## Desktop Management

- ✓ 24x7 System monitoring (connectivity and Asset monitoring)
- ✓ Operating System Updates & Patching
- ✓ AV Software Updating
- ✓ Malware scanning
- ✓ Hardware upgrades
- ✓ Operating system rebuilds
- ✓ Software installation and updating
- ✓ 3rd party vendor liaison
- ✓ Emergency loan computer/laptop

Technical support provides diagnosing and resolving problems including supporting customer specific applications and user orientation. Hardware maintenance services ensures that any faulty hardware is repaired at minimum inconvenience to the user and we will provide a temporary loan device where necessary.

As part of managing your fleet of computers and laptops, we track all hardware details such as Hard Disk size, free disk space, RAM size and CPU type to name a few as well as Software applications installed. We keep a 3-month history of this data and can provide comprehensive reports which will highlight any  trends to be aware of.



DEUSEXLEGION7

Summary

Site: ARMOUR NETWORKS
Description: DEUSEXLEGION7
Type: Laptop
Operating System: Microsoft Windows 11 Enterprise 10.0.22621
Last User: ARMOURNET\iggy
Serial Number: PF3ZX2BJ
Internal IP: 192.168.1.113
External IP: [redacted]
Created: 2022-09-12 11:13:22
Last Audit: 2023-05-02 02:31:30
Last Reboot: 2023-05-02 02:34:58

Agent ID: e7c3df2f-bef4-d9bc-7d5a-aa5ae1d04a5d
Agent Version: 4.4.2195.2195
Network Node: No
SNMP Credential: Please select
Assigned Network Node: – Localhost
Antivirus Status: Running And Up To Date
Patch Status: Fully Patched
Software Status: Non Compliant

System

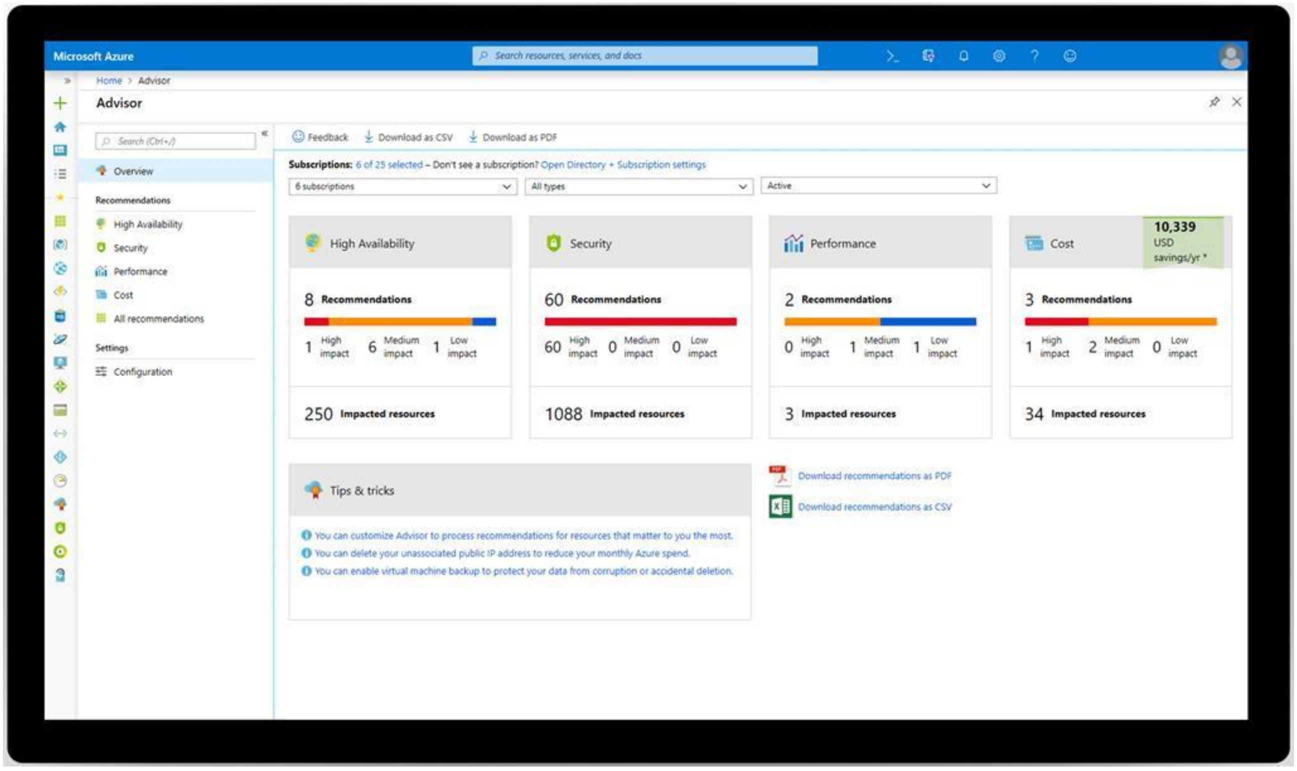
Operating System: Microsoft Windows 11 Enterprise 10.0.22621
Architecture: 64 bit
Windows Version: 10.0.22621.1555
Windows Display Version: 22H2
Windows Installation Type: Client
Last User: ARMOURNET\iggy
Domain: WORKGROUP
Antivirus Product: Windows Defender Antivirus
Warranty Expiration: 2025-08-29
Windows Firewall: Yes
.NET Version: 4.8.09032
Services: 291

Manufacturer: LENOVO
Model: 82K6
Serial Number: PF3ZX2BJ
Motherboard: LENOVO LNVNB161216
Processor: ▪ 11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz
Total Physical Cores: 8
Memory (Installed): 16 GB
Memory (Usable): 15.8 GB
BIOS Name: H1CN52WW
BIOS Version: H1CN52WW
BIOS Released: 2022-11-15
Display Adapters: ▪ NVIDIA GeForce RTX 3070 Laptop GPU ▪ Intel(R) UHD Graphics
Monitors: ▪ Default Monitor ▪ Generic PnP Monitor ▪ Lenovo DisplayHDR

We will provide unlimited remote Technical Support and onsite support where required for your computers and laptops which are pre-registered in our Asset Management system. We also include any effort required to liaise with 3rd party vendors for any hardware or software issues. If you have a complete system failure or loss of device, we will provide you with a temporary loan device all setup and configured with any software/data you require until your device will be repaired/replaced.

## Cloud Services Management

We will optimize your Azure resources for high availability, security, performance, and cost and manage and support all aspects of your cloud environment. This includes managing the Office 365 backend tenancy and users, hosted email services (Online Exchange), distribution groups, contact aliases and public folders.



Subscriptions: 6 of 25 selected – Don't see a subscription? Open Directory + Subscription settings

- You can customize Advisor to process recommendations for resources that matter to you the most.
- You can delete your unassociated public IP address to reduce your monthly Azure spend.
- You can enable virtual machine backup to protect your data from corruption or accidental deletion.

We also provide support with all the core Office 365 Desktop Apps such as Outlook, OneDrive Word, Excel, PowerPoint, OneNote, SharePoint, Planner and Teams as well as any desktop agents used for syncing data.

Outlook OneDrive Word Excel PowerPoint OneNote SharePoint Microsoft Teams

## Backup & Recovery Management

- ✓ Daily Backup checks
- ✓ Troubleshooting of issues with current Backup routine
- ✓ Changes to existing configuration
- ✓ Test restores from backup images
- ✓ Retrieval of file/s from backup when required
- ✓ Full system bare metal restores
- ✓ Annual Disaster Recovery simulation test

To ensure your systems and data are easily recoverable in the case of an emergency we investigate the success of your backup jobs on a daily basis to ensure they were indeed successful and complete.

We will also keep a check on the inclusions of your backup sets ensuring all critical directories and folders are getting backed up. Unlimited troubleshooting with your backup solution is included in the monthly cost. If a scheduled backup job did not run successfully, we will intervene by fixing the cause and will manually re-run the failed backup job, therefore, minimizing any gaps in your backup sets.

We also conduct backup validations from your backup media to ensure that your data is fully retrievable in the case of a crash or unforeseen event. Furthermore, on an annual basis, we will conduct a Disaster Recovery simulation test by executing the operation we would perform in the event of a full disaster. By demonstrating that this procedure can be performed we aim to provide peace of mind to our customers. The process is fully documented and timed with a comprehensive report being kept up to date for your records.

### Server & Desktop Backup Solution

Our recommended Backup and Recovery solution is Datto® and ArcServe® Backup as the solution has been purpose-built from the ground up for cloud-first data protection. Datto® and ArcServe® Backup is backed by TrueDelta deduplication and compression which provides high performance and reliability while sending less data over the wire. All data is kept indefinitely and therefore servers as an Archive which can go back more than 7 years.

### Complete Office 365 Data Protection

SkyKick's Cloud Backup Suite offers the most complete Office 365 backup solution on the market. There is a misconception that Microsoft retains your company's data forever and you can recover it whenever you like. The SkyKick solution protects the full Exchange mailbox including email, calendars, and contacts and stores that data for up to seven years.

## Mobile device Management

- ✓ Setting up and configuring corporate applications
- ✓ Troubleshooting of issues with receiving/sending email

Included in the program is remote support for setting up and troubleshooting business smartphone or tablet computers with connecting up corporate and Office 365 applications.

### MDM software (Licenses required)

Manage and secure mobile devices to reduce risk with fast, automated setup and maintenance of your mobile fleet.

Features:

- ✓ Security: Configure detailed security settings on business-owned devices.
- ✓ Location tracking: Use the built-in GPS on mobile devices to locate lost or stolen smartphones or tablets.
- ✓ Ownership details: Keep track of devices registered to individuals and associated handset details.
- ✓ Data usage monitoring: Help make sure you don't pay extra data usage fines by setting up RMM monitor data usage on your users' registered devices.
- ✓ Remote features: Lock phones, set passwords, or wipe devices without leaving your RMM console. Additionally, you can remotely configure email and Wi-Fi access on your devices.
- ✓ Multiple device types supported: The mobile device management tools support Apple® iOS®, Google® Android®, and Microsoft® Windows® devices and tablets.

## VoIP Management

- ✓ Add, remove users
- ✓ Troubleshooting of issues with call flows
- ✓ Changes to existing configuration
- ✓ Monthly VoIP Server configuration backups

We will look after your VoIP Solution backend and support your users SIP handsets and Soft Phones.

# Customer Support Team

Supporting your Business 24/7, our exceptional IT Support team takes every measure to go above and beyond and will take that extra step to make you feel that we understand what you are going through.

## Superior Response Times

When you subscribe to our ArmourNet MITS Program you will be experiencing one of the best Response Time SLAs in the industry. You can be reassured that if a critical technical problem strikes, a technical support engineer is immediately available when you need us most. We will support all devices at any location when used for business purposes by staff covered under the agreement.

## Extended Operational Hours

We realise that most organisations have staff starting early or working back late. Our technical services team provides support from 7:30am until 6:30pm Monday till Friday. We also have a rostered-on team member who will be available to provide support for any critical issues after hours and over the weekends (See section on After Hours Support).

## After-Hours Support

Our After-Hours support ensures that your users receive prompt technical assistance for any critical issues after hours. Please note that After-Hours support is only intended for critical issues effecting all users such as an entire site outage or Server not responding.

## Response Times (worst case scenarios)

| | Definition | Response Time |
|---|---|---|
| 1. Critical issues | Technical issues stopping workflow for all staff and no work-around is available | Remote Support within 30 minutes |
| | | Onsite Support within 2 hours |
| 2. Serious issues | Technical issues seriously impacting business operations or workflow of critical individuals have ceased | Remote Support within 1 hour |
| | | Onsite Support within 4 hours |
| 3. Minor issues | Minimal Impact on Business Operations i.e. One or several users have non-critical issues | Remote Support within 1 business day |
| | | Onsite Support within 2 business days |

## Liaison with Other Technical Providers

We will save you the time and frustration of liaising between your technology providers by managing all contact with your vendor or 3rd party providers and get the required assistance for the resolution of any issue, or to make changes to your current settings.

## Program Pricing

| | |
|---|---|
| ArmourNet MITS Program – Service Level Agreement (SLA) | $115 user /month |
| Labour rates for out-of-scope work – Business Hours | $170 / hour |
| Labour rates for out-of-scope work – After-Hours | $190 / hour |
| Onsite travel time for out-of-scope work Business Hours | $50 / hour |
| Onsite travel time for out-of-scope work After Hours | $100 / hour |

License Subscription costs:

| License | Assigned to | Explanation | Price /month |
|---|---|---|---|
| **SaaS Backup (365 / Google)** | End-Users | Exchange, SharePoint, OneDrive & Teams. Google Workspace. | Included with MITS |
| **M365 Business Premium** | End-Users | Recommended value for every business. Covers most of the Microsoft important components. | $30.20 |
| **Server Backup**<br>Conventional | Server | Subscription required per Operating System | $60.00 |
| **Workstation Backup**<br>Conventional | Workstation | Subscription required per Operating System | $18.00 |
| **Server DRaaS**<br>Business Continuity | Server/s, Hypervisors | Completely managed, state of art Business Continuity & DR solution. | Scenario-based |
| **Workstation DRaaS**<br>Business Continuity | Workstation/s | Completely managed, state of art Business Continuity & DR solution. | $35.00 |
| **Defender for Office 365 Plan 2**<br>(Formerly ATP P2)<br>Upgrade Addon | Selected users | For phishing, malware, safe links and attachments attack simulation, advanced administration, and management | $6.90 |
| **Cisco Umbrella DNS Protection** | Workstations, Servers, Gateways | Manage mobile devices, automatically install apps, WIFI settings | $8.20 |

Add-Ons:

| License | Assigned to | Explanation | Price /month |
|---|---|---|---|
| **SECaaS – L1**<br>Addon for MITS | End-Users | Essentials 8 – Maturity Level 1 | Included with MITS |
| **SECaaS – L2**<br>Addon for MITS | End-Users | Essentials 8 – Maturity Level 2 | $35.00 |
| **SECaaS – L3**<br>Addon for MITS | End-Users | Essentials 8 – Maturity Level 3 | $50.00 |
| **Token/Key/Biometric Access** | End-Users | Security Token (*per user / one-off) | $130.00 (*) |

*** All pricing is exclusive of GST*