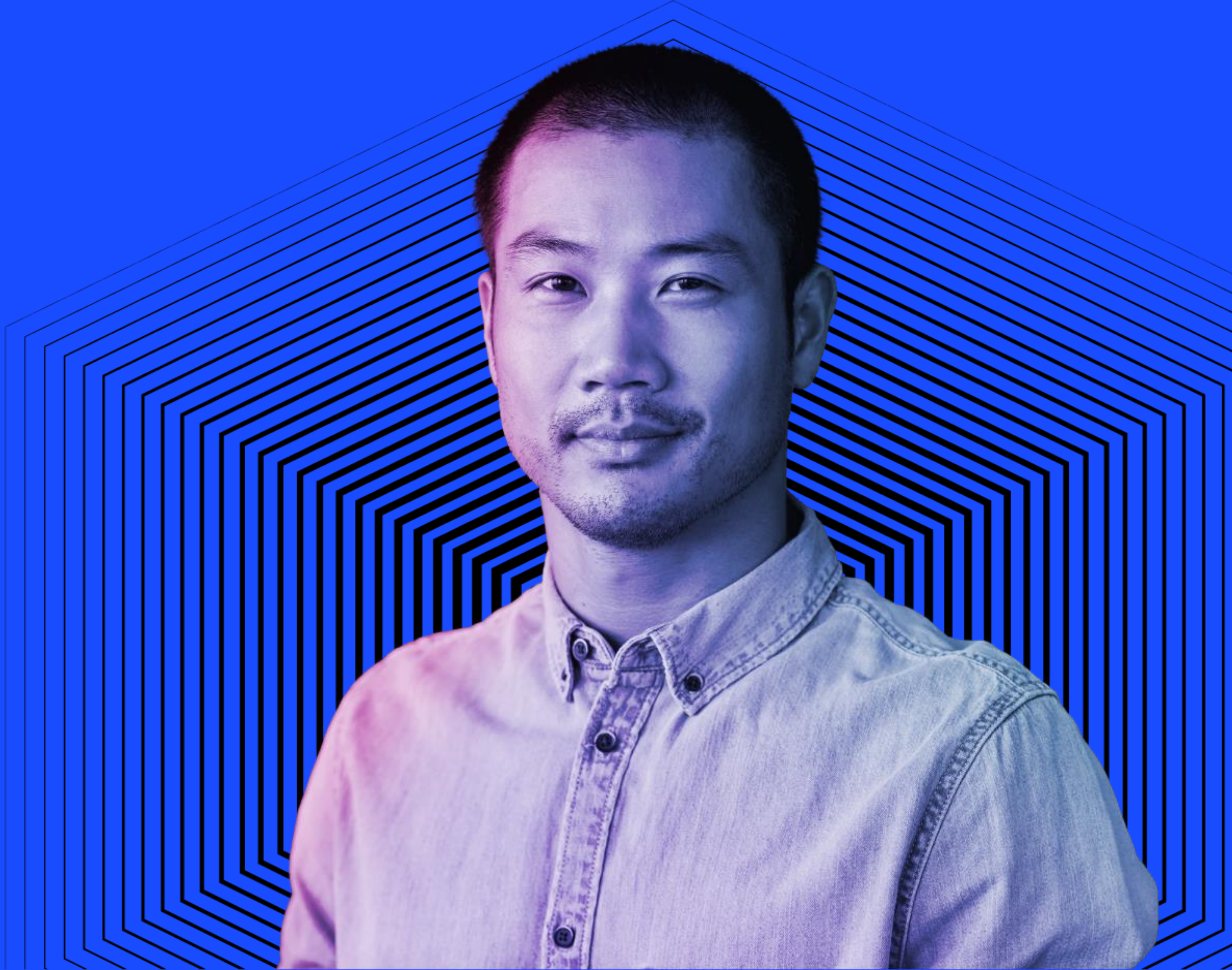
LOGICALIS
Architects of Change

Customer “Onboarding Kit”

for Logicalis Private 5G
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.

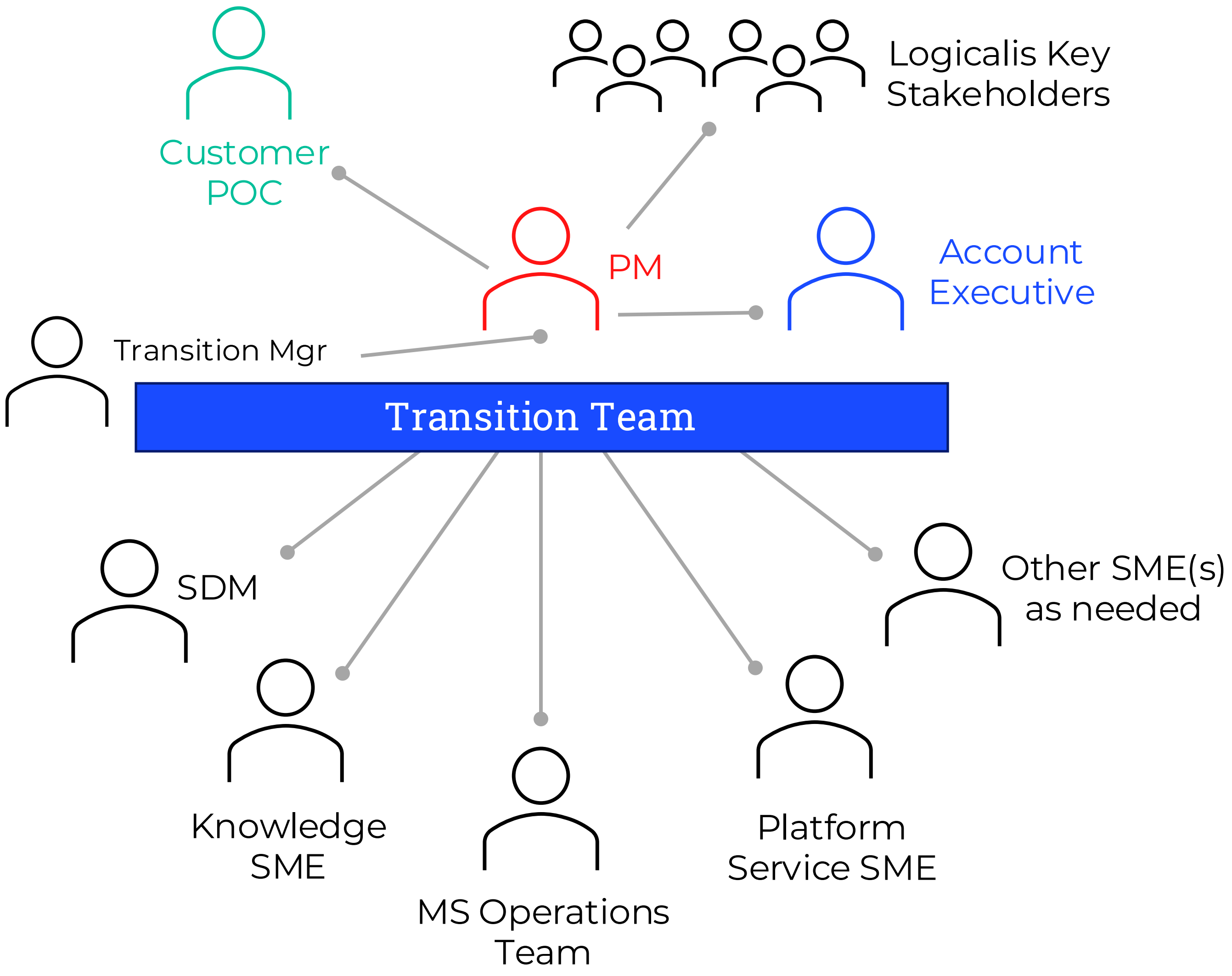
Transitions are expected to be completed in 60 calendar days unless stated otherwise in the SOW.

- 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
- ✓ Engagement in status meetings, risk management, and flexing to the needs of the project

Logicalis Customer Requirements

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

Connectivity

Our customer is expected to build a VM to host Cisco ASAv, configure VPN end point, and possibly manage NAT IPs depending on VPN solution.

Device Information

Provide Logicalis with the supported devices information (hostname, IP, 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

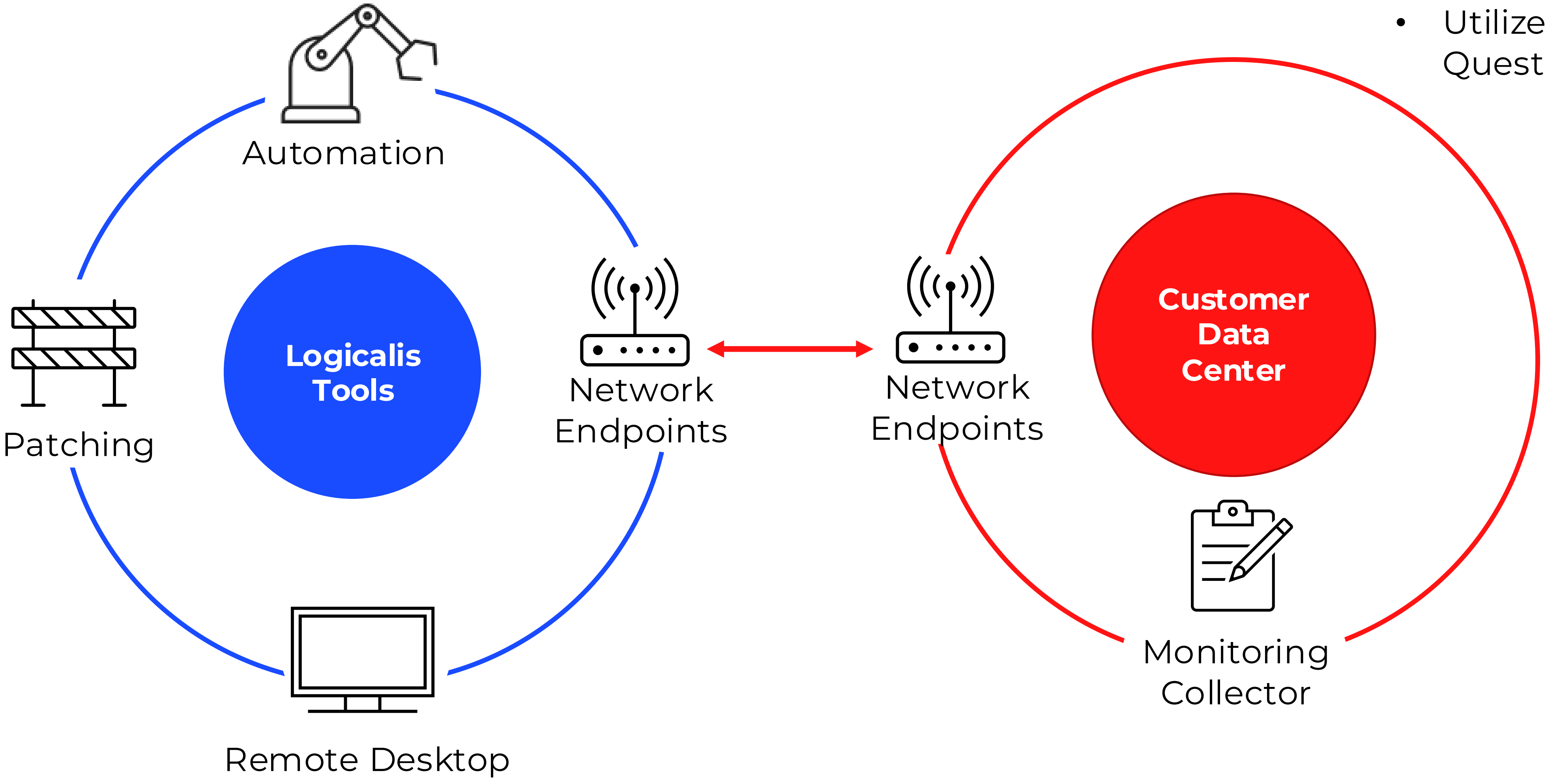
Establishing Connectivity

Step 1

Establishing Connectivity (options)

Questions:

- How will we connect to customer data centers?
- Utilize our connectivity Questionnaire?

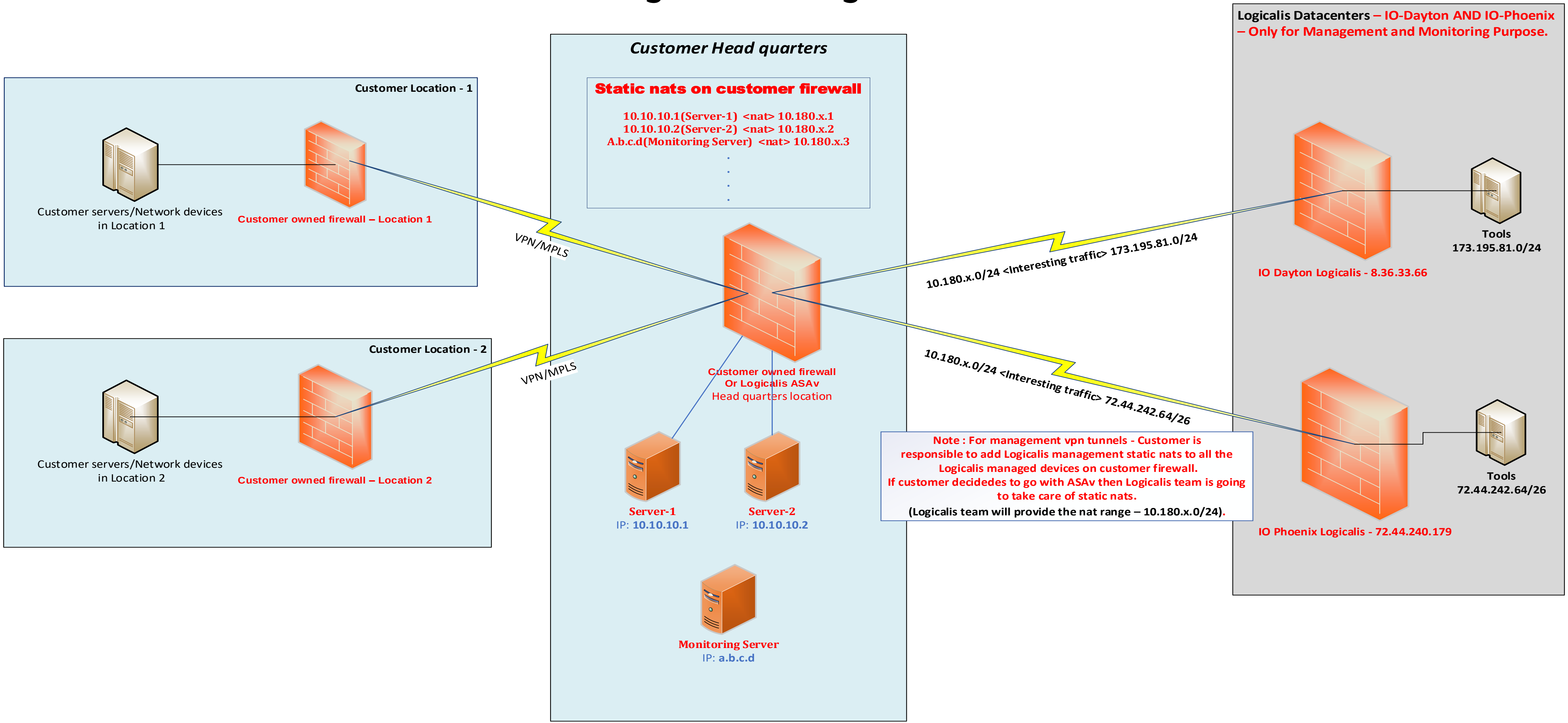


Step 1 – Connectivity

LOGICALIS
Architects of Change

VM hosted VPN ASAv Server Specifications and Information

VPN Tunnel Diagram from Logicalis to Customer


Customer Location - 1
Customer servers/Network devices in Location 1
Customer owned firewall – Location 1
VPN/MPLS
Customer Location - 2
Customer servers/Network devices in Location 2
Customer owned firewall – Location 2
VPN/MPLS
Customer Head quarters
Customer owned firewall Or Logicalis ASAv Head quarters location
Server-1
IP: 10.10.10.1
Server-2
IP: 10.10.10.2
Monitoring Server
IP: a.b.c.d
10.180.x.0/24 <Interesting traffic> 173.195.81.0/24
10.180.x.0/24 <Interesting traffic> 72.44.242.64/26
Logicalis Datacenters – IO-Dayton AND IO-Phoenix – Only for Management and Monitoring Purpose.
IO Dayton Logicalis - 8.36.33.66
Tools
173.195.81.0/24
IO Phoenix Logicalis - 72.44.240.179
Tools
72.44.242.64/26

Static nats on customer firewall

10.10.10.1(Server-1) <nat> 10.180.x.1
10.10.10.2(Server-2) <nat> 10.180.x.2
A.b.c.d(Monitoring Server) <nat> 10.180.x.3
.
.
.
.

Note : For management vpn tunnels - Customer is responsible to add Logicalis management static nats to all the Logicalis managed devices on customer firewall.
If customer decidedes to go with ASAv then Logicalis team is going to take care of static nats.
(Logicalis team will provide the nat range – 10.180.x.0/24).

LOGICALIS
Architects of Change

Onboarding Steps

Step 1 – Connectivity

LOGICALIS
Architects of Change

VM hosted VPN ASAv Server Specifications and Information

Purpose

Network connectivity between Logicalis and the customer are required to access supported devices. Generally, Logicalis connect to our customers via VPN tunnel over the internet. It is preferred if a dedicated VM is provided with Cisco ASAv installed.

Requirements

This page must be filled out with the relevant information by both the customer and a Logicalis Network Engineer. **ALL PARTS IN GREEN ARE REQUIRED TO BE FILLED OUT BY THE CUSTOMER.**

Notes

If there are any other consideration that need to be made to facilitate a VPN tunnel to the Cloud environment, please contact your Project Manager or Service Delivery contact immediately to discuss.

1. VM Server SPECS of ASAv
   a. CPU: 1 cpu
   b. MEMORY: 2gb
   c. Storage 40gb
2. Recommended Hostnames of ASAv
   a. LMS-xxx-ASAv01 (xxx=3 character customer abbreviation)
3. Use Cisco ASAv Version 9.14(3)13
4. Ports needed from Logicalis
   a. TCP HTTPS
   b. TCP 22
   c. ICMP
5. Logicalis ranges
   a. 173.195.81.0/24
   b. 8.36.33.66/32
   c. 72.44.240.179/32
   d. 72.44.242.64/26

Refer this link for any references https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asav/quick-start-book/asav-910-qsg/asav_vmware.html#id_45781

Customer Name		
Site Location		
	Logicalis	**Customer**
Device Model	Cisco ASA	🟩
VPN Peer IP	IO Phoenix - 72.44.240.179 IO Dayton - 8.36.33.66	🟩
Site ID	All DCs	🟩
	PHASE 1 (IKEv2)	
Encryption	AES256	🟩
Hash	SHA256	🟩
DH-Group	14	🟩
Lifetime	86400	
Pre-Shared Key	TBD	
	PHASE 2 (IPSEC – IKEv2)	
Encryption	AES256	🟩
Hash	SHA256	🟩
PFS	14	🟩
Lifetime	3600	
Encrypted Networks		🟩

Step 2

Monitoring Tools Setup and Configuration

Monitoring Collector

The Windows Collector is a physical or 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.

Customer/Logicalis
Connectivity Actions

- Open appropriate ports to allow connectivity to end devices and for Logicalis access to maintain collector
- Provide VM to host Monitoring Collector in customer's infrastructure with access to both in scope supported devices
- Internet access for Monitoring collector to patch OS & install Monitoring and manage collector (details can be found in the attached file)
- Supported devices require SNMP or WMI to be enabled and credentials provided to Logicalis

Customer/Logicalis
Server Build Actions

- Server specifications will be provided during project planning. Server resources are right-sized to project scope
- OVA URL link will be provided to download VM build during transition
- Logicalis will license and manage Monitoring Collector

LM Collector Deployment Guide

Step 3

Logicalis ITSM Toolset

(No Customer Action Required for Step 3)

Information Loaded in our ITSM toolset by the Logicalis Transition Manager:

- Company Information (Name/Address)
- Users – contacts that will receive incident notifications, provide change approvals, require access to ITSM Portal, etc.
- CMDB – central repository for device information
- Transition Project – Required tasks to be completed internally by the Logicalis Managed Services team to onboard the services

Step 4

Supported Device Information (CMDB)

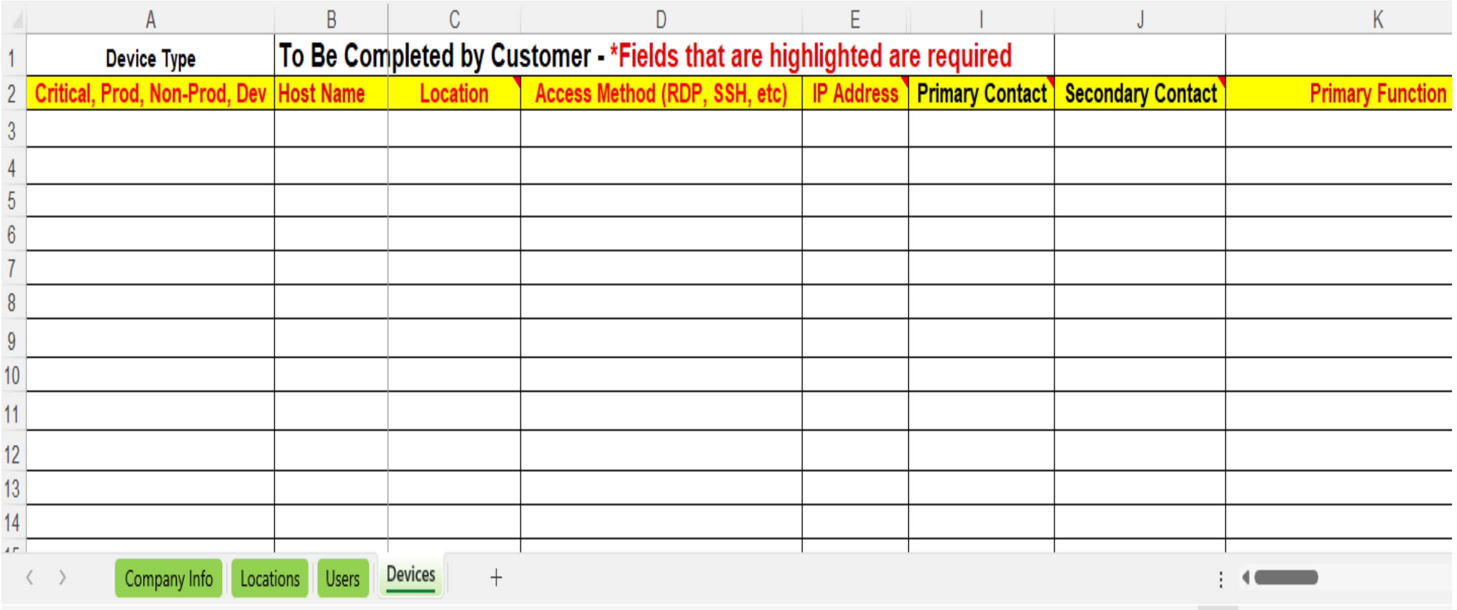
(No Customer Action Required for Step 4)

Logicalis Build Team – Required *Configuration Item Information*

Logicalis may require Customer assistance to collect select CMDB information:

- *Locations – full address of device locations*
- *Users- user email/phone information who will need portal access*
- *Host name*
- *Device Type*
- *Device Location*
- *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 requirements 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 5

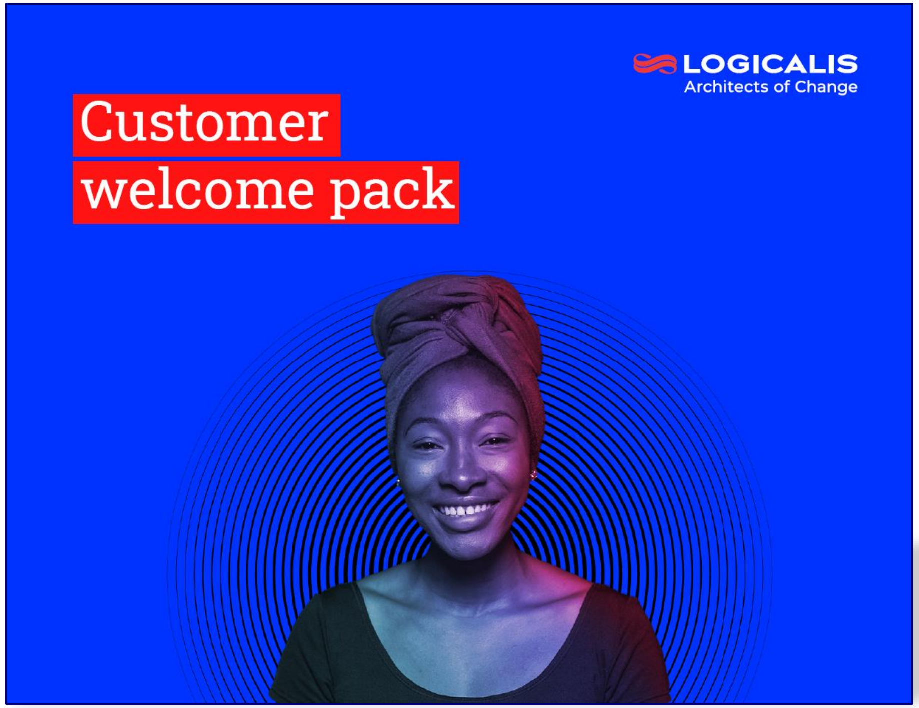
Customer Enablement for Tools, Process, Reporting, etc.

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 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 5)



LOGICALIS
Architects of Change

Customer
welcome pack

LOGICALIS
Architects of Change

Logicalis Secure Access Methodology

Logicalis Managed Services

Management Infrastructure

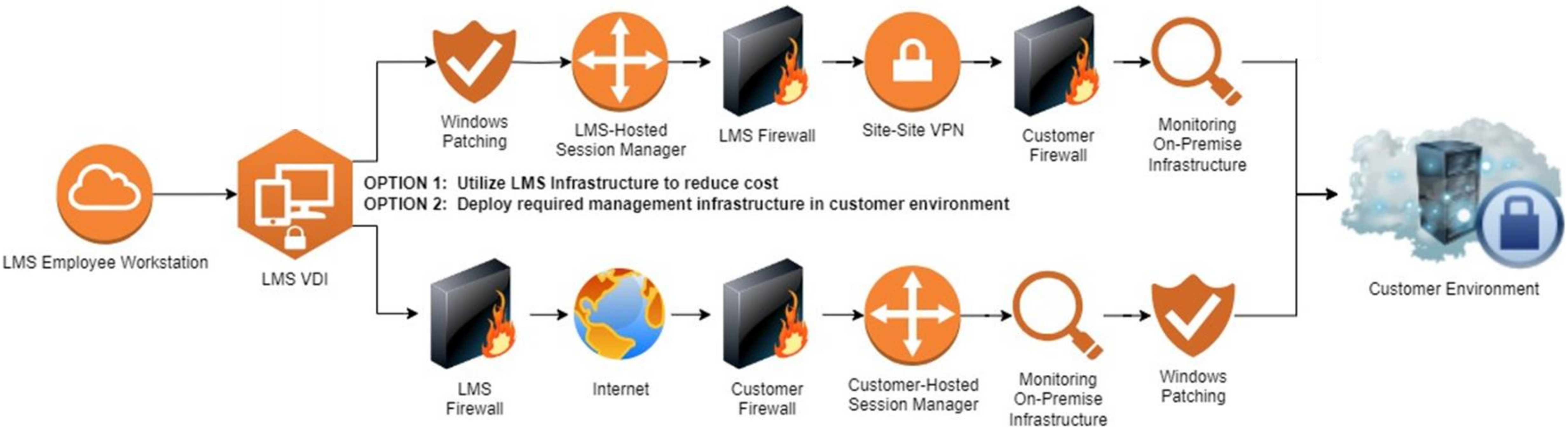
Security is priority, and to ensure strict security between Logicalis and our customers, Logicalis Managed Services uses dedicated Virtual Desktop Infrastructure to connect to supported devices.

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

Access Diagram


LMS Employee Workstation
LMS VDI
Windows Patching
LMS-Hosted Session Manager
LMS Firewall
Site-Site VPN
Customer Firewall
Monitoring On-Premise Infrastructure
OPTION 1: Utilize LMS Infrastructure to reduce cost
OPTION 2: Deploy required management infrastructure in customer environment
LMS Firewall
Internet
Customer Firewall
Customer-Hosted Session Manager
Monitoring On-Premise Infrastructure
Windows Patching
Customer Environment

LOGICALIS
Architects of Change

Thank you