lanmark

Guide to Lanmark Cloud Support for Microsoft Azure

Service Details

Service overview

Many businesses want to leverage the power of Microsoft® Azure® without having to incur the challenge and expense of managing it themselves. Some businesses lack the technical expertise or capacity to operate cloud infrastructure, tools and applications. Others may have the ability, but choose to maintain focus on their core business. Many larger businesses are on a multi-phase journey to the cloud, requiring transition and management services that can adapt to an evolving set of needs.

Lanmark Cloud Support for Microsoft Azure is the answer for businesses facing these challenges. As an Azure Expert Managed Services Partner, Lanmark provides customised cloud service offerings to meet specific needs. These offerings provide the flexibility to change or grow your cloud services as your Azure needs change and to increase value by delivering essential services and support. This includes architecture help, access to experts you need to solve your problems, security assistance, 24x7x365 management, cost governance and many other value-added services – all backed by Azure-certified engineers and architects.

Service level management

Lanmark Cloud Support for Microsoft Azure addresses the core challenges that businesses face in implementing and operating Azure environments. We offer our customers two service levels: Care+ and CloudHealth.

Care+:

Care+ provides tooling and access to human expertise, incorporating best practices and 24x7x365 operational support for your Azure environment. Care+ is for customers who need more of a comprehensive support experience, including guest virtual machine management. We will perform environment build and deployment activities in addition to ongoing management of IaaS VM assets (monitoring, patching and antivirus). To receive Care+ support, resources must be deployed via the Azure Resource Manager (ARM).

CloudHealth:

The CloudHealth service level is designed for customers who want to retain a hands-on capability for the configuration and management of their Azure environment, while relying on Lanmark as a trusted advisor with 24x7x365 availability. CloudHealth is only available for Cloud Solution Provider (CSP) customers.

At this level, customers will have access to people and resources relating to architecture and best practices guidance, standardised deployment templates, Azure service health notifications, and the Lanmark Customer Portal. In addition, Lanmark will serve as an escalation point for issues relating to the Azure platform and services.

Multiple subscriptions and service levels

SLA offerings are applied at the subscription level. A customer can have multiple Azure subscriptions with a mix of Care+ and CloudHealth service levels for their account.

Combining service offers

The Care+ and CloudHealth service offering can be uniquely applied for individual Azure subscriptions. This allows you to choose to have our Lanmark Cloud Support Teams 24x7x365 standing watch over your mission-critical production workloads while avoiding unnecessary costs with development and test environments.

Services	CloudHealth	Care+
Access to Lanmark Opinionated Azure Resource Manager (ARM) Templates • Ability to deploy opinionated resource templates employing Lanmark best practices	Access to self-service templates	Assisted deployment from Lanmark infrastructure template repository; access to self-service templates
Azure Monitoring • Automated alert generation from predefined monitors • Integration with Lanmark incident management systems	Notification of Azure-wide outages and service degradation	Leverage Azure and Lanmark monitoring systems for standard events; up to five custom monitors
Lanmark Cloud Support for Microsoft Azure Control Panel • Access to the Lanmark Cloud Support for Microsoft Azure customer portal	✔	✔
Architecture Guidance • Based on Microsoft and Lanmark practices from certified Azure architects • Scheduled scoping calls	Limited best-practice guidance	Lanmark will customise architecture to your specific application
Technical Onboarding Manager (TOM) Personal contact to assist with onboarding	Initial guidance only	Lanmark coordinates the process of getting your workloads up and running on Azure
Configuration Assistance • 24x7x365 access to a Lanmark team that's experienced in Azure and will assist with configuration changes	Consultation provided upon request	Lanmark will customise architecture to your specific application
Service Delivery Manager (SDM) • Personal contact for ongoing business and technical assistance	✔	✔
Service Management • Tracking and management of requests for information/change, incident and service management via the Lanmark ticketing system	✔	✔
Escalation Support • Ownership of incidents and issues relating to Azure, including Microsoft Premier Support escalations	✔	✔
Detailed Design Document • Detailed Azure design based on application and requirements analysis	Additional services available	✔
Deployment Activities • Resource deployments performed by Lanmark engineers	Additional services available	✔
Operating System Support		✔
Customer Runbook Documentation • Lanmark-coordinated runbook design and escalation list		✔
Account Review • Review Microsoft best practices and Lanmark recommendations • Review resource usage and cost-optimisation opportunities • Technical environment review (alerts, performance) • Runbook evaluation		✔
Incident Response	Urgent: < 4 hours Standard: < 24 hours	Emergency: < 15 min Urgent: < 1 hour Standard: < 4 hours

Add-on Services		
Migration assistance • Assistance getting your app and data migrated to Azure • Depending on requirements, available from Lanmark and/or Lanmark-approved partners	Additional services available	Additional services available
Custom DevOps Professional Services	Additional services available	Additional services available
DBA Services		Additional services available
Lanmark Application Services		Additional services available
Lanmark Managed Security		Additional services available

Support Teams

Your Lanmark Cloud Support for Azure Team

Lanmark Cloud Support for Azure provides specialised resources to deliver ongoing service and support for your business. Lanmark provides you with Azure-certified solutions architects and engineers who are ready to deliver always-on support and expertise to your business, 24x7x365.

Technical Onboarding Manager (TOM)

Lanmark will assign a Technical Onboarding Manager (TOM) during the implementation of your environment. As your dedicated guide, your TOM will work with you to coordinate the resources and project management associated with the deployment of your Azure environment. At the CloudHealth service level, the TOM provides initial guidance on using your account. At the Care+ service level, the TOM coordinates the process of getting your environments up and running on Azure.

Service Delivery Manager (SDM)

Lanmark will also assign an SDM to help guide you through the Lanmark support process and oversee the day-to-day management of your account including service, change and incident management.

Azure-certified Cloud Engineers

Each Service Delivery Manager is backed by a team of Azure-certified engineers, responsible for 24x7x365 monitoring and operational support for Azure subscriptions.

Service operations – Professional Services

With Care+, Lanmark will create your Azure environments. Lanmark Support Operations will also work with you to create a customised runbook to help manage the day-to-day support of your Azure environment, addressing incident and change management policies that we can safely implement for your business.

Architectural guidance and implementation

For Care+ customers, Lanmark will design, build and deploy your Azure solution. Care+ customers will have access to experienced Lanmark personnel who can assist with environment architecting and planning. This assistance is available through our implementation phase, or via scheduled guidance calls and standard ticket correspondence. Care+ customers can engage Lanmark for comprehensive application architecture review. Once we have completed the environment build, per the configuration agreed upon during the implementation process, our Azure support team will provide the day-to-day support of your Azure environments, addressing incidents and change management as well as day-to-day management via a customer runbook.

CloudHealth customers will be limited to using the standardised deployment templates only, and architectural guidance and implementation are not provided.

Lanmark has a repository of proprietary and opinionated best-practice templates that will be available to both CloudHealth and Care+ customers. Using ARM templates for deployments helps ensure that your environment will have up-to-date security improvements, access to the latest Azure services as released by Microsoft, and faster VM deployment times.

Care+:

- Access to template library
- Lanmark will deploy templates on the customer's behalf
- Lanmark will troubleshoot deployment failures
- ARM template creation will be limited to basic infrastructure and services (VM, storage, network, App Service, Azure SQL Database, etc. .) and existing gallery software items. Lanmark can create custom ARM templates through a Professional Services engagement (further changes to custom templates after creation are the responsibility of the customer).

CloudHealth:

- Access to template library
- Customer is responsible for all template deployment and troubleshooting

Customer Runbooks

During the implementation process, your TOM and SDM will work with you to create a customised monitoring response runbook. This runbook defines the immediate responses (IRs) the Lanmark support team will use as our standard operating procedures for your environment(s). Our IRs include custom escalation procedures in accordance with your business needs and best practices. These customer runbooks are designed to present the right information at the right time to our support teams to enable a world-class support experience. Providing relevant and focused guidelines to our support teams increases availability of customer solutions.

How to contact support

Our automated systems will also create tickets for events on your Azure account that require either your attention or the attention of a Lanmark team member. For example, our Datadog Monitoring service will create a ticket when an alarm is raised, and a Lanmark team member will triage the alarm and take appropriate action. Any time a ticket is updated, you will receive an email directing you back to the Lanmark Customer Portal to view the latest comments.

Phone: You can also call your Lanmark Cloud Support Teams 24x7x365.

Microsoft Premier Support escalations

Regardless of whether you purchase your Azure infrastructure directly from Microsoft (EA/Direct) or through the Lanmark Cloud Solution Provider (CSP) agreement, Lanmark serves as your sole point of contact for supporting your Azure environments. As a part of the Cloud Foundation service, if Microsoft ever needs to be contacted for technical escalations, Lanmark will do so on your behalf by leveraging our Microsoft Partner Premier Support agreement.

Escalations may occur for the following scenarios:

- An Azure subscription service limit increase is required (e.g., number of CPU cores).
- An issue that requires the involvement of a specific Azure product and/or engineering team to resolve.
- An issue where multiple customers are impacted (Azure service outages).
- Azure infrastructure SLA credit requests (when infrastructure is purchased through Lanmark CSP).

As a Microsoft-certified Azure Expert MSP with a partner- grade Premier Support agreement, Lanmark provides direct access to Azure Support, product and engineering teams as a part of our Azure management service.

Monitoring (Datadog)

Lanmark utilises a combination of Azure-native monitoring services and Lanmark services, called Datadog, as the primary monitoring and reporting platform for Azure workloads covered by the Care+ Service Level. Datadog is composed of nine discrete components that serve to deliver valuable insights about the health of an Azure environment and to provide our customers a reliable, scalable and intelligent monitoring service. While OMS is available to all Azure subscribers, customers using our Care+ service level can opt to have Lanmark respond to monitoring alarms. As an Care+ customer, you can work with your Lanmark Cloud Support team to create the customised monitoring solution that best fits your needs.

Monitoring components

1. OMS Log Analytics – an Azure-native log aggregation and analytics service that provides a powerful and scalable alerting platform.

2. Lanmark Event Horizon (Alert Processing) – Lanmark event processing system that parses alert data from OMS and provides integration into the Lanmark ticketing system.

3. Lanmark Ticketing – Lanmark ticketing system that is embedded in the Lanmark Customer portal.

4. Lanmark Smart Tickets (Auto Remediation & Enrichment) – Proprietary Lanmark automation framework that enables the delivery of real-time incident enrichment and remediation of incidents by running automation services (PowerShell/Bash for VMs, APL/CLI for Azure platform and PaaS services) in response to defined alerts.

5. Lanmark Alert Suppression (Noise Reduction) – Lanmark-proprietary service that allows for the suppression of alert tickets (and automated remediation activities) during planned events.

6. Lanmark Alert Synchronisation (Alert Governance) – Proprietary Lanmark automation service that performs ongoing synchronisation and enforcement of the production Lanmark alert definitions to all environments within our managed service fleet to ensure our customers have the latest and most up-to-date alert definitions.

7. Lanmark OMS Workspace Synchronisation (Alert Governance) – Lanmark-proprietary automation service that performs ongoing synchronisation and enforcement of the configuration of all standard Lanmark definitions (data sources and solutions) in each of the Azure Workspaces within our managed service fleet.

8. Lanmark PaaS Monitoring Synchronisation (Alert Governance) – Proprietary Lanmark automation platform that enables the configuration and reporting of key resource monitors for PaaS components of the Azure platform.

During the implementation process for Care+ customers, Lanmark will confirm any monitoring requirements and can assist in the creation of URL monitors for service availability upon request.

Alert definitions

Care+ customers will receive Lanmark's complete set of Datadog alerts including coverage for issues associated with antimalware, Windows Active Directory, MSSQL, IIS, Azure Activity logs, general system health and availability, Platform-as-a-Service metrics and numerous Linux and Windows VM performance counters. To receive a copy of the most current list of the Lanmark Datadog alert definitions, please reach out to your SDM.

URL availability monitors

In addition to the Datadog alert definitions, Care+ customers are eligible to request the configuration of up to three web test availability monitors based out of the OMS Application Insights service to help provide stronger service availability monitoring and IR management.

Incident Management

The management of incidents where restoration of the services is the primary objective. For workloads covered by Care+, Lanmark endeavours to restore normal service as quickly as possible when a problem or an incident occurs. Lanmark will aim to apply a consistent approach to all incidents, except where a specific approach has been previously agreed upon with you in accordance with your incident runbook. You can expect the following from the Lanmark incident management process:

Incident events can only be initiated by:

- Authorised customer contacts
- Lanmark
- Event management tools (e.g., Datadog)

- All incidents are logged in tickets accessible via the Lanmark Customer Portal. Lanmark support teams will investigate the incident in accordance with your service level once it is logged.
- Priority for tickets entered manually via the Customer Portal is initially set to "Standard." If required, please phone your Lanmark support team or your assigned Service Delivery Manager to request a priority escalation of your request. Incidents logged with a specific priority will not be changed to another priority without the agreement of all parties involved.
- Prior to investigation, Lanmark support will carefully review instructions on your account as documented via your incident runbook.
- Lanmark will collaborate with you and with any third parties that you nominate as technical contacts on your account to help resolve the incident.
- Lanmark support teams will communicate regularly with you throughout the incident, detailing their findings and any actions taken.
- If a Lanmark support engineer is unable to resolve an incident, they will escalate the incident until resolution is achieved. This escalation may be hierarchical (to a more senior Lanmark engineer or the service delivery manager / lead engineer – if applicable) or functional (involving specialist technical expertise from other functional groups or Microsoft).
- The action required to resolve an incident will vary depending on investigative findings. In some cases, a proposed solution may be complex or cause additional disruptive impact to your Azure environments. In these cases, the incident will be handled as a change through the Lanmark change management process and you will be consulted to determine the time window during which the solution or change may be implemented. Alternately, you may be required to act to resolve the incident, which will be communicated should such a need occur.
- An incident is deemed closed when you confirm that it is resolved. This is achieved through the incident ticket being set to a "solved" status.

Change Management

- Change management includes a standardised set of procedures that enables Lanmark to deliver efficient and prompt handling of all changes in an organised manner to help ensure minimum impact on the Services.
- Your Lanmark Service Delivery Manager will be available to work with you on all operational, technical and commercial changes to the environment.
- All changes will be managed through the Lanmark ticketing systems. This supports long-term tracking of all information and the optimum delivery of services through the various lifecycle processes of deployment, change management, incident management, etc.
- Lanmark will raise a ticket accessible via the Lanmark Cloud Support for Azure Customer Portal for changes that are owned or initiated by Lanmark. Conversely, you can raise a ticket for situations where Lanmark support is required for any changes owned and initiated by your business. You may also call the 24x7x365 support line to discuss a change and request that a ticket be created.
- Lanmark will organise support engineers with specific domain expertise to manage the change as scheduled and keep you fully informed on progress.
- For changes or upgrades to your own internal infrastructure, you are responsible for coordinating with your internal resources and third-party contacts to manage the change as scheduled and to keep Lanmark informed of the progress via a Lanmark support ticket.

Ongoing Management Service

Update management & patching: Lanmark leverages the Azure Update Management service to provide comprehensive reporting, patching and deployment solutions for customers who have a managed Care+ environment. By enabling Azure Update Management, customers can maintain an up-to- date environment with the highest levels of security, ensuring a rapid response to vulnerabilities. During the implementation phase, Lanmark will review your patching requirements and make recommendations based on established best practices for securing environments. After the initial configuration, Lanmark will provide ongoing support in the form of scheduling changes, 24x7x365 alert response for failed patching or failed deployment update runs, and reports on current patch levels within your environment. Customers will be responsible for setting a recurring patching schedule, determining the order of reboot for your environment, and ensuring all services are properly patched. Customers are also welcome to request ad hoc patching runs through a support ticket. For a list of supported Windows and Linux distributions, please refer to the OS section.

Note: Lanmark will not patch middleware or customer applications due to the potential for harming customers' environments when changes have not been thoroughly tested in the specific environment.

Backups: Care+ customers are entitled to have Lanmark support teams configure image -level backups for their Azure VMs. Image-level backups are non-intrusive and provide customers with the ability to restore an entire virtual machine. Currently, Azure supports application-consistent backups for Windows and file-consistent backups on Linux.

Should a backup job fail to complete, Care+ customers will benefit from Lanmark automation services that will automatically attempt to resolve the issue and will attempt to re-run the backup job. If a subsequent failure is detected, the issue will be escalated to the Lanmark support teams to investigate further and to escalate to Microsoft as required.

In the unlikely event that you require data restored from an image-level backup, phone in or log a ticket in the Lanmark Cloud Support for Azure Control Panel. Please provide detailed information regarding the VM instance and Azure Storage Account you need restored and to what VM that snapshot should be attached. Lanmark will only restore an image-based backup to a new volume, and you will be responsible for validating any restored data and moving it into your application. We recommend that customers regularly test restoration as part of normal business continuity planning.

Antivirus: The Care+ service also enables the Lanmark Managed Antivirus solution for Windows operating systems running on the Azure platform to help solve for increasingly complex challenges associated with security and compliance. Leverage our Managed Antivirus service to help ensure that all your VMs within your Windows Server solutions are protected by the enterprise-grade Windows Defender service and backed by our 24x7x365 support teams. Our Managed Antivirus service helps reduce your attack surface of new security threats by helping to ensure that the following is true for every Windows VM deployed into your subscription:

- Windows Defender Antimalware extension properly installed.
- Antimalware extension properly configured.
- Windows Defender service runs the most up-to-date virus definitions.
- If an antimalware event is detected, the Watchman service is leveraged to alert a Lanmark engineer to investigate further.

Operating systems support (Care+ only): Customers with Azure subscriptions covered under the Care+ service are entitled to operating system support for their Azure VM instances running supported operating systems versions/distributions.

Service Reviews

Service Reviews are available upon request for Care+ customers and provide an opportunity for regular governance sessions of your environment's performance and to review operational information such as the status of backups, patching and antivirus. The review may include the following items:

- Support tickets
- Monitoring alerts
- Upcoming change or maintenance events
- Product roadmap updates
- Microsoft Azure announcements

Response Time Guarantees

Support Tickets fall into one of the following severity levels:

- Emergency: Business-Critical System Outage / Extreme Business Impact – 15-Minute SLA (Care+ only)
- Urgent: Production System Impaired / Moderate Business Impact – 1-Hour SLA (Care+ only)
- Standard: Issues and Requests / Minimal Business Impact – 4-Hour SLA for Care+ / 24 Hour for CloudHealth

Note: All customer-submitted requests via the Control Panel are automatically categorised as Standard requests by the Lanmark Ticketing system. Please call Lanmark support 24x7x365 to escalate the issue to an urgent or emergency classification.

Additional services

Lanmark DBA Services

Lanmark has extensive experience and comprehensive support expertise to provide database support for MS SQL. We operate teams of highly trained and certified database experts focused on delivering an exceptional experience, 24x7x365. Our experts are available through every stage of your project, from architecture and design to administration and monitoring.

As part of our Care+ offering, Lanmark will provide support for Microsoft SQL Server and Azure SQL Server instances, including installation, basic configuration, monitoring, troubleshooting and backups, as illustrated below. Additionally, Lanmark can provide advanced DBA services tailored to your specific needs for an additional fee.

Lanmark Application Services (RAS)

Available as an add-on service for Care+ customers, Lanmark Application Services (RAS) extends always-on support up the stack to the application layer. RAS provides application expertise, performance monitoring and proactive support for your mission- critical websites and applications. RAS enables end-to-end transaction visibility and real-time end-user experience monitoring using industry-leading tools to help you meet uptime requirements for mission-critical applications with a cost-effective model. RAS is available in blocks of 10, 20 or 40 hours per month. Benefits include:

- The ultimate application services experience (set up, monitoring and proactive optimisation)
- 100% Production Platform Uptime Guarantee with approved HA environments
- Proactive guidance to ensure stable application environments
- Proactive application and infrastructure monitoring and tuning for maximum application performance
- Constant analysis of performance metrics and trending reports
- Highly customised solutions delivering a complete view of your environment
- End-user experience analysis and incident detection
- Real-time transaction-level monitoring
- Diagnostic performance reporting

Lanmark Managed Security (RMS)

Available as an add-on service for Care+ customers, Lanmark Managed Security – Proactive Detection and Response (RMS – PDR) helps protect your IT environment against advanced persistent threats (APTs) and other cyberattacks. Lanmark provides deep security knowledge, leading technology and advanced threat intelligence, tailored to your business needs. Our 24x7x365 defense actively hunts for threats in your environment and when detected, we take ownership of responding to them immediately. This frees your staff to focus on the initiatives that drive your business forward, usually for much less than the cost of internally developed security solutions.

Feature	Benefits
Host and network protection	Get advanced host and network protection platforms targeted at zero-day and non-malware attacks and traditional compromise tactics.
Vulnerability management	Get advanced scanning and agent technologies to understand environment specifics and respond to threats and attacks based on your needs.
Log management	Use Lanmark to collect standard operating system logs and assist in identifying additional data that may be collected.

Reasons to choose Lanmark Managed Security

1. 24x7x365 detection and response: Our experienced Lanmark security team monitors and manages your environment around the clock, responding to threats based on your specific business needs and IT requirements.

2. Leverage security experts: Use Lanmark Managed Security service as a security force multiplier. We tailor support to meet your security goals, whether it's strategic planning for best-practice cloud security or tactical day-to-day security monitoring and threat analysis.

3. Employ industry best practices and advanced security solutions: Lanmark works closely with a select list of security providers to provide access to collective expertise from across the industry and advanced technology to protect your managed cloud.

4. Meet security goals while lowering TCO: The advanced security protection of Lanmark Managed Security can significantly lower TCO over internally developed security operations centers and comparable managed security service offerings.

Lanmark Professional Services

Application Migration Assistance

Transitioning from an existing environment to Microsoft Azure requires specific expertise and resources skilled in technology transformation, migration planning and risk mitigation. For an additional fee and with assistance from other businesses where needed, Lanmark will own the process of migrating your applications to Azure. For more information about pricing and timelines, please engage your sales representative.

Custom DevOps Professional Services

Lanmark has extensive experience working with DevOps methodologies, practices and toolchains. We can assist customers, via a Professional Services engagement, in adopting DevOps methodologies and practices inside their own organisations.

Lanmark DevOps Professional Services has two methods of delivering DevOps outcomes for customers:

- Working with you to identify and implement any additional custom tooling necessary to achieve your business goals.
- Assisting you in evaluating and assessing the maturity of DevOps practices within your organisation if you are in the early stages of your DevOps journey.

You can expect the following from our Professional Services engagement:

- Creation of in-depth customisation for your application utilising the Microsoft DevOps toolchain.
- Assistance in the writing of customised configuration management code using third-party tools.
- Implementation and customisation of continuous integration/continuous deployment (CI/CD) toolchains using third- party tools.
- Custom plug-in integration between DevOps and ChatOps tools like Slack.

DevOps maturity and strategy planning

As part of a DevOps Professional Services workshop, Lanmark will help deliver the outcomes required via internal or trusted partner-led resources. These are one-time engagements using an agreed-upon fixed time box, where we, or third parties that we work with, can help assess your current DevOps maturity and define a strategy to meet your objectives. These include, but are not limited to, assistance with configuration management, continuous integration/continuous deployment and release management, application architecture, containerisation, automation and monitoring capabilities. During the engagement, you'll:

- Learn the principles, benefits and tools behind a successful DevOps culture.
- Discover the techniques for building modern applications that are self-healing and self-sustaining.
- Review your current build and deployment processes with our experts.

- Develop a roadmap that outlines your goals and timelines and defines how to integrate DevOps automation into your environment.
- Classify applications and identify key stakeholders to help drive the adoption of DevOps practices.
- Receive application architecture design options and propose solutions.

Appendix A:

Subscription management requirements

As a part of the Lanmark Cloud Support for Azure offering, Lanmark will be required to perform actions in your Azure environment as a trusted partner. Lanmark cannot fulfill our role as your managed service provider without the correct level of access and permissions. Lanmark takes your trust and your security very seriously and has integrated safeguards into our management service to avoid abuse of these services, leveraging Lanmark corporate identities (along with the built-in security features like MFA credentials, password rotation, etc.) . If Lanmark is unable to secure the appropriate level of access required to deliver our management services, we are unable to deliver our managed services in an at-scale manner using automation services and consistent tool sets for our global team of support engineers (helping Lanmark drive cost efficiency into our managed service which we pass along to our clients).

Owner/contributor access

To deliver our Lanmark Cloud Support for Azure service, Lanmark requires “Owner” or “Contributor” permissions to all Azure subscriptions under our management. Several of our support offerings and/or tools require that the Owner/Contributor account be configured as an “organisational account” rather than as a “Microsoft account.” If you are unable or unwilling to provide Lanmark with an organisational account setup for Owner/Contributor permissions, some support services may not be available or may be limited in scope.

The Owner/Contributor account credentials will be stored within a secure password repository at Lanmark and only utilised by our technicians during support, troubleshooting, deployment and other similar activities.

Azure Active Directory service principals

Lanmark requires the configuration of Service Principal Names (SPNs) to enable our management services to access resources that are secured by an Azure AD tenant. During onboarding activities, the user will be presented with an Azure AD application to consent the required permission for Lanmark to access resources within a tenant.

Lanmark SPNs are assigned a “least-permission levels” model, where we have defined the access policy and permissions, authentication and authorisation to deliver programmatic access to resources within that subscription, enabling a whole host of automation services to deliver Lanmark Cloud Support for Azure. SPN credentials are stored securely in a KeyVault within Lanmark’s Managed Azure Subscription. The keys are encrypted at rest and in transit.