LOGICALIS
Architects of Change

Customer “Onboarding Kit”

MS Security 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

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.

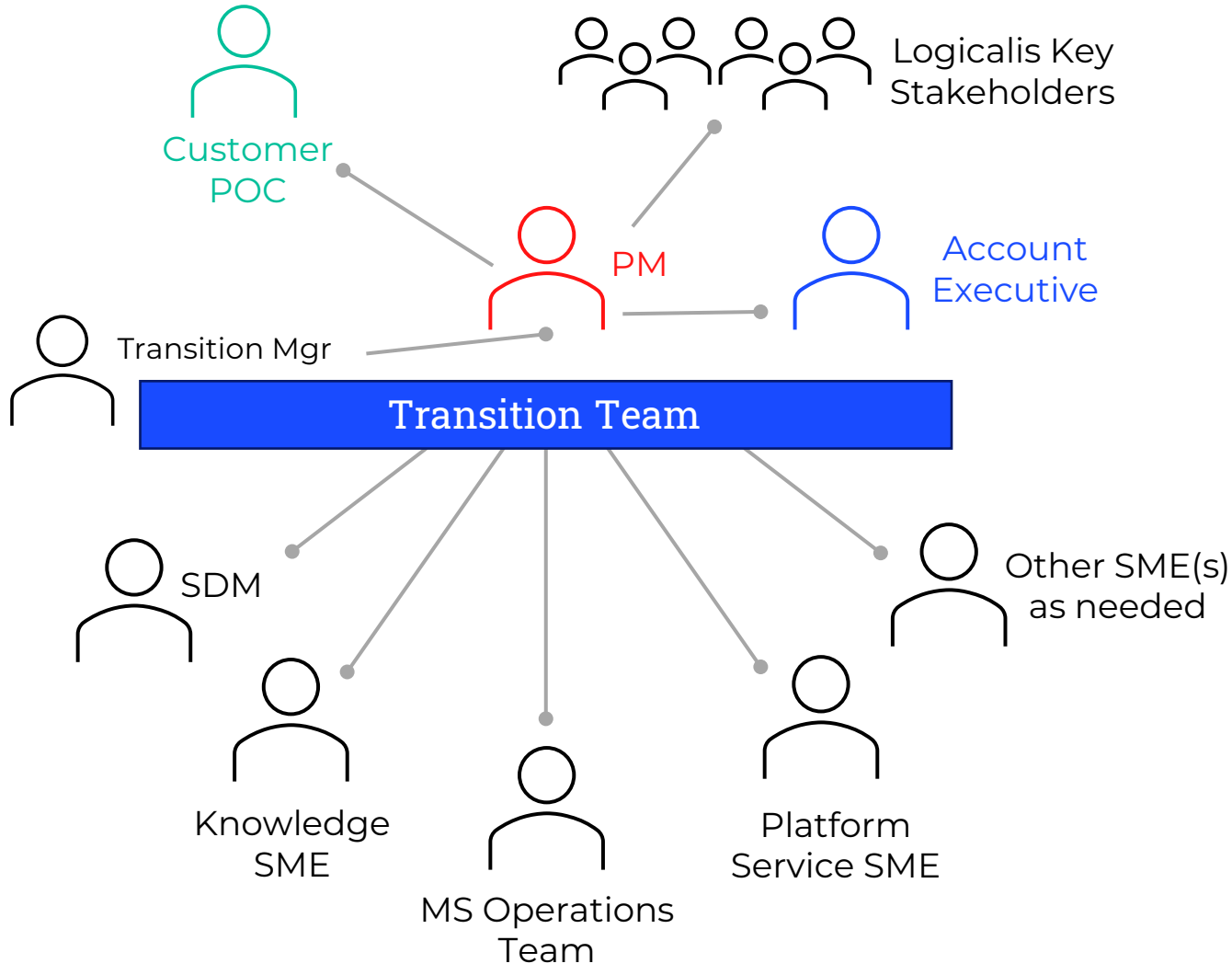
Here are few ways our Customers can facilitate a timely Transition:

- ✓ 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

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.



Logicalis Approach to Transition – Customer View

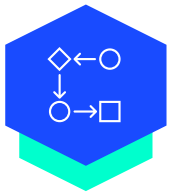
Here are the areas of onboarding where you play a role and in ensuring quality and a timely completion of the Transition

Establish connectivity with your IT environment

Add your customer information to our database

Configure our monitoring device and tools for your environment

Load all of your in-scope supported devices into our tools



Customer enablement for support, communications, ticketing, and reporting systems

Logicalis Customer Requirements

To be successful, Logicalis will need the following from the customer

Connectivity

Our customer is expected to build 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 assistance in provisioning Logicalis device/ environment access accounts with appropriate permissions to deliver the contracted services.

Tools

Provide a VM/server for hosting 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

Managed Services-Security Services

MS Security Services

OnMesh

To be successful, Logicalis will need the following from the customer

- Necessary level of access (temporary) to Customer Azure environment given to **Logicalis Professional Service** to configure Sentinel and reporting tools. Depending on customer environment, Logicalis may need Global or Security access.
- Detailed list of all Data Sources (i.e. Meraki) to be onboarded into the service along with Network design and documentation.
- Documented requirements for compliance frameworks supplied including data retention (PCI/DSS/NIST/ISO27001)
- Documentation of required customer custom user cases. If custom user cases, will need to collaborate with customer contact.
- Access to customer resource with capacity to perform required internal engineering changes for onboarding of a datasource – this can include installation of AMA agent on on-premise servers, provision of server (virtual or physical for Event Log forwarder where required) or forwarding on logs for Firewalls, Switches etc.
- Completion of customer incident escalation document and current customer Change Process.

MS Security Services

Defender for Endpoint

To be successful, Logicalis will need the following from the customer

- Necessary access to Customer Defender environment given to Logicalis Professional Service engineer at the level of “Security Administrator” for Tenant
- Customer Office 365 Account required for Microsoft Defender Logic App
- Detailed list of all endpoint and Servers to be onboarded into the service.
- Documentation of Customers Endpoint deployment mechanism – Intune, SCCM or Group Policy
- Access to customer resource that can perform required internal engineering changes for onboarding of Endpoints/Servers – this can include installation of Endpoint/Server agents, providing information on required policy exclusions, or General Endpoint workshops.
- Completion of customer incident escalation document and confirmation of customer Change Process, along with Rules of Engagement.

MS Security Services

Cisco Next-Gen Firewall (FirePower)

To be successful, Logicalis will need the following from the customer

- Direct access to customer firewall environment and FMC.
- Provision of server environment for Logicalis Utility VM
- Documentation of Network design or diagram
- Access to customer resource with capacity during Health Check period to ask any relevant Firewall rule or design questions.
- Completion of customer incident escalation document and confirmation of customer Change Process.

MS Security Services

Fortigate Next-Gen Firewall

To be successful, Logicalis will need the following from the customer

- Access to customer firewall environment, or Fortimanager/FortiAnalyser as applicable
- Provision of server environment for Logicalis Utility VM *(for firewall configuration backup, jump server, etc., as applicable)*
- Documentation of Network design or diagram
- Access to customer resource with capacity during Health Check period to ask any relevant Firewall rule or design questions.
- Completion of customer incident escalation document and confirmation of customer Change Process.

MS Security Services

Palo Alto Next Gen Firewall

To be successful, Logicalis will need the following from the customer

- Access to customer firewall environment, or Palo Alto Panorama as applicable.
- Provision of server environment for Logicalis Utility VM *(for firewall configuration backup, jump server, etc., as applicable)*
- Documentation of Network design or diagram
- Access to customer resource with capacity during Health Check period to ask any relevant Firewall rule or design questions.
- Completion of customer incident escalation document and confirmation of customer Change Process.

MS Security Services

Vulnerability Services

To be successful, Logicalis will need the following from the customer

- Access to customer Vulnerability Management tool
- Detailed list of all required devices in scope to be scanned along with Network design and documentation, including any required exclusions.
- Access to customer resource with capacity during Health Check period to ask any vulnerability scanning question, including any potential Licensing requirements or internal engineering requirements for additional device agents or scanning appliances.
- Completion of customer incident escalation document and confirmation of Customer Change Process.
- Confirmation of existing Vulnerability platform design and methodology of Vulnerability Management Lifecycle

LOGICALIS
Architects of Change

Establishing Connectivity

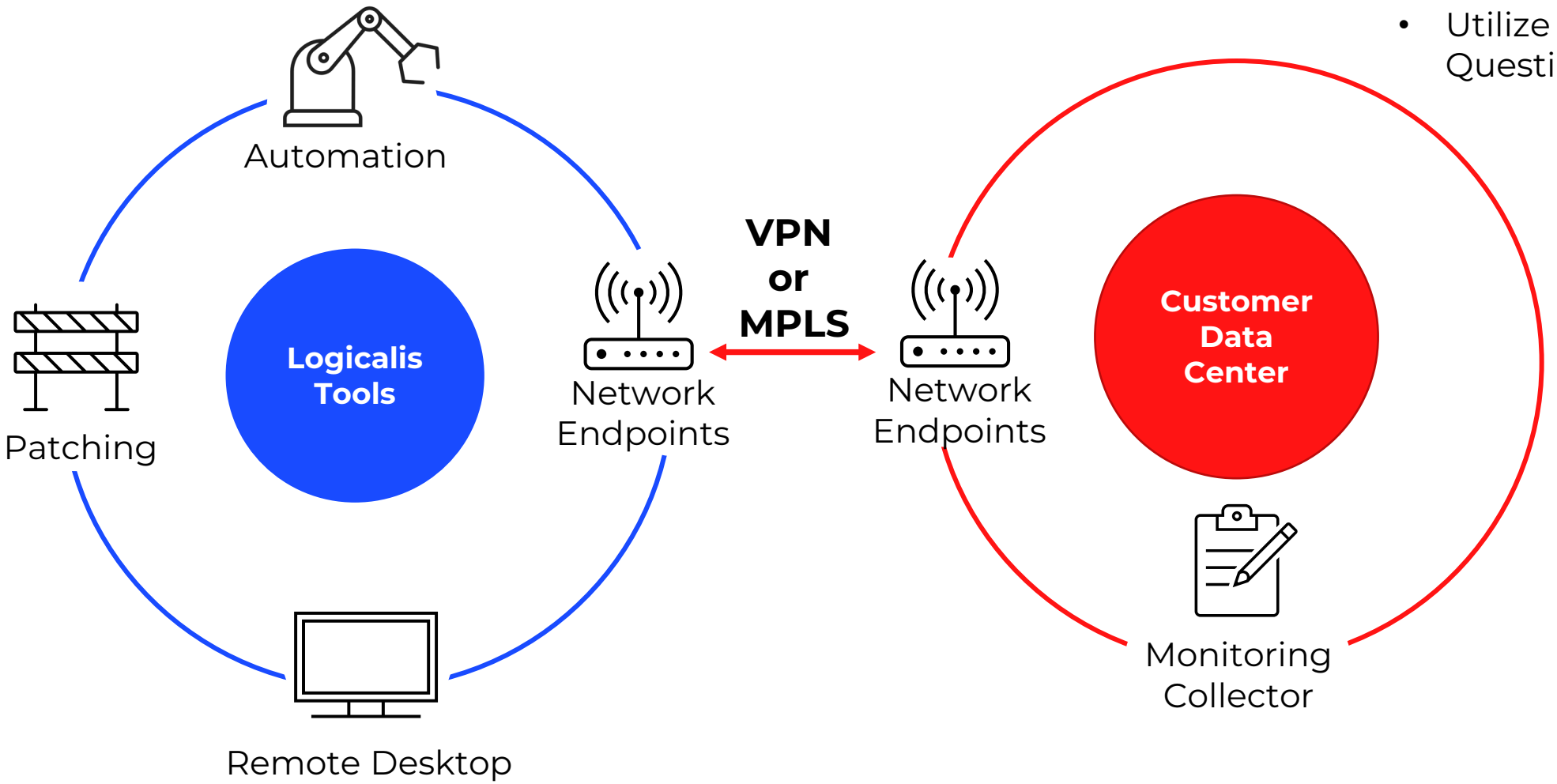
Step 1

Establishing Connectivity (options)

LOGICALIS
Architects of Change

Questions:

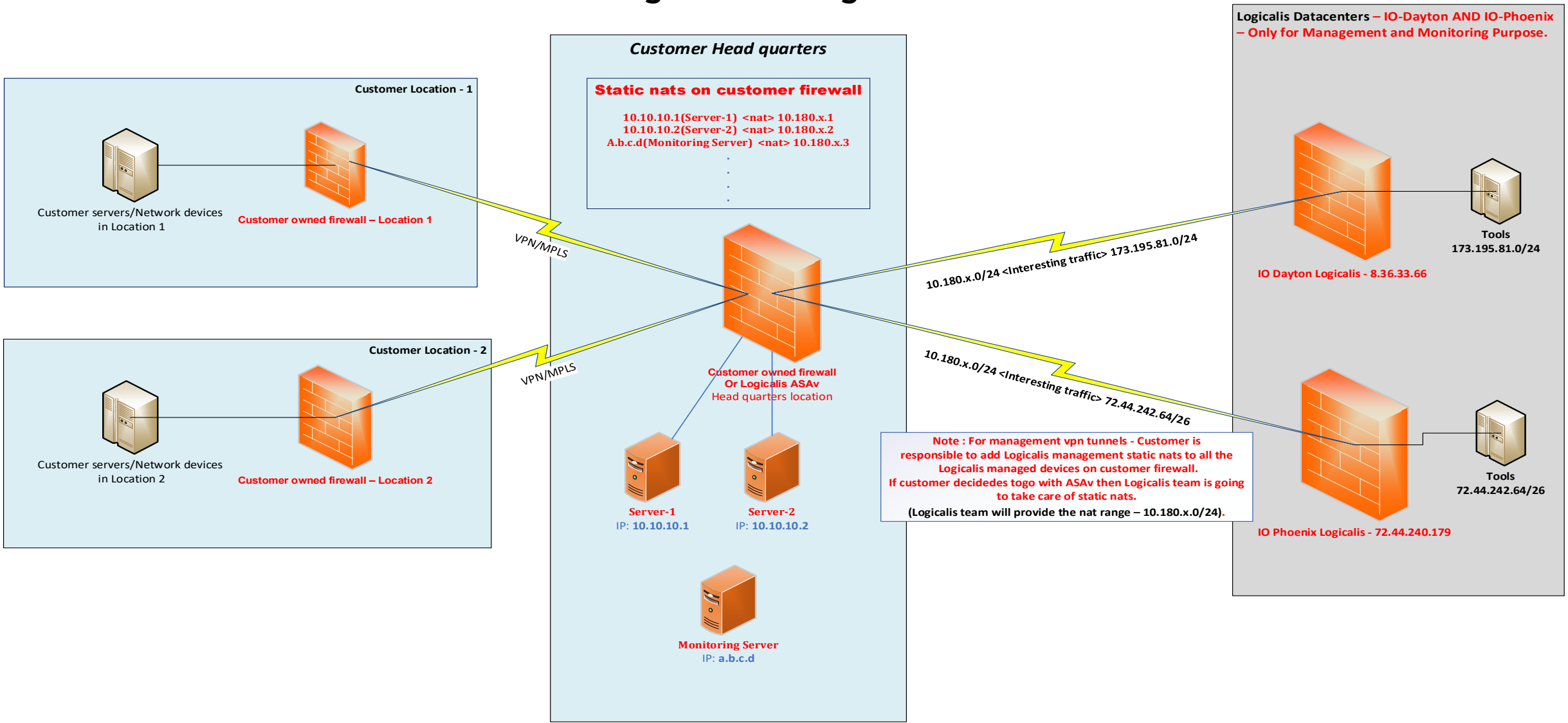
- How will we connect to customer data centers?
- Utilize our connectivity Questionnaire?



Step 1 – Connectivity

VM hosted VPN ASAv Server Specifications and Information

VPN Tunnel Diagram from Logicalis to Customer



LOGICALIS
Architects of Change

Onboarding Steps

Step 1 – Connectivity

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

DFP Monitoring Tool

The Windows Collector is a physical or virtual server used by Logicalis for all device monitoring contracts. This document provides details on the collector itself and the standard practices used to deploy the collector.

Customer Connectivity Requirements

- Open appropriate ports to allow connectivity to end devices and for Logicalis access to maintain collector
- Provide VM to host the DFP Monitoring Tool in customer's infrastructure with access to both in scope supported devices
- Internet access for the DFP Monitoring Tool to patch OS & install DFP 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

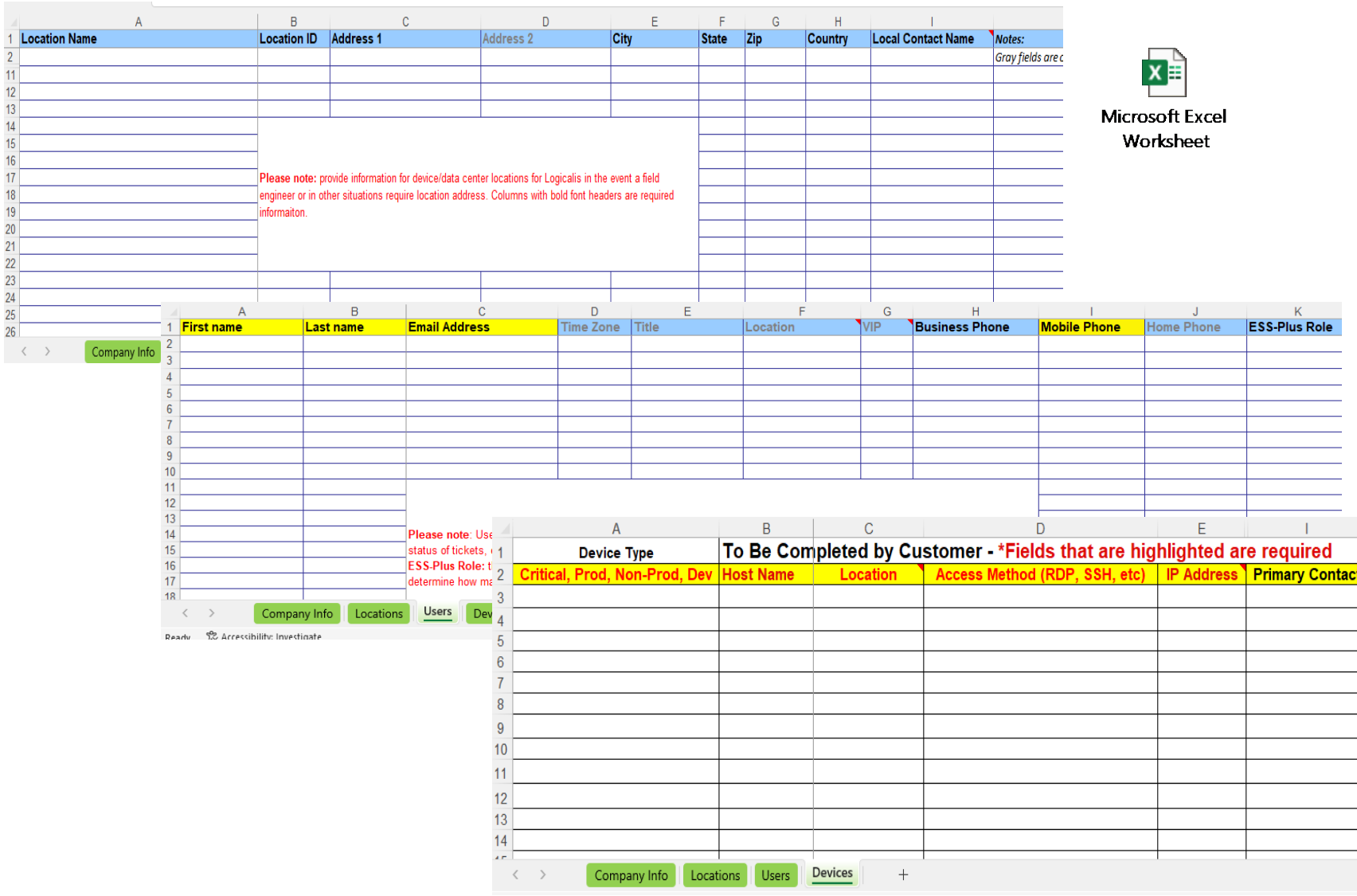
Customer Server Build Requirements

- 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 the DFP Monitoring Tool

LM Collector Deployment Guide

Step 3

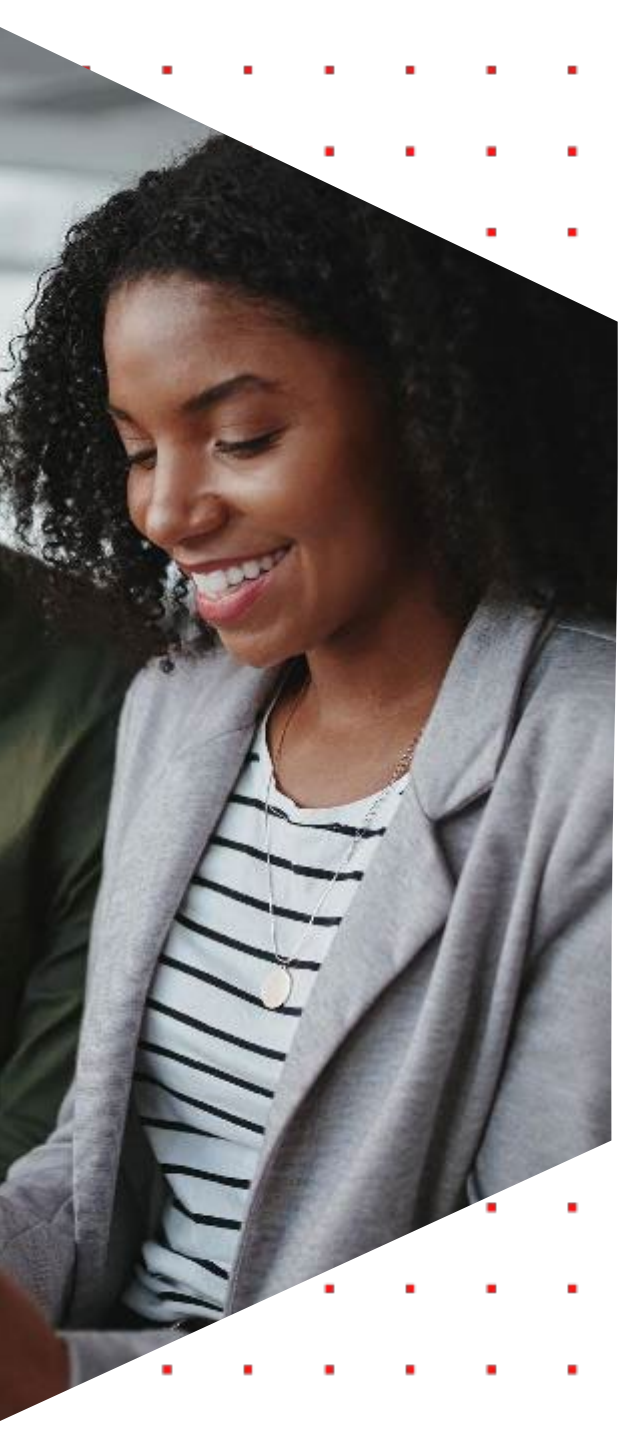
Collect Information on Supported Devices (CMDB)



Microsoft Excel Worksheet

Configuration Item Information

- Location address of all devices
- User information for who will need access to DFP (ITSM tool)
- Device information (hostname, IP, location, Primary contacts, etc.)



Step 4

Logicalis ITSM Tool –Digital Fabric Platform (DFP)

Information Loaded in DFP by the Logicalis Transition Manager:

- Company Information (Name/Address)
- Users – contacts that will receive incident notifications, provide change approvals, require access to the DFP portal, etc.
- CMDB – central repository for device information
- Transition Project – project with required tasks to be completed by Logicalis Managed Services

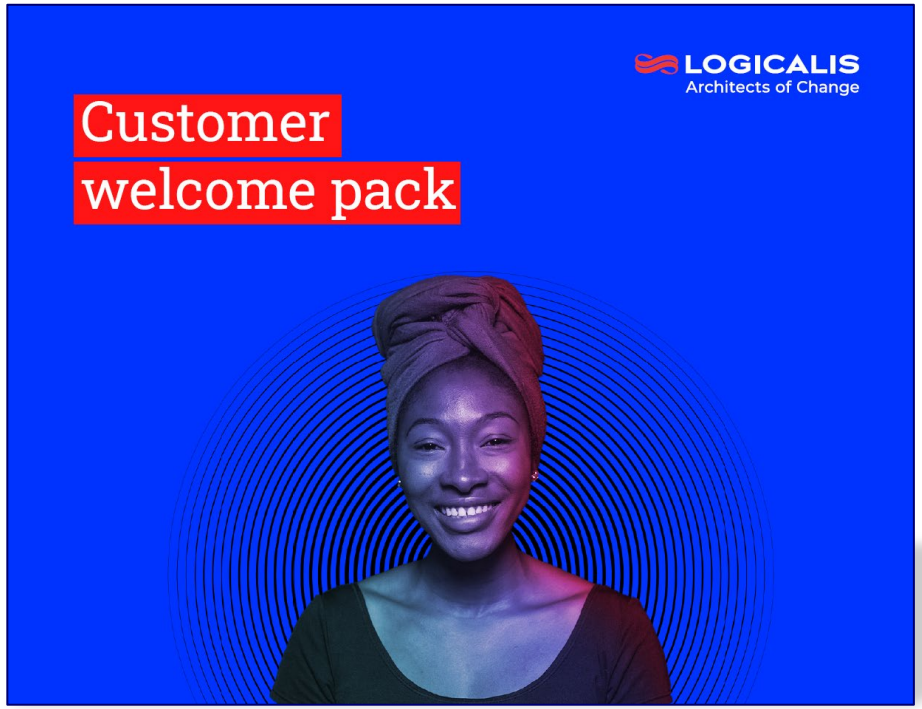
Step 5

Customer Enablement for Tools, Process, Reporting, etc.

Logicalis "Customer Welcome Pack"

- ✓ Escalation & contact Information
- ✓ Portal Training - How to open incident or request
- ✓ Navigating the DFP Portal
- ✓ How to view reporting

The Logicalis SDM will schedule time to provide Customer training



LOGICALIS
Architects of Change

Q&A

LOGICALIS
Architects of Change

Thank you