Principle networks

Service Description

Security Managed Service

Table of Contents

Introduction

This Service Description is provided as a supplement to Principle Networks General Terms and Conditions. Principle Networks may update this Service Description from time to time without notification.

This document describes the managed service, service levels and enhanced options provided by Principle Networks. This Service Description applies specifically to Principle Networks '**Security Managed Service**'.

Our solutions, services and support are certified against the following standards:

Security Managed Service Overview

Principle Networks will offer the following as part of the managed service, enhanced options are available to add-on to the service:

Service	Managed Service	Enhanced Options
Service Management	✓	
Pre-Paid Days Contracts		✓
Ad-Hoc Service Reporting	✓	
Principle Networks Customer Portal Access	✓	
Monitoring Platform Access	✓	
Proactive Monitoring Minor/Alert (8-6)	✓	
Proactive Monitoring Critical/High (24/7) Client updates/app connector	✓	
24/7 Servicedesk	✓	
Access to 3rd Line Engineers	✓	
Hardware Break Fix	✓	
End-of-Life Management	✓	
Patch Management (High/Critical Vulnerabilities)	✓	
Patch Management (Non-High/Non-Critical Vulnerabilities)		✓
Backup / Configuration management – Gold Config, no backup	✓	
Failover Testing (Scheduled Intervals)		✓
Co-Management Arrangements	✓	
Escalation Management	✓	
Maintenance Notifications	✓	
Vulnerability Scanning of Internet Facing Appliances	✓	
External Vulnerability Testing		✓
Business Review (Service Management Review)		✓
Firewall Review		✓
Zscaler Managed Service		✓
Zscaler - Secure Internet & SaaS Access (ZIA)		✓
Zscaler - Secure Private App Access (ZPA)		✓
Zscaler - Digital User Experience (ZDX)		✓
CyberArk Privilege Access Management (PAM)		✓
Arctic Wolf Managed Detection and Response (MDR)		✓

Details of the services offered above can be found throughout this document.

Service Management

Principle Networks operate under an ISO 20000:1 accredited Service Management System with telephone, email, and web portal access to raise Incident and service requests which are managed against the following target service levels.

Offering	Description
Network Managed Service	Principle Networks will respond to Service Requests, Change Requests and reports of Incidents submitted by Customers through its Authorised Contacts.
Coverage Hours	24 x 7 x 365
Incident Response Times	Target Response times for Incidents are dependent on the severity level: • P1 - Critical event will be responded within ≤30 Mins. • P2 - Urgent event will be responded within ≤ 30 Mins. • P3 - Important event will be responded within ≤2 hours. • P4 - A request will be responded within ≤4 hours. ***Please see "Service Levels" section of this document for more detail.***
Target Fix Times	Target Fix times for Incidents are dependent on the severity level: • P1 - Critical event, target fix within ≤4 hour • P2 - Urgent event will be responded within ≤8 hours. • P3 - Important event, target fix within ≤32 hours • P4 - A request will be actioned within ≤48 hours. ***Please see "Service Levels" section of this document for more detail.***
Vendor Support Escalation	Principle Networks will escalate items which the Principle Networks Servicedesk team are unable to resolve.

Contacting the Servicedesk

Principle Networks Managed Network Customers have access to the Principle Networks Servicedesk team. Principle Networks Servicedesk can be contacted as follows:

Contact Method	Details
Email	Servicedesk@principle-networks.com
Portal	https://portal.principle-networks.com
Telephone	03330 124 003 (Option 1)

Priority 1 and Priority 2 incidents should be raised via a telephone call to our 24/7 servicedesk number above.

Any fault or service affecting issue will be dealt with by the Principle Networks Servicedesk. Where subject matter experts input is required, cases will be escalated to the appropriate engineers, 3rd parties or vendors in accordance with prevailing Service Levels. Alternative Service Levels will apply to Change Requests.

Servicedesk Communication

Principle Networks Servicedesk has various methods whereby it communicates to customers. These contacts can be updated via service request or the customer portal by the named '**Authorised - Including Delegation**'. There are three main contacts that our Servicedesk engineers use to contact customers:

- **Servicedesk Contact** - Is usually a Servicedesk / IT Department distribution list or a named contact who will be contacted by Principle Networks in the first instance.
- **Out of Hours Contact** - Can also be an email distribution list or a named contact who Principle Networks will call/email OOH should this be required.
- **Escalation Contact** - This contact will be used if the Servicedesk and/or OOH contact cannot be reached.

Note: Customer contacts who submit tickets via email or through the customer portal will remain the primary case contact. This can be changed by request, or via the customer portal. In a P1/MSO scenario that is proactively raised by Principle Networks both the Servicedesk Contact and the Escalation contact will be contacted.

Servicedesk Permissions

For security access reasons Principle Networks has options to set customer permissions for its contacts. These permissions can be updated via service request or the customer portal by the named '**Authorised - Including Delegation**'.

- **Problem Permissions** – Permissions to Raise Problem Cases or Queries.
- **Change Permissions** – Permissions to Authorise or Make Changes, including Service Requests.
- *Options: '**Authorised**' / '**Not Authorised**' / '**Authorised - Including Delegation**'. The latter being a management contact who can manage permissions of other contacts within their business E.g. Head of IT, Director)*
- **Maintenance Notifications** – Will receive notifications relating to maintenance/service. E.g. Planned works or Critical Vulnerabilities effecting supported products. *Options: Allow / Do Not Allow*

Note: Should a contact not be authorised to make changes or raise problems Principle Networks Servicedesk engineers will notify the contact and will request authorisation from a user with '**Authorised - Including Delegation**' permissions.

IT Service Management

The following ITSM processes are implemented:

- Incident Management
- Request Management
- Change Management
- Problem Management
- Configuration Management Database (CMDB) Management
- Continuous Service Improvement

Incident Management

Principle Networks handle Incident Management with precision, adhering to specific Service Level Agreements (SLAs). Each incident is carefully classified and prioritised. Our Servicedesk team then conducts thorough investigations, diagnoses the issue, and ensures swift resolution with root cause, all in accordance with our ISO 20000:1 service management standards.

P1 and MSO Process

Principle Networks have internal Priority 1 incident and major service outage processes to tackle those incidents that need urgent attention.

Request Management

Customers can make service requests in relation to their Principle Networks managed service. For example, ask question about their service or VPN user creation.

Where a request type is deemed as a chargeable requirement the customers pre-paid days contract can be used for professional services time. Should a request fall out of scope of a pre-paid day's contract then the request will be passed onto the customer's account manager to progress as a project.

There are two case types that Principle Networks use within our IT Service Management (ITSM) System to categorise service requests; these are:

Query – A query can be a question or request for information about a customer's existing service or a service a customer may want to consume. Often queries develop into a change request or a referral to the customer's account manager should any further actions be required such as scoping requirements for a project.

Service Request – Is a formal low risk request for something to be provided. For example, this could be a password reset, or a new VPN user request. These requests a low impact changes that are quick to action which save the use of having to go through the change management process.

Change Management

All changes will be categorised as a change request within with Principle Networks ITSM system and will be sub categorised as Standard or Normal changes. Either change can be assigned a priority level between P1 (Emergency) and P4.

All changes are chargeable with time taken from the customer pre-paid days contract, as described within this document. Changes adhere to Principle Networks' standard Service Levels defined within this document. As standard, all changes are prioritised as P4 and completed in hours as defined in the SLA.

Changes may be completed out of hours at customer request when Principle Networks resource is available. Out of hours change time is taken from a customer pre-paid days contract at double time.

Multiple changes of the above types or those that are estimated to take longer than 4 hours could be seen a larger piece of work. Where this is the case, the request would be directed through to an account manager to produce a scope of works and will be chargeable based on the scope.

Change Request Authorisation

To ensure security and accountability, all change requests must be submitted by an authorised representative from your organisation. This representative must be pre-approved by an "Authorised - Including Delegation" contact, as defined on page 6. Typically, these individuals hold key roles such as IT Director, IT Manager, or an equivalent position. The "Authorised - Including Delegation" contact is responsible for owning and maintaining the list of approved contacts who are permitted to request or approve changes. For added security, Principle Networks securely stores these authorised contact details within our ITSM system, ensuring that only verified personnel can initiate or authorise change requests.

Standard Change Request

Standard Changes have been defined as a '**Business as Usual**' task and do not follow the full normal change management process. All standard changed requests will be give the P4 SLA.

A Standard Change request is categorised as a low risk / low impact change which is usually commonly requested and frequently implemented. They follow company work processes where appropriate and have a proven history of success.

Types of changes covered by a standard change (Subject to complexity):

- System reboot
- Minor software and OS patching
- Security Policy additions
- Traffic Routing (Minor)
- Port and or VLAN Configuration
- Port Channel
- Existing VPN Configuration
- Firmware Upgrade

Normal Change Request

Normal change requests are considered those that do not fall into either a standard change category. The impact is often moderate to very high and holds a medium to very high risk. Formal procedures must be followed to ensure that each step of a normal change request case is completed in line with this process.

Every normal change must undergo a detailed review of the customers requirement which comprises of:

- Change Reason and Justification
- Change Details and Associated Equipment
- Post Change Test Details
- Impact Analysis, Highlighted Risks and Mitigation
- Rollback Details

Emergency Change Request

The emergency change process is in place to work around or resolve high impact and high-risk incidents that are causing substantial business disruption. An Emergency Change could also be utilised to protect the customer's business from threats such as are likely to result in an incident if not addressed promptly, for example a critical security vulnerability that could result in a cyber-attack. Emergency changes follow the incident management P1 process and maintain the standard case type of '**Change Request**'.

Problem Management

Principle Networks follows a robust and structured Problem Management process designed to identify, investigate, and resolve the root causes of recurring or major incidents. This process ensures minimal disruption to services and supports continuous improvement in line with best practices. Our approach aligns with the Problem Management guidelines audited and certified under ISO/IEC 20000-1, ensuring compliance with international standards for IT Service Management. Through proactive and reactive problem management, we deliver consistent, high-quality outcomes for our clients.

Configuration Management Database

The Configuration Management database (CMDB) underpins all ITSM services and provides the data required for effective Incident, Request, Change and Problem Management. Principle Networks CMDB holds information about all supported assets and services such as servers, routers and switches and holds key pieces of information about them such as device name, site locations, management IP address information, product types, serial numbers, and software version.

Continuous Service Improvement (CSI)

At Principle Networks, we are committed to continually enhancing and evolving our services. We actively collaborate with our customers, encouraging feedback on our performance and identifying opportunities where we can add greater value and make meaningful improvements.

We encourage feedback after closure of every service case and all feedback is reviewed. Feedback can be about the service, a service feature request or feedback to an individual Servicedesk engineer. Improvement suggestions and feature requests will be added to Principle Networks continuous service improvement (CSI) register and will be reviewed regularly. Strategic focus for service operations is defined by what can be achieved through our continuous service improvement program.

Pre-Paid Days Contracts

Except for patching for high or critical vulnerabilities, Principle Networks does not include any other changes within the standard service. For other changes, we offer pre-paid day contracts as a flexible solution, allowing customers to incorporate change requests into their Managed Service contract. This can be arranged as part of a monthly allowance or purchased on an ad-hoc basis, depending on the customer's preference.

Pre-paid days contracts may only be utilised for change and works in relation to services Principle Networks support, unless explicitly agreed. They may not be utilised for break fix or high priority problems and faults and are handled through the Managed Service for supported solutions.

Time is recorded for all work is in increments of 30 minutes, thus this is the minimum amount of time per change. Anything that is estimated to take over 4 hours or more may be classed within a project scope and will need the appropriate resource assigned to fulfil the requirement and may require a full scope of works and/or project management and may be charged against a separate quote signed by the customer.

Customers have the option to purchase monthly hours that can be used for ongoing service and change. Monthly hours top the customer's recurring hours back to the contracted value of the 1st of each calendar month. Hours not used within the calendar month are lost.

Additionally, there is the flexibility to buy a bank of non-recurring hours, which serve as a reserve that can be utilized as needed. This system provides a convenient way to manage time allocation for services, allowing customers to plan and budget their support needs effectively.

If more time is used in a month than what is contracted, the excess time will be deducted from the non-contracted 'bucket'. If there is no time available in the non-contracted bucket, overuse will result in a negative balance. Any underuse in subsequent months will then reduce this negative balance until it is eliminated. If overuse continues to accumulate, your account manager will reach out to discuss increasing the contracted amount or potentially introducing a hard limit to prevent further overuse of Change time and avoid additional charges.

A monthly report is available to customers to detail hours used and highlight the remaining pre-paid days allowance. This can be enabled by the customer through the Principle Networks Portal or by raising a service request with servicedesk@principle-networks.com.

Note: Pre-paid day time is billed at double the standard rate for out-of-hours (OOH) services. If hours extend into arrears, customers may be required to either pay for the additional time used over the agreed contract or modify their existing agreement to accommodate the increased use of the service. This revision aims to clarify the billing practices for pre-paid time and the options available to customers should they exceed their allocated hours.

Ad-Hoc Service Reporting

High-Level Ad-Hoc Reporting Upon Request (Service Request): Customers can request service reports, including availability, incident counts, and SLA adherence, through a service request. The service management team will generate these reports tailored to the customer's specific needs.

Please note that this service may incur charges, which will be deducted from the customer's pre-paid days contracts. For comprehensive service management solutions, Principle Networks provides a dedicated service. For more information, customers are encouraged to reach out to their respective account manager**.**

Monitoring Platform

Customers can request Read-Only access to the Principle Networks monitoring platform. If you wish to obtain access, please send an email to servicedesk@principle-networks.com. Ensure that you are a designated change authority for your company or have an authorised contact within your company submit the request on your behalf.

Customer Portal

Customers are invited to request access to the Principle Networks customer portal. This portal allows you to track your support tickets, view contracts, and update company contacts. To gain access, please email servicedesk@principle-networks.com. You must be a designated change authority for your organisation, or alternatively, an authorised contact within your company can request access on your behalf.

An existing portal user from your organisation with admin rights can also provide you with portal access by assigning your portal role from the User Management page.

Proactive/Reactive Monitoring of Solution and Services

- Proactive Monitoring for Critical/High Alerts - Available 24/7
- Proactive Monitoring for Minor/Trouble Alerts - Operational from 8 AM to 6 PM

Principle Network's monitoring platform diligently tracks hardware availability around the clock, every day of the year. Customers may request access to this platform to examine historical availability data and other pertinent metrics.

Our monitoring platform goes beyond traditional network managed service capabilities, providing advanced intelligence and proactive oversight to ensure optimal performance. Endpoint monitoring is conducted through protocols such as SNMP, WMI, API, and ICMP, it includes comprehensive hardware health monitoring, continuously assessing critical components such as CPU, memory, disk usage, and even power supplies for potential issues. The platform also utilises AI-driven learning to establish baselines of normal behaviour, enabling it to detect and respond to uncharacteristic patterns or anomalies proactively. When issues are identified an automatic fault is generated and escalated to the Principle Networks Service Desk for resolution. This proactive and intelligent approach ensures issues are addressed promptly, in line with the agreed Service Level Agreement (SLA), minimising downtime and enhancing overall reliability.

Please note that Principle Networks offers reactive support only on Wi-Fi access points, meaning proactive monitoring for these devices is not provided.

24x7 Service Operation

Managed customers benefit from 24/7 Servicedesk access, ensuring they receive prompt assistance for high-priority incidents or emergency changes. It is important to note that customers need to initiate a phone call to request this level of support. For detailed definitions of each priority level, customers should refer to the Service Level Agreements (SLAs) provided in the appendix of the document. This structure helps maintain an efficient and responsive support system.

Note: Principle Networks collaborate and support your organisation's IT and servicedesk teams, so 1st and 2nd line support for end users within your organisation is still a requirement

Access to 3rd line engineers

Principle Networks ensures that their managed customers have direct access to 3rd line engineers. To delve into what this means:

- Expertise - When you encounter complex technical challenges, our senior engineers bring a wealth of knowledge, skills, and experience to the table. Our engineers swiftly analyse issues, propose solutions, and guide your team effectively.
- Speed - The service operations are automated and technology-driven, ensuring efficiency and saving valuable time. When critical incidents arise, our engineers respond promptly, minimising downtime.
- Quality - Principle Networks adheres to best practice service management standards. Our 3rd line engineers maintain consistency, ensuring high-quality support and governance.
- Assurance - With industry-leading Service Level Agreements (SLAs) and proactive support, you can trust that any network issues will be resolved rapidly, minimising impact on your operations.

Principle Networks' 3rd line engineers play a crucial role in maintaining reliable, secure, and high-performing networks.

Hardware Break Fix

Principle Networks ensures that all hardware is protected under a warranty for replacement or repair, with certain exceptions. This warranty service is coordinated by Principle Networks and executed by external partners who are experts in the field and have global access to necessary replacement parts. The warranty period commences from the initial delivery date to the customer's location.

Efforts will be made to repair any defective hardware or components; however, the standard procedure under the hardware warranty is to provide a replacement. Customers can opt for either a 4-hour onsite response or a next-business-day response, either supported by on-site engineers and remote specialists based on the service ordered.

Exceptions may apply to customer-owned equipment, particularly when Principle Networks assumes responsibility for pre-existing network infrastructures, or as part of a longer-term migration.

End-of-Life Management

Principle Networks provides proactive monitoring of End-of-Life (EoL) hardware within the network and is a crucial practice that involves keeping track of the lifecycle status of this equipment for supported vendors. Supported vendors are those that provide API access to the information. Principle Networks monitor the EoL timeline against end of software updates, security patches, and technical support and flag supported equipment approaching these key milestones. The key benefits this brings to customers is that it maintains a secure, efficient, and compliant network by ensuring timely updates and replacements of out of support equipment. It is a forward-looking and strategic approach that minimises risks associated with outdated technology that can save time, resources, and money overall.

Due to End-of-Life status or changing requirements of the customer, appliance upgrades may from time to time be necessary and will be proactively communicated by an account manager. Any such upgrades will attract the appropriate charges from Principle Networks.

Patch Management (High/Critical Vulnerabilities)

Principle Networks' Servicedesk team is responsible for applying patches to appliance operating systems exposed to a critical or high-risk vulnerability. This task is performed proactively for supported vendors in accordance with our change management procedures during standard working hours. Out of hours patching can also be arranged without charge. We aim to complete these updates within 14 days of notification from the vendor in question.

Our proactive approach to patch management ensures the ongoing security and stability of your network infrastructure. We are dedicated to protecting all managed devices from potential threats.

A patch is considered critical or High risk solely by Principle Networks based on whether the vulnerability impacts the service's functionality or security.

Patch Management (Non-High/Non-Critical Vulnerabilities)

For patches deemed non-critical or not high-risk, the standard change management process applies, and these will be accounted for against a customer's pre-paid days contract.

Backup / Configuration management

Regular backups are taken on all managed devices against a 24-hour Recovery Point Objective (RPO). Backups are securely stored, either within Public or Private cloud and follow industry best practices for security. These backups can be called upon within the solution specific Recovery Time Objective (RTO) in the event they are required.

For configuration backups, application features such as configuration difference comparisons can be used to checked for changes within a troubleshooting scenario, or they can be called upon for compliance purposes should this be necessary.

Certificate Management

We take a proactive approach to certificate management. Our robust system monitors certificate expiration dates diligently. As soon as a certificate approaches 30 days of its expiry date, our ITSM will automatically raise a Change Request. We promptly notify our managed services customers, ensuring they have ample time to renew certificates before any potential service disruptions occur. With our expert's support to help replace expiring certificates and ensuring the network remains secure and operational.

Certificate Management is limited to certain device types. We regularly add support for new device types and may add support for additional device types upon request.

Co-Management Arrangements

Principle Networks provide customers with a tiered co-management access (vendor supporting), this can be restricted to a level to allow customers to undertake minor changes or complex changes depending on their requirements and experience. As part of co-management customers are free to manage their own internal change process or are welcome to use principle networks to peer review or as an escalation point for changes where appropriate. We expect customers to have access to their own hardware equipment or environments (Microsoft Azure, Zscaler, Microsoft Security or Meraki Dashboards for example).

It is the customers responsibility to ensure any changes they make have been verified and tested prior to implementation to ensure no unanticipated downtime to their network services. We strongly recommend customers utilise their own UAT plans (user acceptance testing) after each change. Should any support on changes be required it is advised that customers log the change request to the principle networks Servicedesk for the team to verify and support the change.

Escalation and Management

Any service partner or hardware vendor escalations will be managed by Principle Networks as an integral part of our service. Our commitment extends to ensuring seamless communication and resolution with external partners.

Comprehensive vendor support applies only to Principle Networks managed services. In cases where a service is unmanaged, the responsibility for escalations lies solely with the customer**.**

Principle Networks Escalation

For customers wanting to escalate a part of their Principle Networks service the process can be found in the appendix of this document.

Maintenance Notifications

Principle Networks work with several service partners who from time to time perform planned maintenance to continuously improve the stability of their products and services. Using downtime schedules Principle Networks ensure that any notification of planned works that they receive that is service affecting will be added to a downtime schedule and a calendar invite will be sent to the selected maintenance contacts to ensure the customers are kept informed of all planned works.

Customers can request maintenance notifications by emailing the servicedesk@principle-networks.com and raising a service request. Notifications can also be stopped using the same method.

Customer Maintenance

It is the customers responsibility to notify in advance any planned work taking place that will affect the managed service solution supported by Principle Networks. A downtime schedule will be created for the date/time of the work and a description will be added including the case number to ensure all parties are aware.

The downtime schedules ensure that alarms are suppressed for the duration of planned work. Once the end date and time has lapsed alarm suppression is lifted automatically and normal service monitoring of the solution is resumed.

False alarms resulting in a pro-active response to the issue by Principle Networks caused by customer maintenance not communicated in advance may be deemed chargeable or recorded against the customer's prepaid days contract.

Vulnerability Scans of Internet Facing Appliances

Principle Networks conducts regular Vulnerability Scans on all network-managed internet facing appliances to ensure that common ports are not left open, either by vulnerabilities or administrative error. By identifying and addressing potential vulnerabilities, we proactively enhance the security posture of our customer environments, safeguarding against threats and unauthorised access.

Enhanced Security Managed Service Overview

Failover Testing (Scheduled Intervals)

As part of the Principle Networks solution acceptance testing, we test failover to all components that have been designed to as per the scope of works from project delivery. The Principle Networks Failover Testing service is designed to proactively assess and enhance the resilience of your network infrastructure to provide peace of mind once the solution is live and BAU. By conducting regular, systematic tests at predetermined intervals, Principle Networks ensure that Network can effectively handle unexpected disruptions, maintaining operational continuity and minimising downtime.

Key Features include, but not limited to:

Regular Testing Schedule - We establish a fixed schedule for failover tests, ensuring consistent evaluation of your network's performance and reliability. This proactive approach helps identify potential vulnerabilities before they impact your operations.

Comprehensive Testing Scenarios - The service includes a variety of testing scenarios, such as:

- **Hardware Failures**: Simulating the failure of critical components to validate backup systems.
- **Network Outages**: Assessing the effectiveness of backup connections during complete network failures.
- **Software Failures**: Evaluating recovery processes from software crashes or bugs (If applicable).

Adaptability to Change - We understand that over time, changes in your network environment may not be factored into existing failover scenarios. By regularly conducting these tests, we can identify potential problems before they arise, ensuring your systems are prepared for any failover event.

Reporting and Analysis - After each scheduled test, we can provide a summary report detailing findings, performance metrics (if applicable), and actionable recommendations for enhancing your failover strategies.

Benefits:

- **Increased Reliability:** Ensure your systems are prepared for unexpected disruptions, enhancing overall service continuity.
- **Proactive Risk Management:** Identify and address potential issues before they escalate into significant problems.
- **Compliance:** Ensuring that a failover technical test has been conducted as part of a holistic DR testing plan.
- **Peace of Mind:** Trust that your network is equipped to handle failures efficiently, allowing you to focus on your core business activities.

With our Failover Testing service, you can confidently safeguard your network against disruptions. Let Principle Networks help you fortify your infrastructure and ensure uninterrupted service.

Note: What is the difference between a failover and DR test? A Failover test is a technical test of system redundancy and immediate availability. A DR test is a holistic approach encompassing recovery of infrastructure, applications, and business operations after a major disruption.

In short, failover testing is typically a subset of the larger disaster recovery testing process.

External Vulnerability Testing

External vulnerability testing is a key component of maintaining a secure IT environment. Here is a more detailed explanation of the process and its benefits:

Vulnerability testing, also known as vulnerability assessment, is the process of identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures. It provides organizations with the necessary information to understand and mitigate risks associated with these vulnerabilities.

Detailed Reports - After conducting vulnerability tests, detailed reports are generated. These reports typically include:

- **Risk Levels** - Each vulnerability is categorized by its risk level, from critical to low.
- **Vulnerability Details** - Information about the nature of each vulnerability, how it can be exploited, and the potential impact.
- **Remediation Steps** - Recommended actions to fix or mitigate the vulnerabilities.
- **Compliance Status** - Assessment of how the vulnerabilities affect compliance with relevant regulations and standards.

Benefits of Regular Testing:

- **Proactive Security** - Regular testing helps in identifying vulnerabilities before attackers can exploit them.
- **Risk Management** - By understanding the risk levels, organizations can prioritize their response efforts effectively.
- **Compliance Assurance** - Regular assessments ensure that systems remain compliant with industry standards and regulations.
- **Trust and Reliability** - It builds trust with customers and partners by demonstrating a commitment to security.

External vulnerability testing provides detailed reporting and is essential for any organization looking to secure its IT services and protect against emerging threats. It is a proactive measure that not only enhances security but also supports compliance and operational reliability.

Zscaler Managed Service

In today's digital age, cyber security is crucial for protecting your business. Small and medium-sized enterprises (SMEs) often face challenges in keeping up with the evolving landscape of cyber threats. At Principle Networks, we provide a fully managed Zscaler service designed to meet the specific needs of SMEs. We handle the deployment, management, operation, and support of Zscaler's state-of-the-art cyber security solutions — keeping your organisation always protected and resilient.

Supporting a Secure Hybrid Workforce

Enabling a hybrid workforce requires flexible solutions that support employees and third parties wherever they work, using any device. Our Zscaler managed service ensures a fast, secure, and reliable user experience when accessing applications and data. Unlike traditional solutions, Zscaler's modern approach scales with your business and prioritises data protection at every step.

Simplified Security Through Our Zscaler Managed Service

We eliminate the complexity of managing multiple security products by offering a comprehensive cloud-based Zscaler platform. Our managed service reduces operational overhead, allowing you to focus on running your business while we manage your cyber security needs.

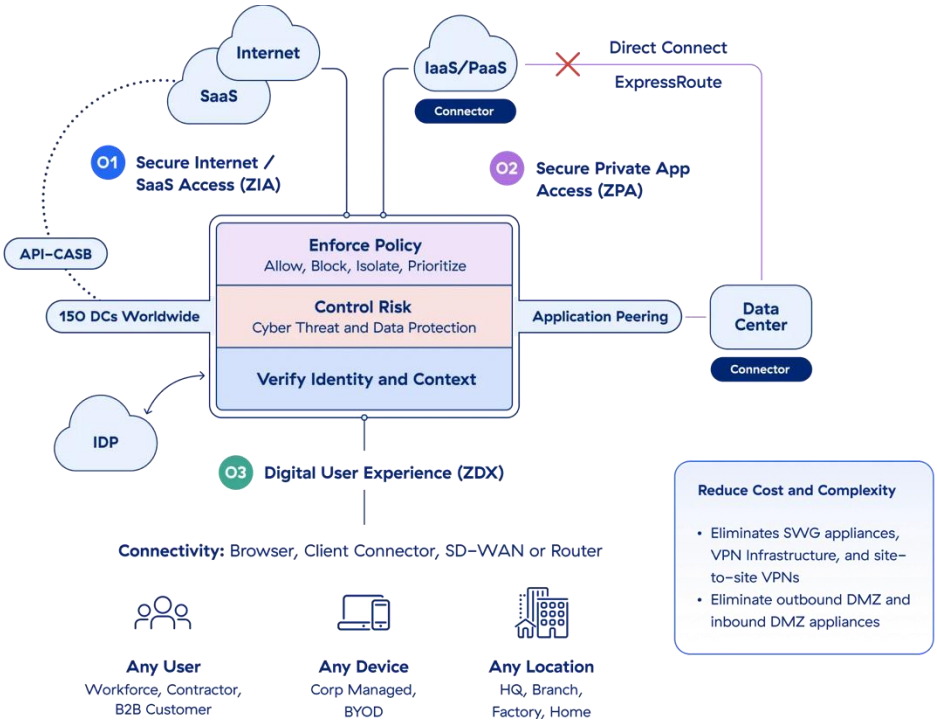
Key Benefits of Our Zscaler Managed Service:

- **Cyber Threat Protection** - A holistic approach to securing users, workloads, and devices against evolving cyber threats.
- **Data Protection** - Complete data security through full TLS/SSL inspection at scale within the Zscaler Secure Service Edge (SSE) platform.
- **Zero Trust Connectivity** (ZTNA) - Secure access to applications — not networks — preventing lateral movement and ensuring a Zero Trust security model.
- **Digital Experience Management** - Continuous monitoring to identify and resolve performance issues, ensuring seamless user experience and productivity.

With Principle Network's Zscaler managed service, you gain peace of mind knowing that your business is protected by experts who manage and maintain your security infrastructure. Stay secure, resilient, and focused on your core business while we handle your cyber security needs.

Zscaler for Users

Zscaler for Users comprises three areas of functionality to improve security, data protection, and digital experiences, all powered by the Zscaler Zero Trust Exchange.



Deployment

The service begins with a comprehensive deployment process. At Principle Networks, we understand that every company is unique, so we take the time to fully understand your specific requirements. Our experts carry out a detailed analysis of your existing infrastructure and workflows to identify your company's needs. Using this insight, we configure and implement the cyber security solution seamlessly, ensuring it integrates smoothly with your systems and operations. Our goal is to deliver a deployment that minimises disruption while maximising protection and efficiency.

Secure Internet & SaaS Access (ZIA)

Provide users with fast, secure, and reliable internet and SaaS access while protecting against advanced threats and data loss.

- **Secure web gateway** - Control and protect web traffic from sophisticated threats; includes full TLS/SSL inspection.
- **Cloud firewall & IPS** - Secure all traffic on every device with superior access control and vulnerability protection.
- **Sandbox** - Stop emerging threats with AI-powered malware prevention and inline quarantine.
- **Data loss prevention** - Control and protect web traffic from sophisticated threats; includes full TLS/SSL inspection.
- **Cloud access security broker** - Protect data-at-rest and ensure compliance across SaaS applications.
- **Browser isolation** - Isolate users from suspicious web content without disrupting business workflows.

Secure Private App Access (ZPA)

Connect users seamlessly and securely to private apps, services, and OT devices with the industry's only next-gen zero trust network access (ZTNA) platform.

- **Private cloud and data centre** - Deliver secure access to private apps from anywhere with direct connectivity.
- **Public cloud** - Gain secure zero trust remote access to internal applications running on AWS and Azure.
- **Adversary engagement** - Lure, detect, and analyse attackers with proactive decoy apps that generate high-confidence alerts.

Digital User Experience (ZDX)

Monitor digital experiences from the end user's perspective to optimize performance and rapidly fix application, network, and device issues.

- **Hybrid workforce experience monitoring** - Detect issues that impact user experience, reduce mean time to resolution, and keep employee's productive no matter where they are.
- **UCaaS monitoring** - Ensure optimal experiences with an integrated view of application, network, and device health as well as the audio, video, and sharing quality of Microsoft Teams and Zoom calls.
- **ZTNA (Zero Trust Network Architectures) Visibility** - Regain end-to-end visibility to operate effectively, optimize performance, and rapidly fix issues impacting end user experience and productivity.

CyberArk Privilege Access Management (PAM)

At Principle Networks, we provide CyberArk Privileged Access Management (PAM) as part of our commitment to securing your organisation's most sensitive assets. Privileged accounts — such as administrator, service, and root accounts — are prime targets for cyber attackers due to their elevated access levels. Our managed CyberArk PAM service ensures these accounts are secured, monitored, and controlled, protecting your business from potential breaches and misuse.

Key Benefits of Our CyberArk PAM Service:

- **Credential Vaulting:** We securely store and automatically rotate privileged credentials to prevent unauthorised access.
- **Session Management:** Real-time monitoring and recording of privileged sessions for accountability and swift detection of suspicious activity.
- **Least Privilege Enforcement:** We ensure users only have the access necessary to perform their tasks, reducing the risk of privilege misuse.
- **Threat Detection and Response:** Advanced analytics identify and respond to potential threats in real time, keeping your environment secure.
- **Compliance and Reporting:** Comprehensive audit trails and reports help you meet regulatory standards and enhance security governance.

Our managed CyberArk PAM service allows you to focus on your core business while we ensure that your privileged access remains secure, compliant, and resilient against evolving cyber threats.

Arctic Wolf Managed Detection and Response (MDR)

At Principle Networks, we partner with Arctic Wolf Managed Detection and Response (MDR) services to help protect your organisation from advanced cyber threats. With the increasing sophistication of cyber-attacks, it is essential to have a proactive approach to detecting and responding to security incidents. Our Arctic Wolf MDR service delivers continuous monitoring, threat detection, and rapid response, ensuring your business remains secure and resilient.

Key Benefits of Our Arctic Wolf MDR Service:

- **24/7 Monitoring and Threat Detection:** Continuous monitoring of your systems to identify and respond to potential threats in real time.
- **Expert Analysis and Response:** Security experts investigate threats, provide actionable insights, and guide your team through swift incident response.
- **Advanced Threat Intelligence:** Utilises up-to-date threat intelligence to identify and stop emerging threats before they cause harm.
- **Security Operations Support:** Access to an experienced Security Operations Centre (SOC) team that enhances your internal capabilities.
- **Comprehensive Reporting:** Detailed reports and insights to help you understand your security posture and meet compliance requirements.
- **Escalation –** Principle Networks escalation processes.
- **Account Reviews –** Where principle Networks can be invited, on customer request.

Our Arctic Wolf MDR service allows you to focus on your business operations while we handle the complexities of threat detection and response, providing the protection and expertise needed to stay ahead of evolving cyber threats.

Business Review

Business Reviews comprises of a Service Management Review, Security Review, Technology Review, and a Business Update and can be added to the service, typically on a quarterly basis.

During the Business Review, we present a PowerPoint Presentation prepared during the initial phase. The appropriate parties (Service Manager, Solutions Architect, Account Manager, etc.) leads the discussion, with the final stage facilitated by the Account Manager.

Service Management Review

- The Service Manager provides an in-depth analysis of service levels, cases, and overall performance.
- We discuss how well Principle Networks met Service Level Agreement (SLA) Key Performance Indicators (KPIs).
- Challenges related to service delivery within the customer's business context are addressed.

Security Review

- This section focuses on security services purchased through Principle Networks (e.g., external penetration testing, Zscaler, Umbrella).
- We review findings since the last Business Review, including documented security events and attacks.
- High-risk events or security cases are discussed.
- Both the Service Manager and Cyber Security Consultant (or Solution Architect) contribute to this section.

Technology Review

- The Solution Architect or Subject Matter Expert (SME) leads the Technology Review.
- Opportunities for new solutions, licensing, and existing technology deployments are highlighted.
- Customer interests and follow-up actions are recorded.

Business Update

- The Account Manager manages the final stage of the Business Review.
- We invite the customer to discuss their business plans, key strategic objectives, and any relevant changes or developments so Principle Networks can better align our service to support the customer.

Overall, the business review meeting is designed to ensure that all aspects of the company's operations are aligned with strategic goals, risks are managed effectively, and opportunities for growth and improvement are identified and acted upon.

For more information or to schedule a Business Review, please feel free to reach out to us. We value our partnership and look forward to continued collaboration!

Firewall Review

Principle networks offers a comprehensive Firewall Review the process involves the following steps and is not limited to (Example based around a Fortigate Firewall):

Current Firmware Assessment

- Our team begins by assessing the current firmware version of your firewall.
- We gather information about the existing setup, including hardware specifications.

Upgrade Options Evaluation

- We explore upgrade options available for your firewall.
- This includes researching the latest firmware releases and compatibility with your specific hardware model.

Release Notes Examination

- Our experts meticulously review the release notes provided by the firewall vendor.
- We pay attention to new features, bug fixes, and security enhancements.

Special Notices and Known Issues

- We identify any special notices or known issues associated with the proposed firmware upgrade.
- Transparency is crucial—we communicate any potential impact on your network.

Hardware Support Assessment

- As part of the process, we evaluate hardware support.
- If any components require replacement or if technical assistance is needed (TAC), we address it proactively.

Additional Security Features

- Review of current licensing and features.
- Assess security enhancements based on unutilised capabilities.
- Technical guidance of implementation of features.

Risk Identification

- We assess the risks associated with the upgrade.
- Factors such as downtime, compatibility, and potential disruptions are considered.

Pre-Upgrade Checks

- Before proceeding, we perform thorough pre-upgrade checks.
- This ensures that the network environment is ready for the firmware update.

Upgrade Execution

- Our team executes the firmware upgrade following best practices.
- We minimize downtime and closely monitor the process.

Post-Upgrade Validation

- After the upgrade, we validate the firewall's functionality.
- We ensure that all services are operational, and security settings remain intact.

User Acceptance Testing (UAT)

- We collaborate with your team to create a UAT test plan.
- This involves testing critical functionalities and verifying that the firewall meets your requirements.

Documentation and Communication

- We document the entire process, including upgrade details and any adjustments made.
- Clear communication ensures that your team is informed about the changes.

At Principle Networks, we prioritize security, reliability, and seamless transitions. If you have any questions or need further assistance, feel free to reach out.

Appendix

Minimum Data Set (Incident Ticket)

It is the responsibility of the customer to provide as much information about an incident as possible to enable Principle Networks to respond efficiently and resolve the issue as quickly as possible. Here is a guide to help provide a minimum set of information to the Servicedesk upon logging a case.

- Date and time problem occurred:
- Detailed Description of the fault/change request:
- Asset(s) affected if known:
- Any recent changes made:
- What is the impact to the customers business (often dictates the priority):
    - No. Sites affected:
    - No. Users Affected:
- Has the kit been power cycled (if applicable):
- What is the hardware (Router/NTE etc) light status (if applicable):
- Site contact and access times:
- Specific error messages (if applicable):
- Screenshots attached? Yes/No:
- Troubleshooting steps tried to resolve the issue:

Service Levels (SLAs)

Principle Networks Managed Services are monitored 24 x 7 x 365. Within contracted support hours, Principle Networks will respond to autogenerated cases raised by the monitoring systems or to cases raised by the customer within the Service Level Agreement terms.

See the below the description of Service Level against the target response and resolve times:

Priority	Description
P1	A Critical business service is non-operational impacting the customer organisation, multiple users, or multiple sites; or Severe functional error or degradation of service affecting production, demanding immediate attention. **Business risk is high, with immediate financial, legal, or reputational impact.**
P2	The client is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the client or service has been affected, although a workaround may exist; or Application functionality is lost; or significant number of users or major site is affected. **Business risk is high.**
P3	The client is experiencing a problem that causes moderate to low business impact. The impact is limited to a small number of users; or incident has moderate, not widespread impact; or the customer or service may not have been affected. **Business risk is low.**
P4	Standard service request; Change request; Enquiry; or updating documentation; system patch or upgrade. **Low or Minor localised impact.**

The following table describes the target response and fix times for the levels of service for incidents raised.

Priority	Target Response Time	Target fix time *	Working time
P1	30 minutes	2 hours – resilient solution 4 hours – hardware replacement 5 hours – leased-line connectivity	24 hours, 7 days a week, 365 days a year
P2	30 minutes	8 hours	24 hours, 7 days a week, 365 days a year
P3	120 minutes	32 hours	Monday – Friday 8am – 5:30pm
P4	240 minutes	48 hours	Monday – Friday 8am – 5:30pm

***Target fix times may be limited by 3rd party providers and their associated SLA, which may hinder Principle Networks ability to fully restore service.**

Fault Resolution

The Fault Resolution measures apply to Incidents which represent a Service Failure. The duration of a Service Failure and related target maximum Resolution Time is measured, during Contracted Hours, from the point at which the Customer or Principle Networks register the fault within Principle Network's IT Service Management (ITSM) to the point at which Service Failure is no longer present.

Fault Response and Resolution

Principle Networks shall endeavour to respond to and resolve Service Failures within the Response Times and the Target Resolution Times stated above. If it is identified during fault investigation that due to circumstances beyond Principle Networks control, restoration times will exceed the stated target Resolution Times, the Customer will be notified. Principle Networks shall not be liable to the Customer should the Response Times and Target Resolution Times not be met.

Escalations Process

Please raise your escalation by emailing directly to the intended recipient and cc any relevant parties. All previous correspondence should be included. Also please note that when the next escalation has more than one contact, all parties should be included.

Our escalations contacts can also be reached by phone call. If the contact is unavailable, please leave a message and wait for their reply. In the absence of any contacts listed, please be directed to the secondary contact stated in their out of office message.

Should you not receive an acknowledgement to your escalation within the stated timeframe, please escalate to the next level.

A service case priority level is agreed between the customer and Principle Networks when the initial call is raised. The priority level of a given case may be increased by the customer due to a change in circumstances or the amount of time elapsed during the support process. Should a customer feel a case is not being handled as expected the following escalation paths can be followed and available 24/7, also known as a hierarchical escalation:

Escalation Level	Contact	Telephone	Email
Level 1	Servicedesk Lead	07399 329 504	adnan.fatah@principle-networks.com
Level 2	Head of Service Operations	07572 160 006	richard.tm@principle-networks.com
Level 3	Co-Chief Executive Officer	07738 022 937	alex.steer@principle-networks.com

Complaints Process

Principle networks takes great pride on delivering an exceptional service to its customers. Should a customer feel that Principle Networks high standards have fallen short of their expectation the customer should contact the head of service operations by email at:

richard.tm@principle-networks.com

Upon receipt of correspondence from the customer, Principle Networks will respond to the customers complaint within (5) business days.

Principle networks

Technology Delivered Better

03330 124 003
enquiries@principle-networks.com
www.principle-networks.com