alfa connections

Microsoft Cybersecurity Solution Assessment

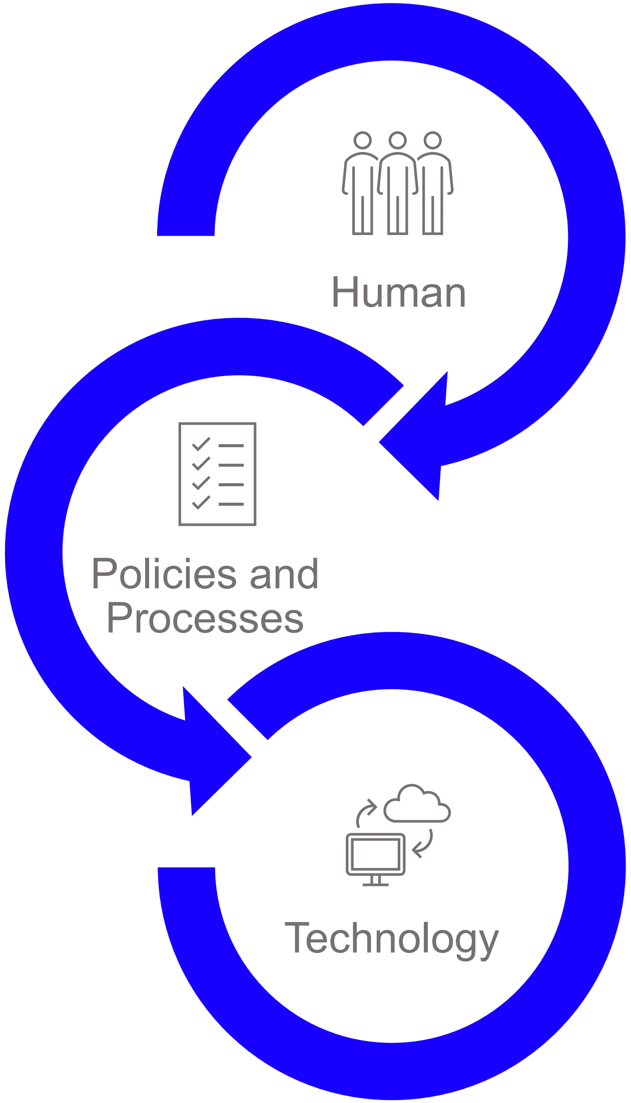
CSAT

Singapore | Malaysia | Vietnam | Thailand | Philippines | Myanmar | Indonesia

Agenda

Cybersecurity Overview
CSAT concept and workings
Technical Pre-requisites
Project Timeline

Cybersecurity Overview



Staff Training and Security Awareness
Enhance human Firewall

Define how the organization's activities, roles and documentation are used

Identify cyber risks to look at what tools and controls to put in place

Methodology

Goals

- Provide an analysis of your cybersecurity maturity status, visibility and insights into security.
- Assessment of cybersecurity-related policies and procedures.
- Help to create a cybersecurity roadmap to better protect your IT assets.

Deliverables

- Final report with analysis of current cybersecurity status.
- Cybersecurity maturity with CIS controls v7.1 framework (released April 2019).
- Recommendations based on facts.
- Cybersecurity improvement with an action plan.

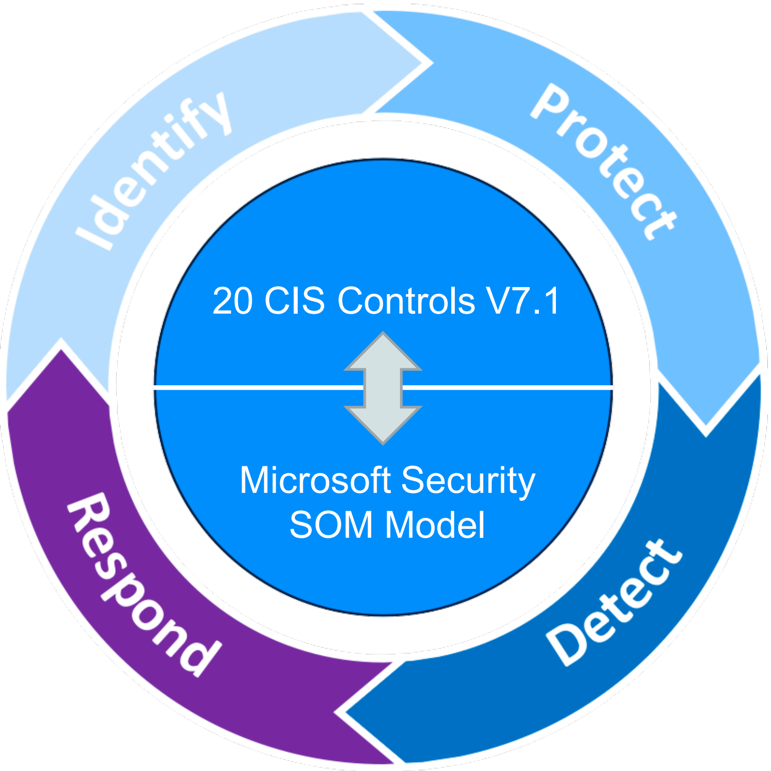
Stakeholders

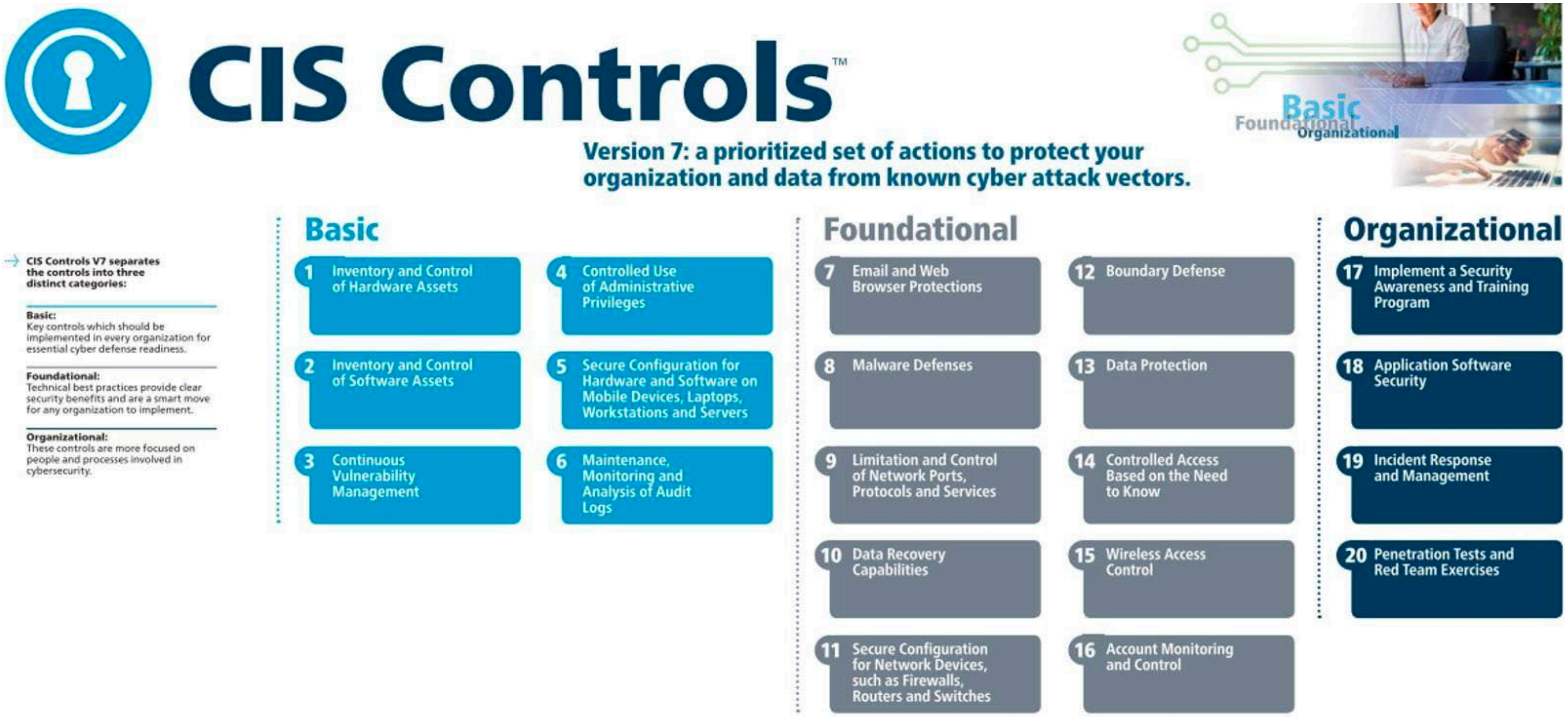
Performed by Microsoft Partners

- Alfa Connections in cooperation with Microsoft Local Partner or Microsoft Local.
- Assessment and Final Report by Alfa Connections.
- Follow-up actions by Microsoft Local Partner.

Methodology

- Assessment is performed using CSAT tool developed by Microsoft ISV Global Partner QS Solutions
- Cybersecurity maturity is based on CIS controls v7.1 framework and Microsoft security SOM Model





CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

Basic
Foundational
Organizational

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Source: Microsoft 365 + the NIST cybersecurity framework

alfa connections

CSAT Concept And Workings

What Do We Need To Deliver The Final Report?

Consultancy Services

CSAT

An on-premise tool to be installed on a Server / VM

- Data Collection
- Questionnaire answering
- Creating of Final Report

Automated Technical Scan

- Collect security related data from your IT environment
- Analyse technical data

Questionnaire / Interview

- Collect organizational and procedural security information
- Based on the Microsoft CIS v7.1 Cybersecurity Questionnaire

CSAT

The Cybersecurity Assessment Tool is a software product developed by experienced security experts. It collects relevant data from:

Endpoints
(Windows & Linux OS)

Office 365
SharePoint & Intune

Active Directory &
Azure AD

Gsuite & Network
Devices (SNMP)

alfa connections

Technical Pre-requisites

CSAT Server - Recommended Hardware

UP TO DATE
WINDOWS OS

4 CPU CORES
FROM 1 CPU SOCKET

CPU

RAM
8-16 GB

SSD / HDD
AT LEAST 80 GB

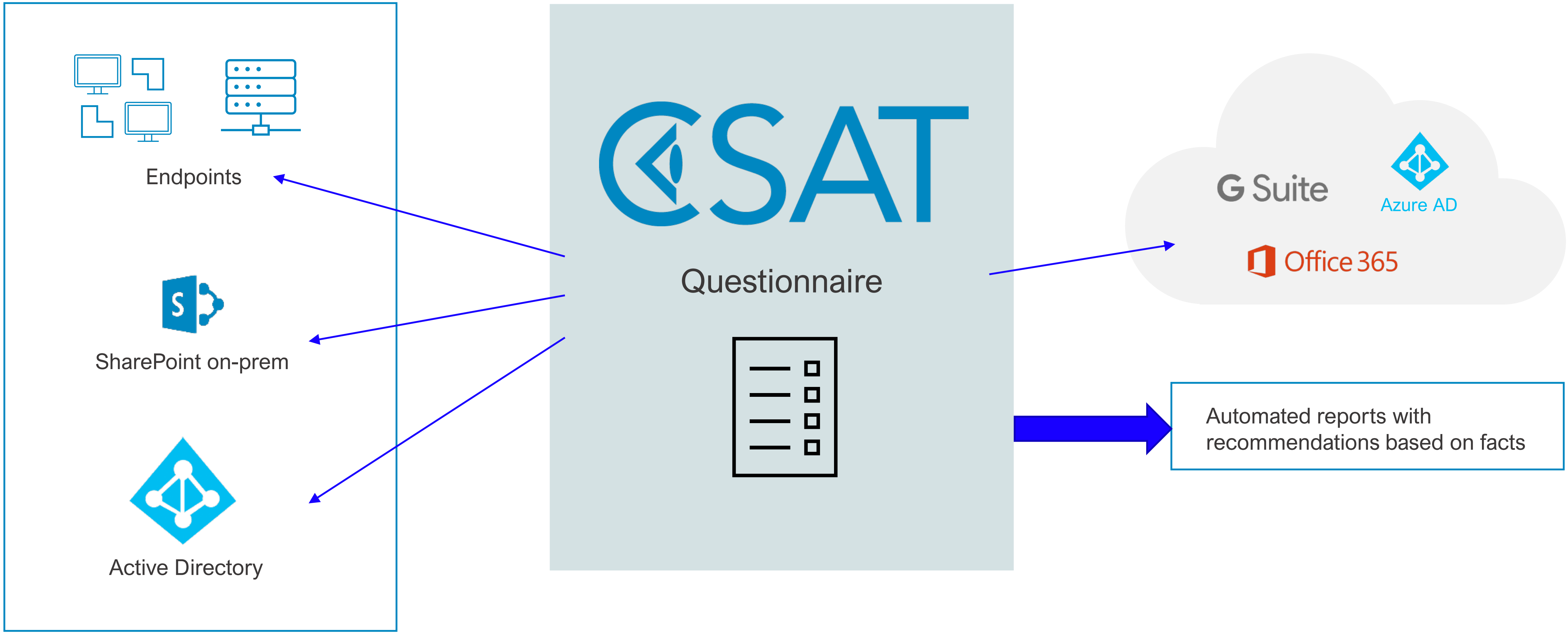
4.6 OR HIGHER

Microsoft
.NET

SCREEN
1920 X 1080

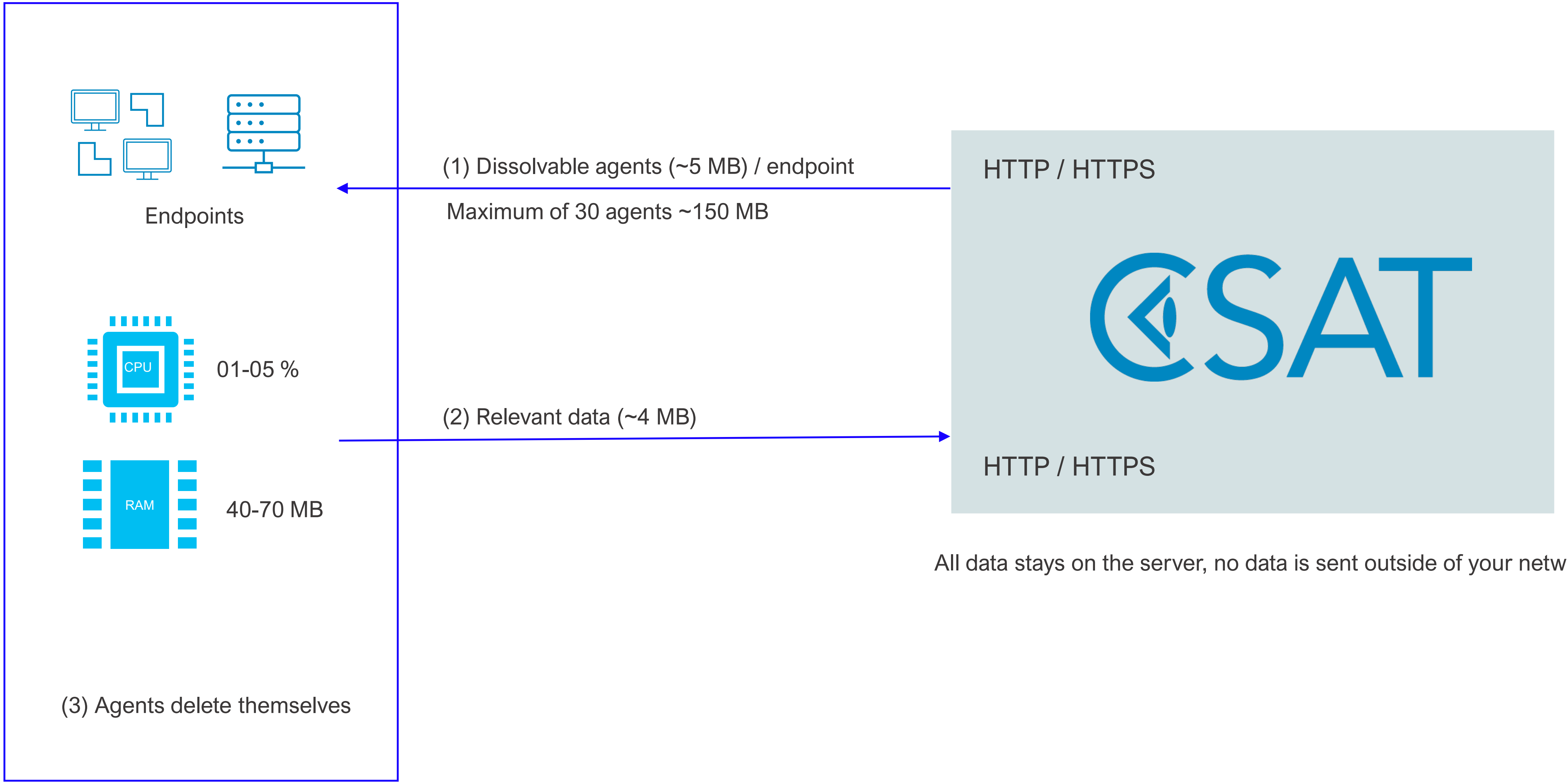
Data Collection

By using agents which delete themselves following the endpoint scan, effort required from the internal IT department is kept to a minimum.



Automated reports with recommendations based on facts

Network Traffic



Endpoints

CPU 01-05 %

RAM 40-70 MB

(1) Dissolvable agents (~5 MB) / endpoint

Maximum of 30 agents ~150 MB

(2) Relevant data (~4 MB)

HTTP / HTTPS

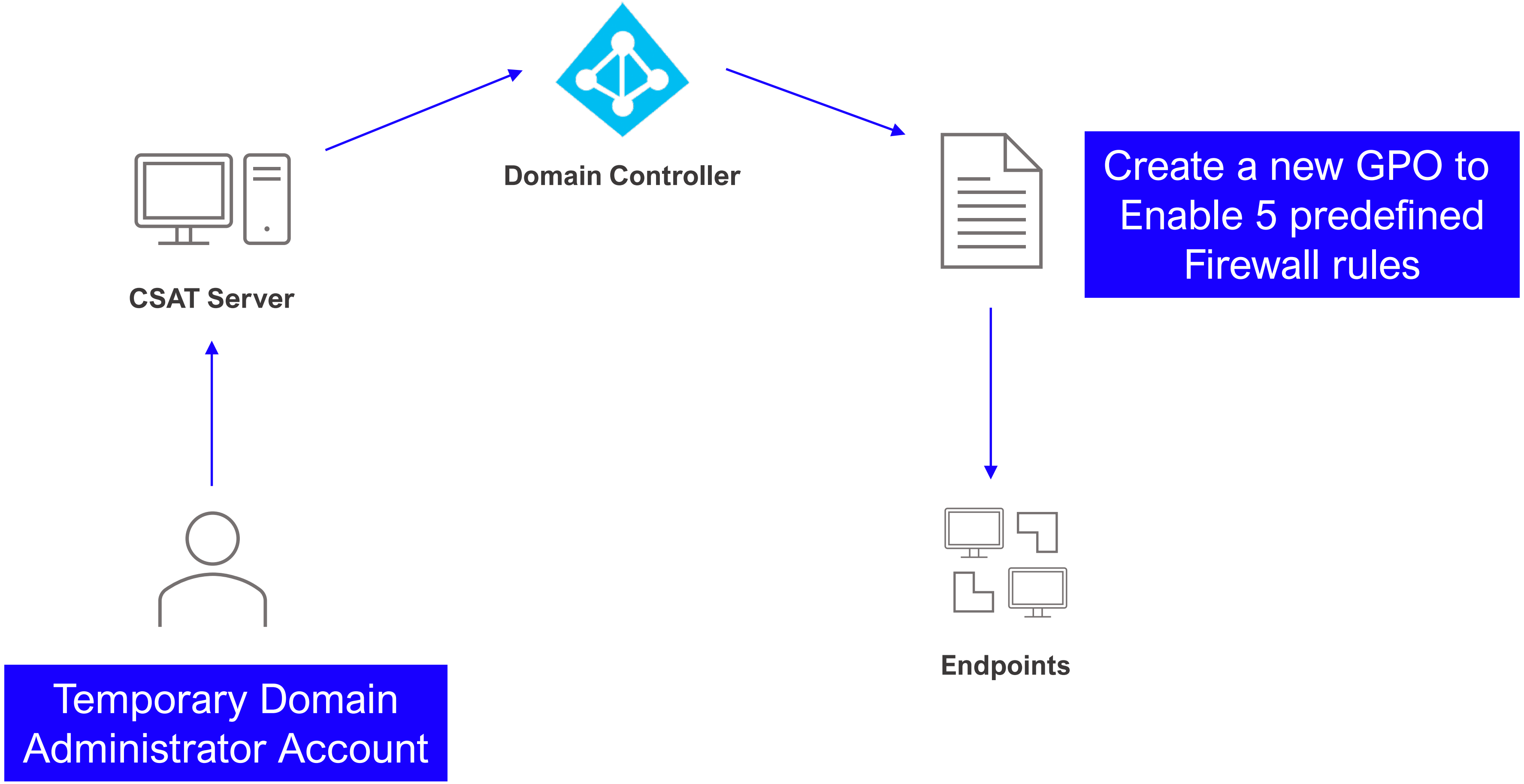
CSAT

HTTP / HTTPS

(3) Agents delete themselves

All data stays on the server, no data is sent outside of your network

Managed Environment (Active Directory)


Domain Controller
CSAT Server
Create a new GPO to Enable 5 predefined Firewall rules
Endpoints
Temporary Domain Administrator Account

Note: GPO will need some time to apply its policy to entire endpoints in the OU, this should be done before **2-3 days** of the scan.

Endpoints

The following inbound firewall rules are needed to be enabled for the active firewall profile on the endpoint that you want to scan:

Firewall Rule Name	Group	Port
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	139
File and Printer Sharing (NB-In)	File and Printer Sharing	445
Remote Scheduled Task Management (RPC)	Remote Scheduled Task Management	RPC Dynamics Ports
Windows Management Instrumentation (DCOM-In)	Windows Management Instrumentation	135
Windows Management Instrumentation (WMI-In)	Windows Management Instrumentation	All (only allow svchost.exe)

Exceptional case *(mostly for TrendMicro and Symantec Antivirus)*:
if customer uses 3rd party Antivirus software, an additional configuration on management console is required.

CSAT Server – Supported OS Version

Prepare a **FRESH** OS installation on customer's server/VM with one of the below supported Windows OS Version to install CSAT

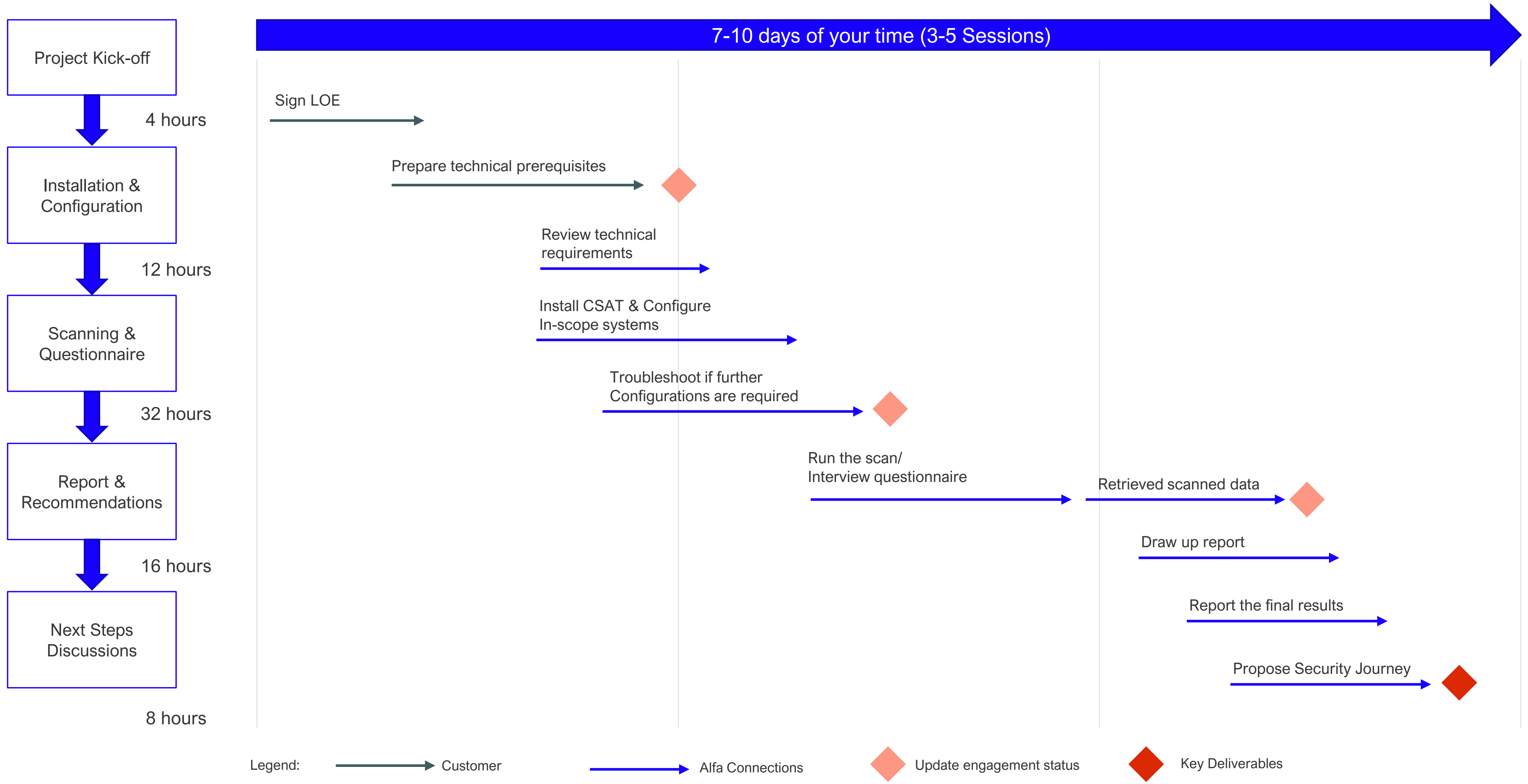
WINDOWS SERVER 2016

WINDOWS SERVER 2019

WINDOWS 10 PRO OR ENT

BUILD 1607 OR HIGHER

Assessment Timeline



Project Kick-off

4 hours

Installation & Configuration

12 hours

Scanning & Questionnaire

32 hours

Report & Recommendations

16 hours

Next Steps Discussions

8 hours

7-10 days of your time (3-5 Sessions)

Sign LOE

Prepare technical prerequisites

Review technical requirements

Install CSAT & Configure In-scope systems

Troubleshoot if further Configurations are required

Run the scan/ Interview questionnaire

Retrieved scanned data

Draw up report

Report the final results

Propose Security Journey

Legend: → Customer → Alfa Connections ◆ Update engagement status ◆ Key Deliverables