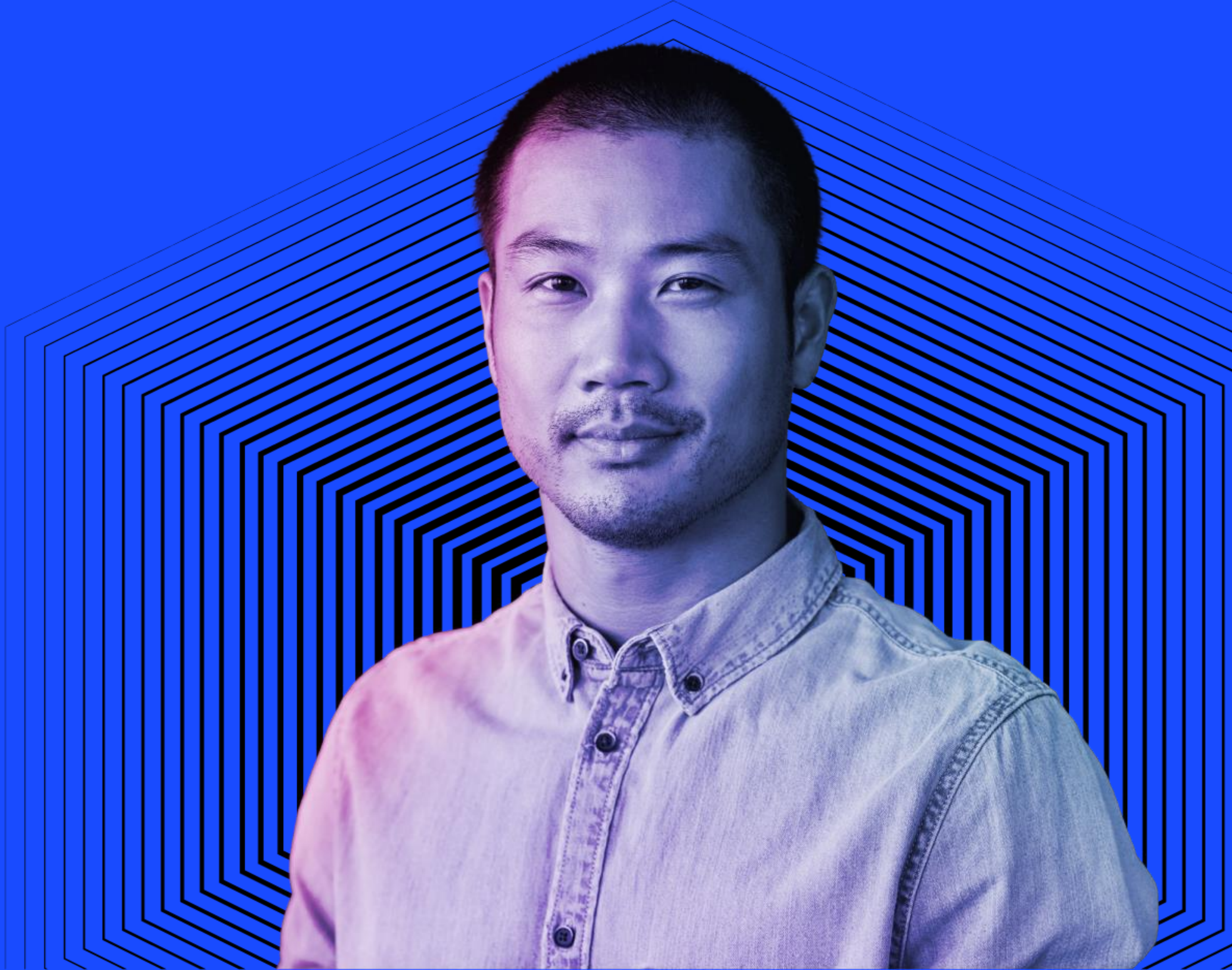
LOGICALIS
Architects of Change

Customer “Onboarding Kit”

for Logicalis Azure Managed Services



Logicalis Transition Methodology Phases

Although projects by definition are unique, having a consistent approach to delivering them is the entry point to an efficiently planned Transition and a successful outcome.

The Logicalis Transition Methodology is thoughtfully constructed based on decades of implementations, experience gained from lessons learned, and a focus on continual service improvement.

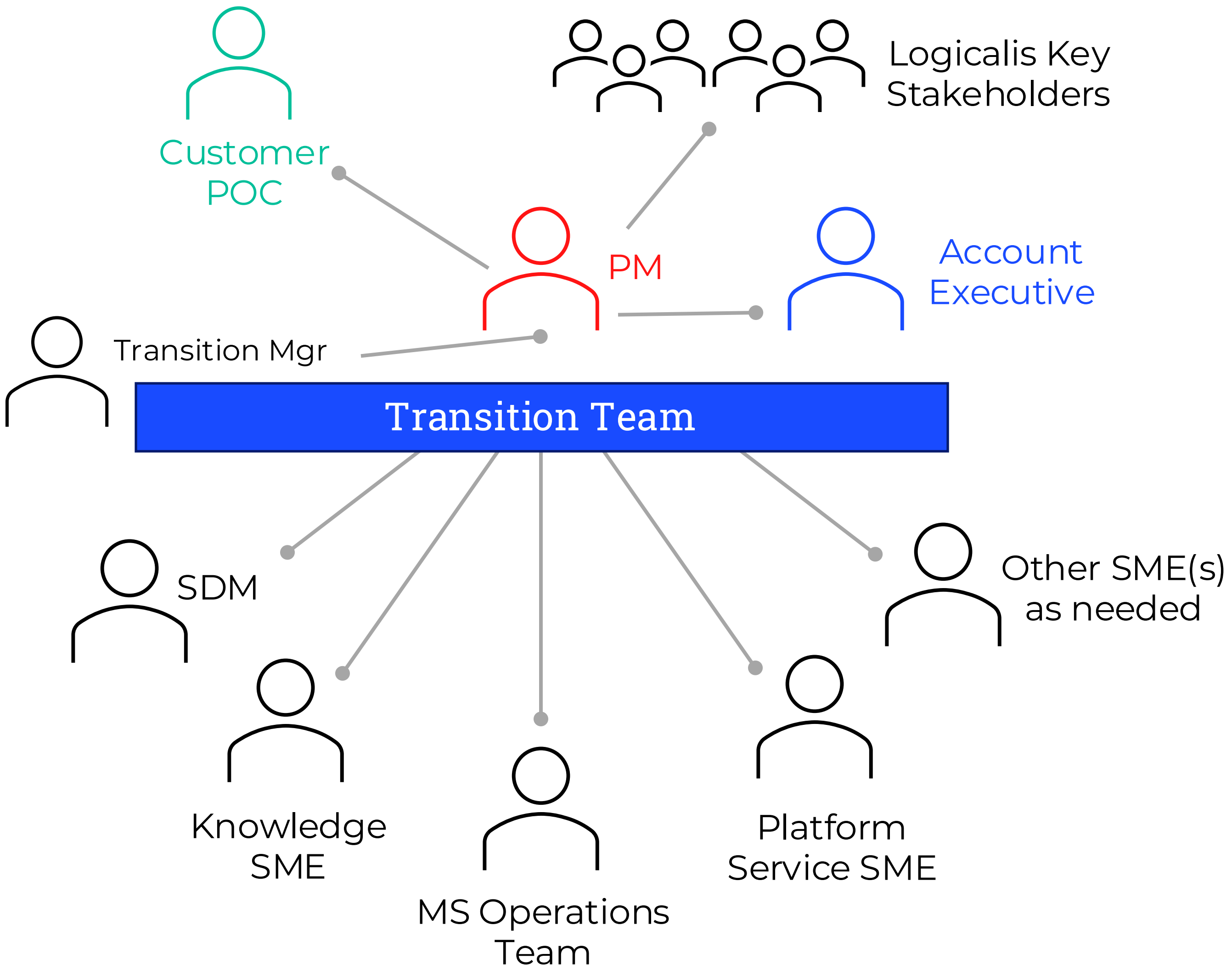
Transitions are expected to be completed in 60 calendar days unless stated otherwise in the SOW.

- Initiation
- Plan
- Onboard
- Test & Validate
- Cutover & Hypercare
- Transition Close

Transition Project Governance

The Logicalis Project Manager will be at the center of the Governance Model and *accountable to the Customer Point of Contact* and Logicalis Key Stakeholder(s).

The Transition Team Subject Matter Experts (SMEs) represent and are accountable to the Transition Manager and PM for the onboarding requirements and tasks for their respective organization.



Customer Role in Transition

Our most successful and timely Transitions are those in which the Customer has been highly collaborative and engaged at the necessary points in the project. Logicalis will provide the guidance and do the heavy lifting but there are some dependencies on the Customer to provide the necessary information, access, and actions to fuel the project engine.

Here are few ways our Customers can facilitate a timely Transition:

- Designate a Customer Project Manager or primary Point of Contact (POC) to act as the counterpart to the Logicalis PM
- Make available Customer Subject Matter Experts (SMEs) for knowledge transfer, planning, workshops, and assigned Customer tasks in support of the Transition
- Prioritize Logicalis access, credentials, and implementation of the selected mode of Customer/Logicalis interface *(i.e. VPN and device connectivity)*
- If not already readily available, start gathering Configuration Item (CI) data for in-scope infrastructure
- Be prepared to share and contribute to Knowledge Base development
- Consistent participation and engagement in status meetings, risk management, and Project Plan execution

LOGICALIS
Architects of Change

Logicalis Customer Requirements

Hear are some ways our customers contribute to an efficient and successful Transition

Connectivity

Our customers are expected to allow Logicalis to access their Azure environment through app registration

Device Information

Logicalis will use monitoring tool to discover devices.
Customer will need to Provide Logicalis with the supported devices information (Locations, Users, etc.) for our CMDB

Access

Instructions and timely assistance in provisioning Logicalis necessary access with appropriate permissions to deliver the contracted services.

Tools

Provide a VM/server for hosting our monitoring tools.

Support Documentation

Share essential documentation to our Service Delivery teams to share knowledge about your environment *(Network diagram, Build sheets, IT Support escalation matrix, etc.)*

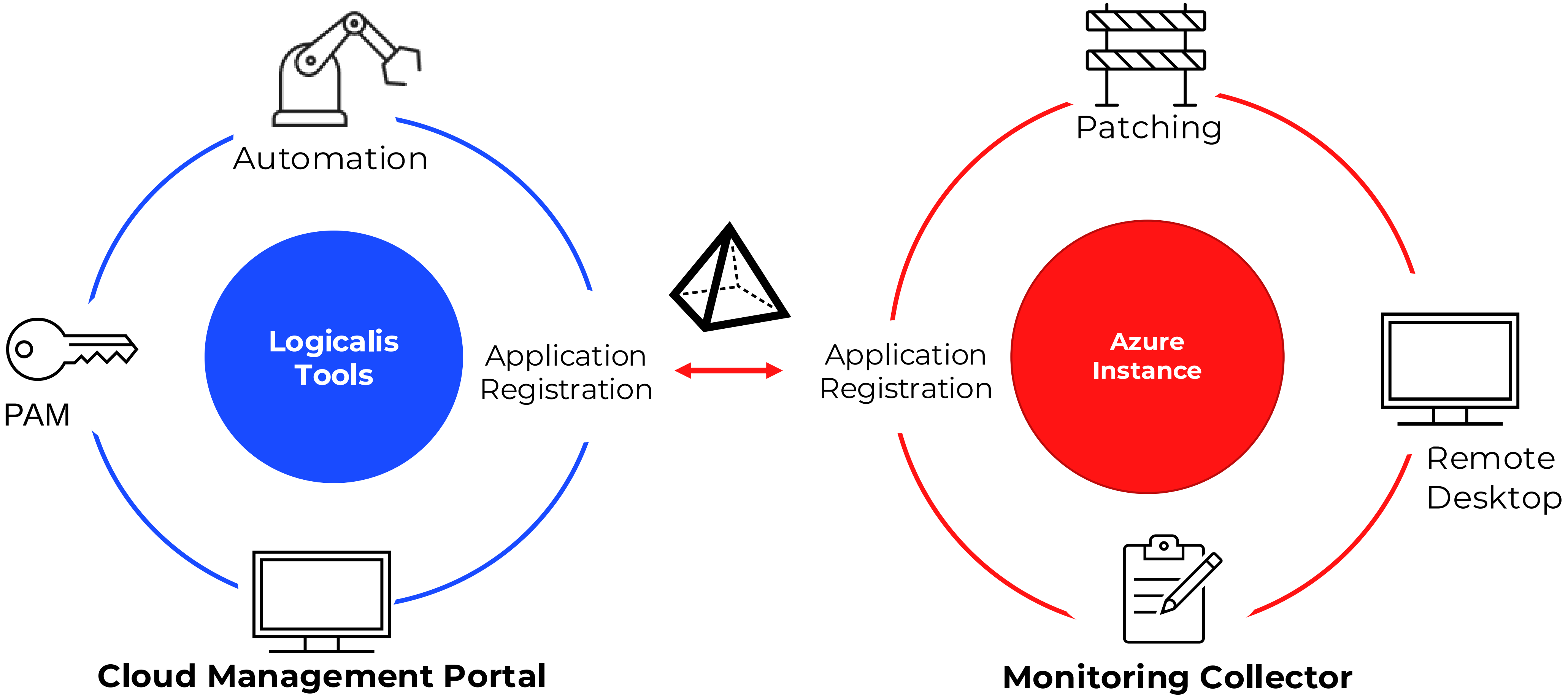
LOGICALIS
Architects of Change

Establishing Connectivity-Access

Step 1

Establishing Connectivity-Access

LOGICALIS
Architects of Change



Logicalis Managed Services pricing is based on a fully deployed, functional, tested, and production-ready customer environment at contract commencement utilizing Logicalis recommended secure interface protocols and tools. Logicalis reserves the right to adjust the pricing based on information found during due diligence or for a customized integration.

Step 2

Azure Tools Setup and Configuration

(No Customer Action Required for Step 2)

LOGICALIS
Architects of Change

Lighthouse

Azure Lighthouse enables multi-tenant management with scalability, higher automation, and enhanced governance across resources.

With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust tooling built into the platform. Customers maintain control over who has access to their tenant, which resources they can access, and what actions can be taken. Enterprise organizations managing resources across multiple tenants can use Azure Lighthouse to streamline management tasks.

Beyond Trust/Xton

Logicalis will deploy a remote access privileged identity management / privileged access management (PIM/PAM) tool with specific privileged remote access for managing Azure hosted devices

Cloud Management Portal

Cloud Management Portal for Microsoft Azure is a simple way to view and track all of your Azure subscription usage and spending. CMP dashboard and reporting features give you a clear understanding of your Azure consumption and expenditure.

Logicalis Professional Services will set up and configure these Managed Services Azure tools

Logicalis Access Permissions

Lighthouse for Azure Portal

- Utilizes existing Logicalis individual accounts
- Contributor role for Tier 2+ Engineers
- Reader role for Tier 1 and Service Deliver Managers
- Rights elevation (just-in-time) for Global Admin with customer approval
- Conditional Access (IP based)

PAM Access Requirements

- Utilizes existing Logicalis individual accounts to access PAM solution
- Customer Windows Servers Rights
  - Single Administrative Account in Administrators group
  - Prefer domain account given local admin rights
  - If domain controller, must be domain admin
  - If necessary, can be individual local accounts
- Service Account for Monitoring
  - Must have same admin rights, but can be denied interactive login
  - Non-Expiring 32 to 128 character password

Cloud Management Portal

- Cloud Management Portal Access
- Read Account for all the environment
- Contributor to policies

LOGICALIS
Architects of Change

Step 3

Monitoring Tools Setup and Configuration

LogicMonitor Collector

The Windows Collector is a virtual server used by Logicalis for all device monitoring contracts. The customer and Logicalis will both need to complete some actions to complete this Step.

Logicalis - *Connectivity Actions*

- Build VM to host monitoring tools in customer's infrastructure with access to both in scope supported devices
- Supported devices require WMI to be enabled and credentials provided to Logicalis

Logicalis - *Server Build Actions*

- Server specifications will be provided during project planning. Server resources are right-sized to project scope
- Logicalis will license and manage LogicMonitor Collector

LOGICALIS
Architects of Change

Onboarding Steps

Step 4

Logicalis ITSM Tool

(No Customer Action Required for Step 4)

Information Loaded into ITSM by the Logicalis Transition Manager:

- Company Information (Name/Address)
- Users – Contacts that will receive incident notifications, provide change approvals, requiring access to our "OSM Portal" (ITSM tool)
- CMDB – Central repository for supported device information
- Transition Project – Required tasks to be completed internally by the Logicalis Managed Services team to onboard the services

Step 5

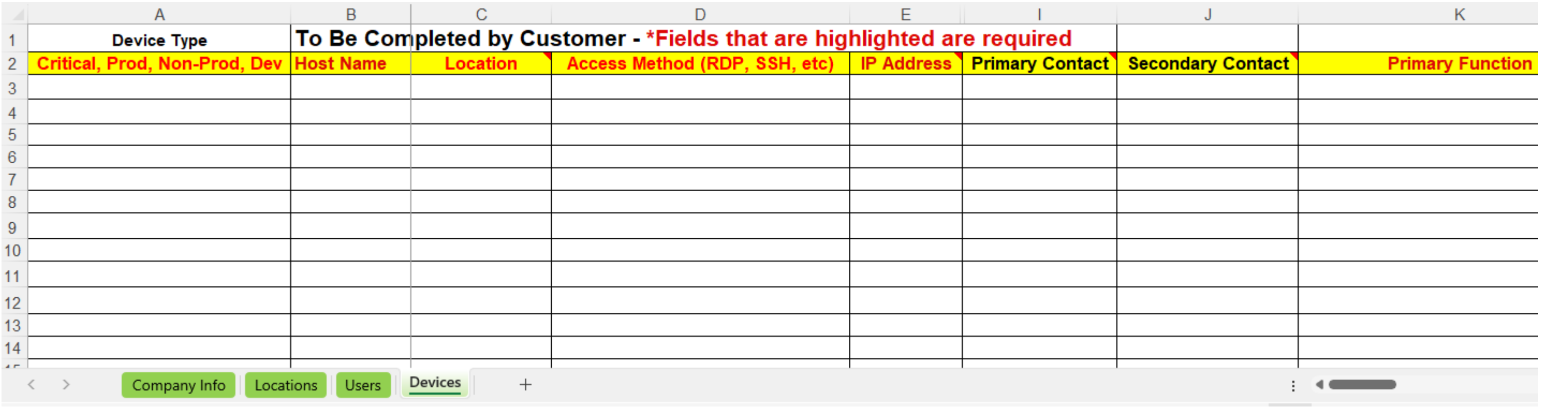
Supported Device Information (CMDB)

Customer - *Configuration Item Information Requirements*

Logicalis may require Customer assistance to collect select CMDB information:

- *Users- user email/phone information who will need portal access*
- *Primary & Secondary customer contacts for notification and/or support*
- *Primary function of the device*
- *Device priority (Critical, Prod, Non-Prod)*

The Logicalis Transition Manager will input any additional information required



	A	B	C	D	E	I	J	K
1	Device Type	To Be Completed by Customer - *Fields that are highlighted are required						
2	Critical, Prod, Non-Prod, Dev	Host Name	Location	Access Method (RDP, SSH, etc)	IP Address	Primary Contact	Secondary Contact	Primary Function
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								

Step 6

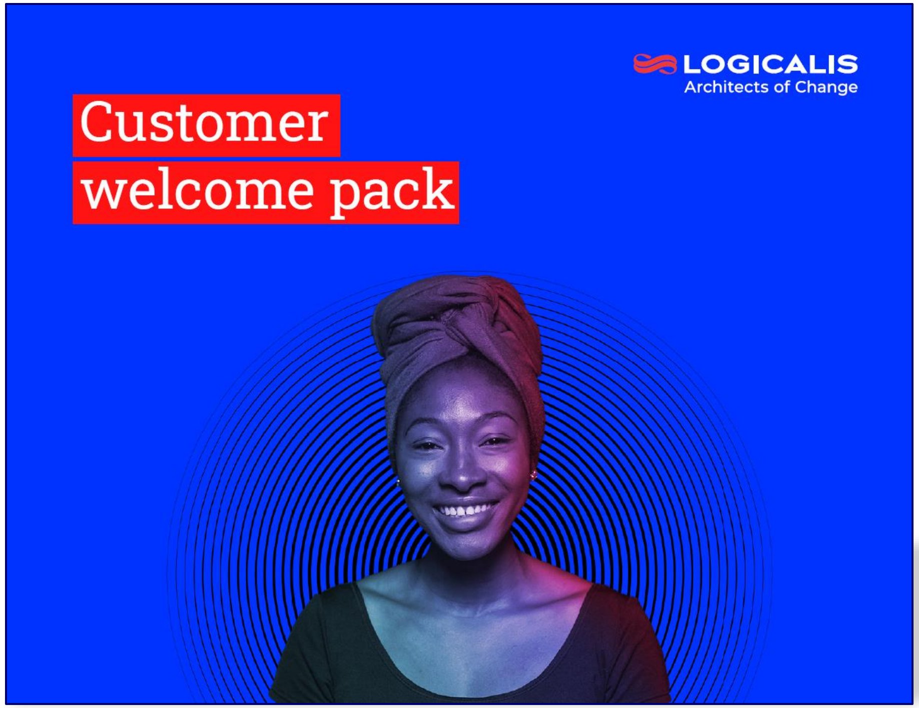
Customer Enablement for Tools, Process, Reporting, etc.

Logicalis “Customer Welcome Pack”

- ✓ Escalation & contact information
- ✓ Portal Training - How to open an incident or request
- ✓ Approve change request
- ✓ Navigating the ITSM Portal
- ✓ How to view DFP reporting

*The Logicalis **SDM** will provide Customer Welcome Pack and schedule time to provide Customer user training*

(Customer participation in training is the only action required for Step 6)



LOGICALIS
Architects of Change

Customer
welcome pack

LOGICALIS
Architects of Change

Logicalis Managed Services Access Tool

LOGICALIS
Architects of Change

Logicalis Managed Services:

Management Infrastructure

Security is priority, and to ensure strict security between Logicalis and our customers Logicalis Managed Services uses dedicated Virtual Desktop Infrastructure to connect to supported devices.

LMS VDI:

- Industry Security Standards – Scanned, Audited, and Maintained
- Individual Identity Source – Access Approved, Audited, and Automated
- Multi-Factor Authentication – Enforced and Automated Configuration
- Monitored – Security Information and Event Management (SIEM)
- Video Session Recording – All activity
- Device Credentials – Role-Based Access, Logged, and Audited
- Network Segmentation

Logicalis Managed Services:

Azure Portal Access

Logicalis Managed Services uses additional security for accessing customer's Azure Portal.

Conditional Access Policy

- Azure Portal only accessible from within the Secured LMS VDI environment

Individual Identity Source – Azure Lighthouse

- Role-Based Access Control
- Secondary MFA
- No Additional Account Management Overhead
- See Microsoft site for additional Azure Lighthouse information

Session Manager Gateway

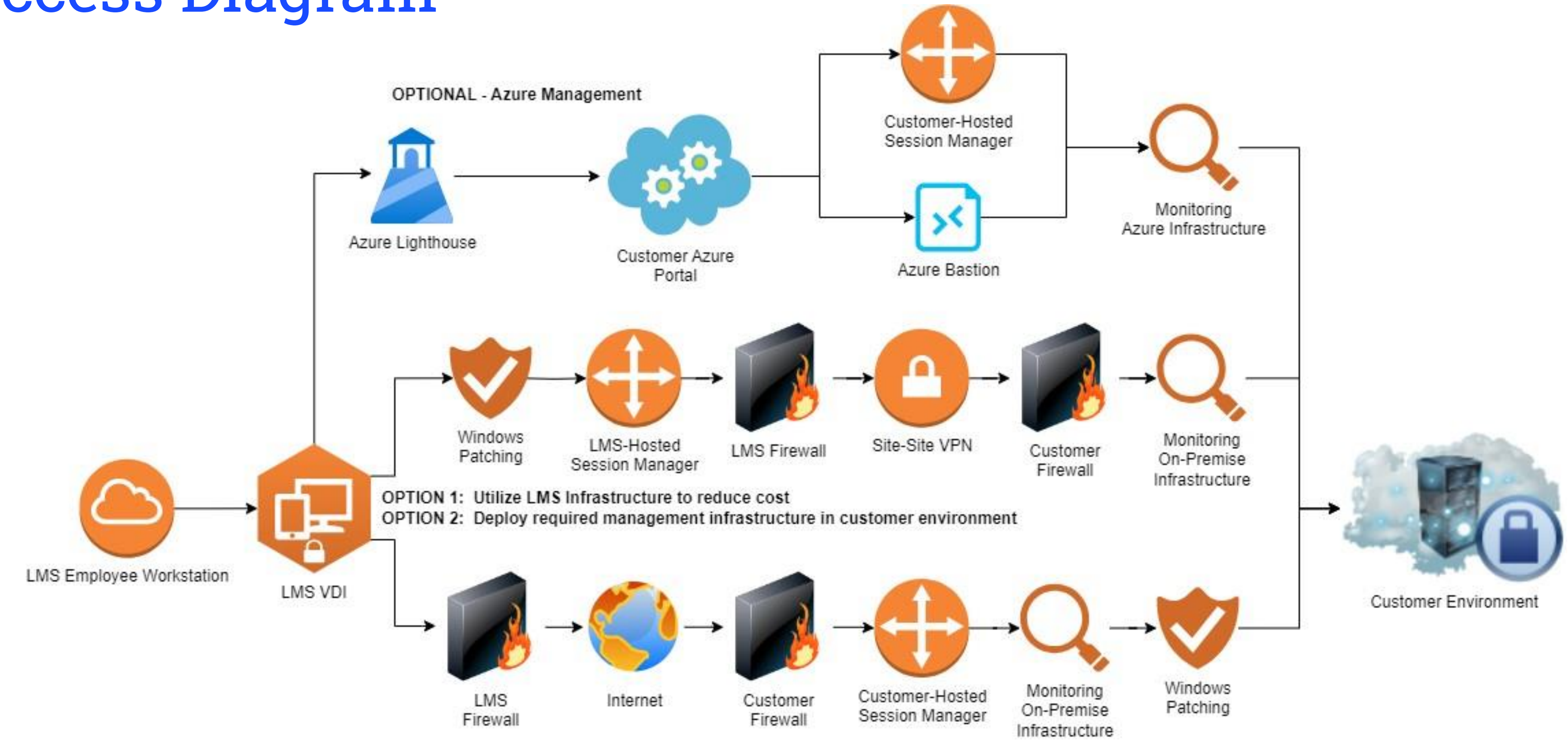
- Secures remote management sessions regardless of protocol

Bastion

- Azure native remote control of Azure virtual machines
- Only used when necessary

Logicalis Managed Services:

Access Diagram


OPTIONAL - Azure Management
Azure Lighthouse
Customer Azure Portal
Customer-Hosted Session Manager
Azure Bastion
Monitoring Azure Infrastructure
Windows Patching
LMS-Hosted Session Manager
LMS Firewall
Site-Site VPN
Customer Firewall
Monitoring On-Premise Infrastructure
LMS Employee Workstation
LMS VDI
Customer Environment
LMS Firewall
Internet
Customer Firewall
Customer-Hosted Session Manager
Monitoring On-Premise Infrastructure
Windows Patching

OPTION 1: Utilize LMS Infrastructure to reduce cost
OPTION 2: Deploy required management infrastructure in customer environment

LOGICALIS
Architects of Change

Thank you