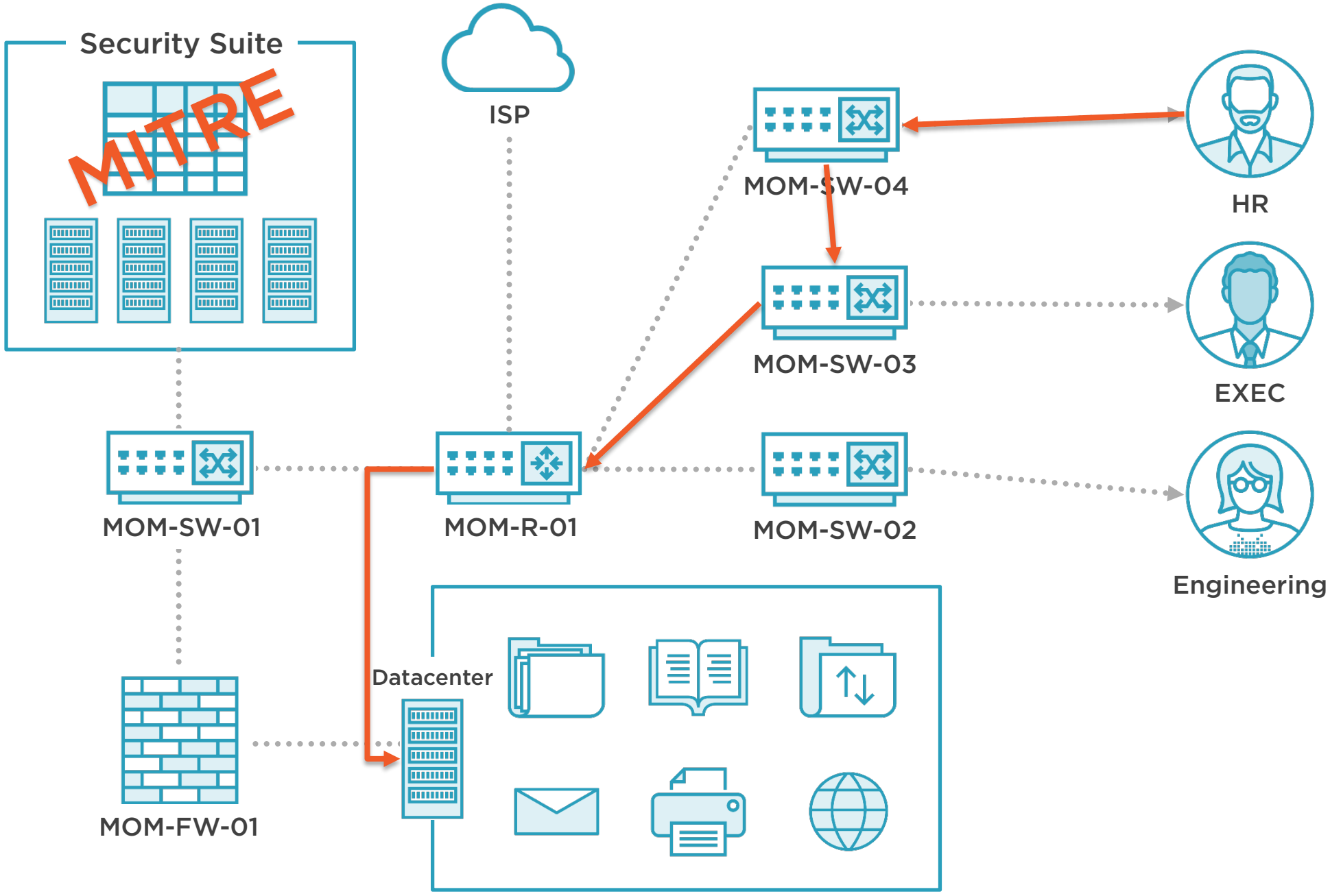
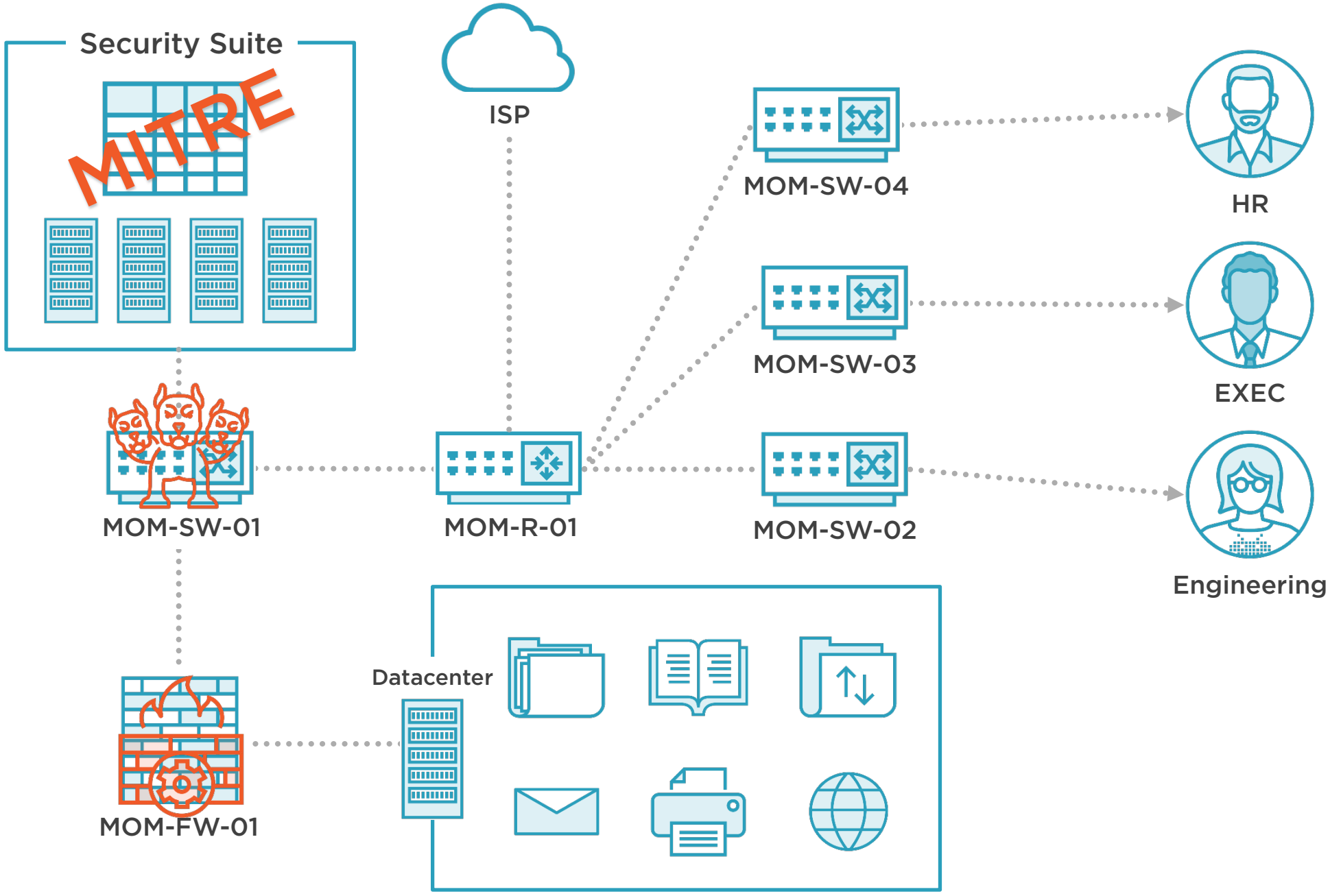
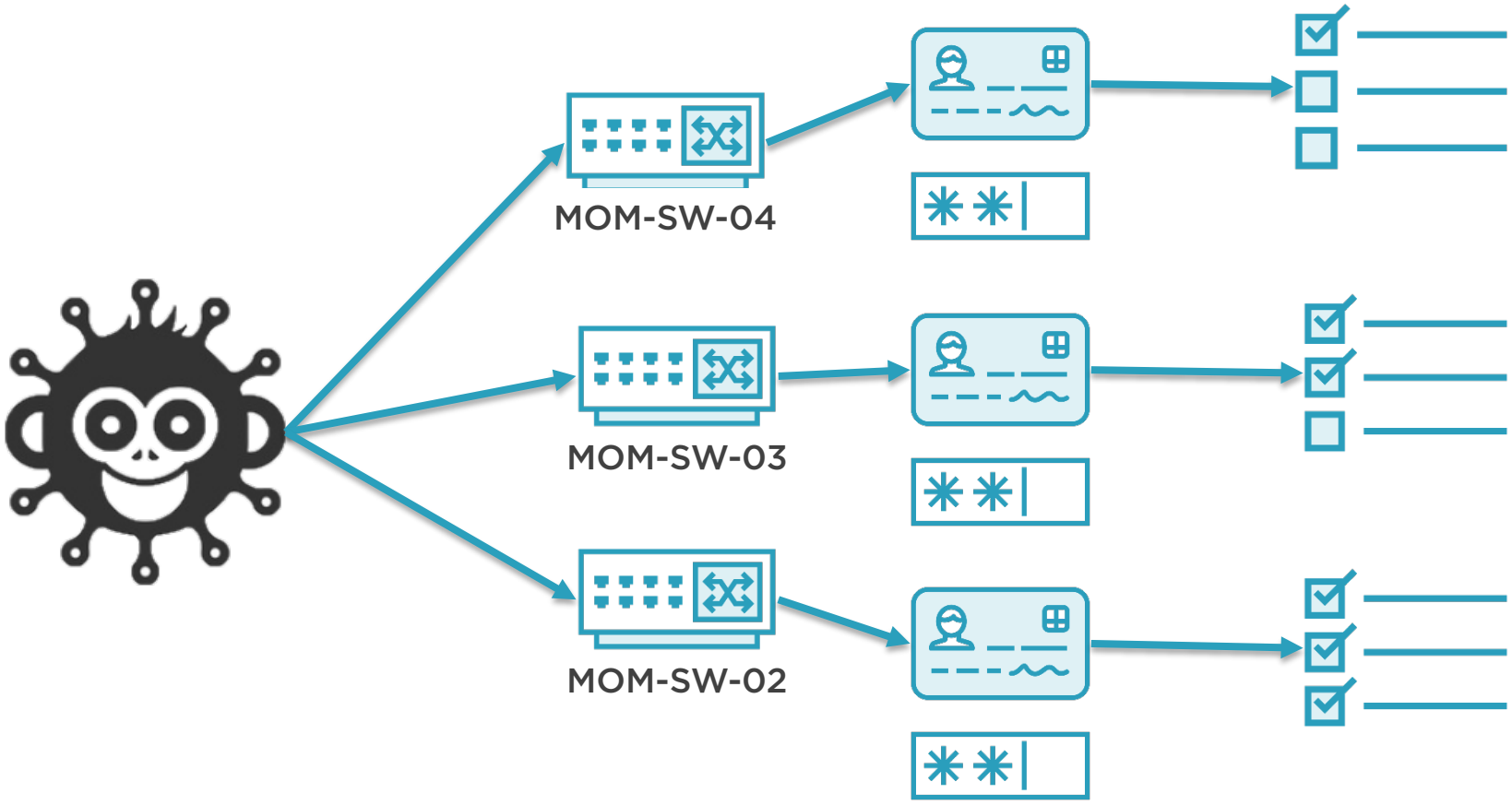
Lateral Movement with Infection Monkey

Maril Vernon
PENETRATION TESTER

@shewhohacks linkedin.com/in/marilvernon


Security Suite
MITRE
ISP
MOM-SW-04
HR
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01


Security Suite
MITRE
ISP
MOM-SW-04
HR
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01


MOM-SW-04
MOM-SW-03
MOM-SW-02

Overview

Discovers, compromises, and maps networks in real time

Rogue asset detection

Demo: Lateral Movement

- MITRE ATT&CK testing
- Zero Trust

Demo: Network Segmentation

- Secondary controls

Creator: Guardicore

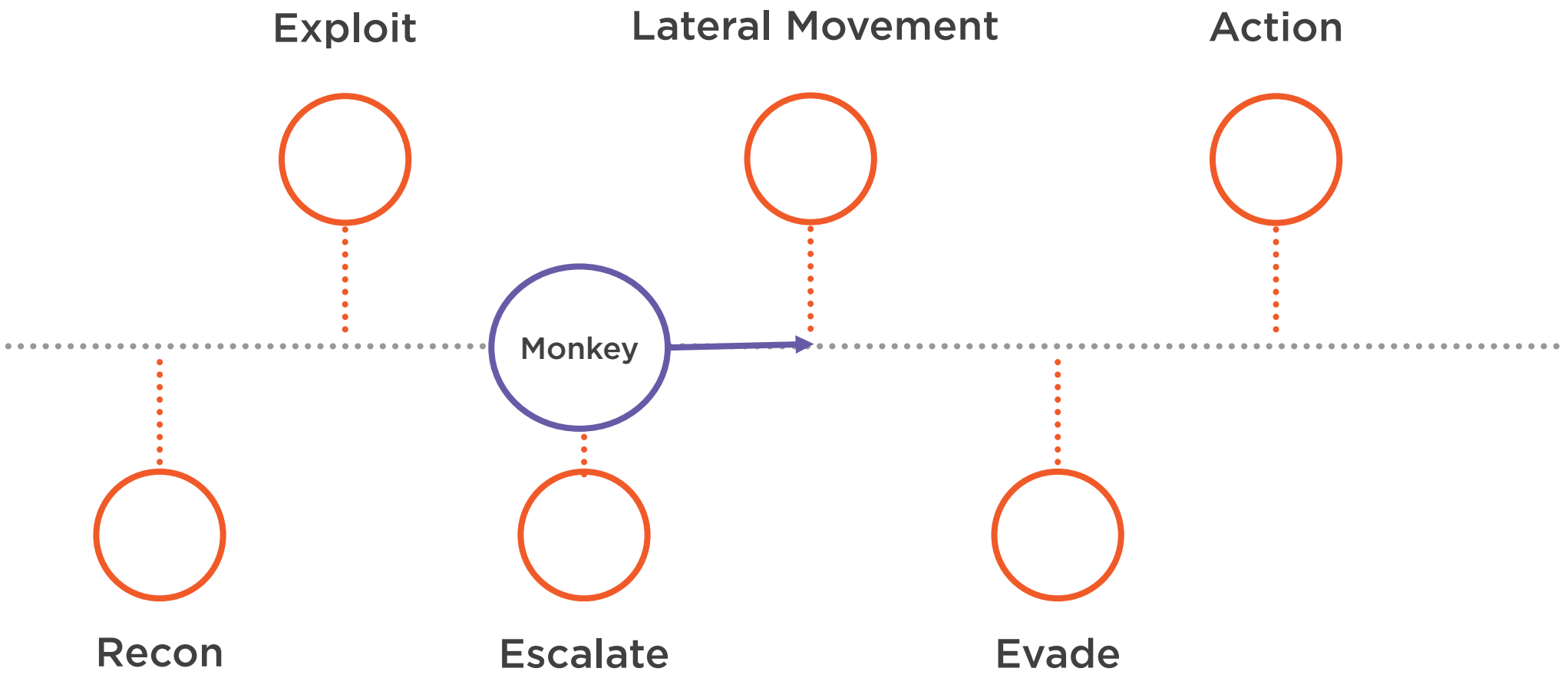
The Infection Monkey is an open source security tool for testing a network's to perimeter breaches and internal server infection. The Monkey uses built-in exploits to self propagate across a system and reports success to a centralized Monkey Island server.

Infection Monkey is downloadable through Guardicore's website in any available platform format.

Infection Monkey is a self-propagating payload that scans, discovers, and compromises connected hosts on a network.

The Monkey is not adversary emulation. Payloads are real.

Kill Chain

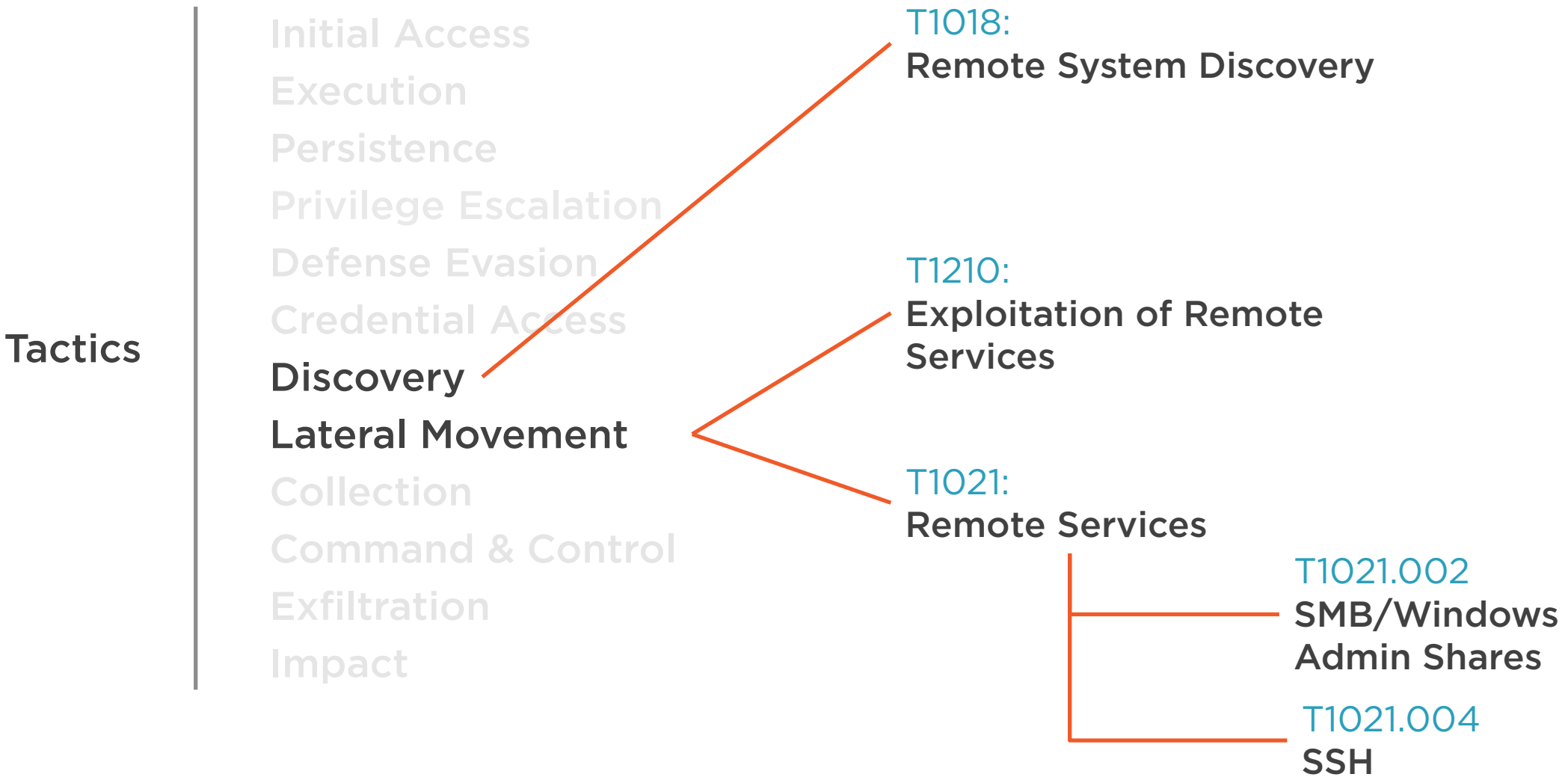

Exploit
Lateral Movement
Action
Monkey
Recon
Escalate
Evade

Infection Monkey and MITRE ATT&CK

MITRE ATT&CK

Tactics	Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Command & Control Exfiltration Impact

MITRE ATT&CK


Tactics
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact
T1018:
Remote System Discovery
T1210:
Exploitation of Remote Services
T1021:
Remote Services
T1021.002
SMB/Windows Admin Shares
T1021.004
SSH

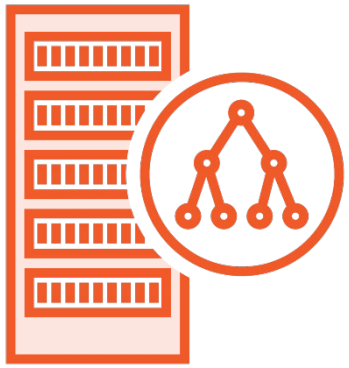
Zero Trust Model

Zero Trust Model

"Never trust, always verify"

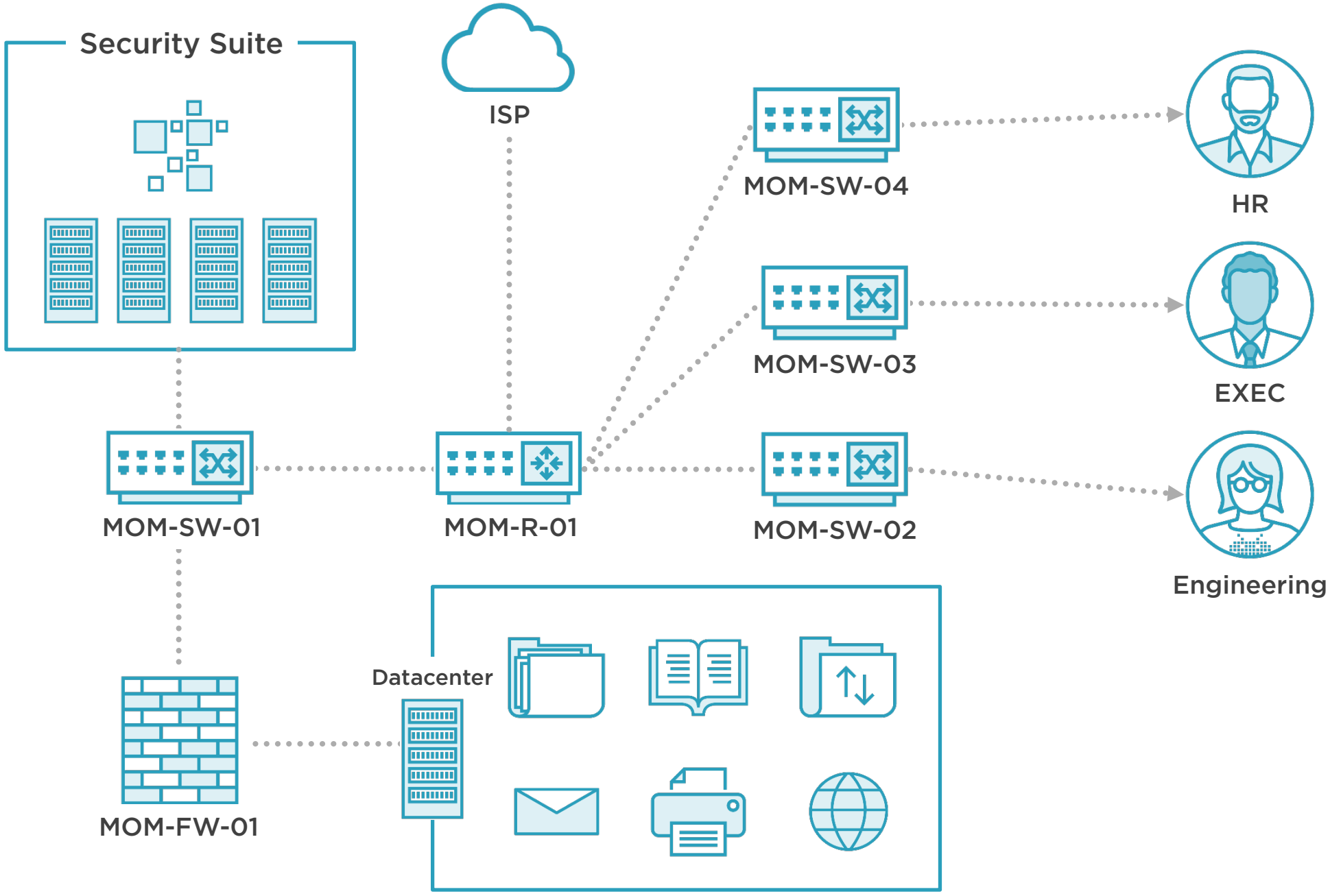
Zero Trust Framework

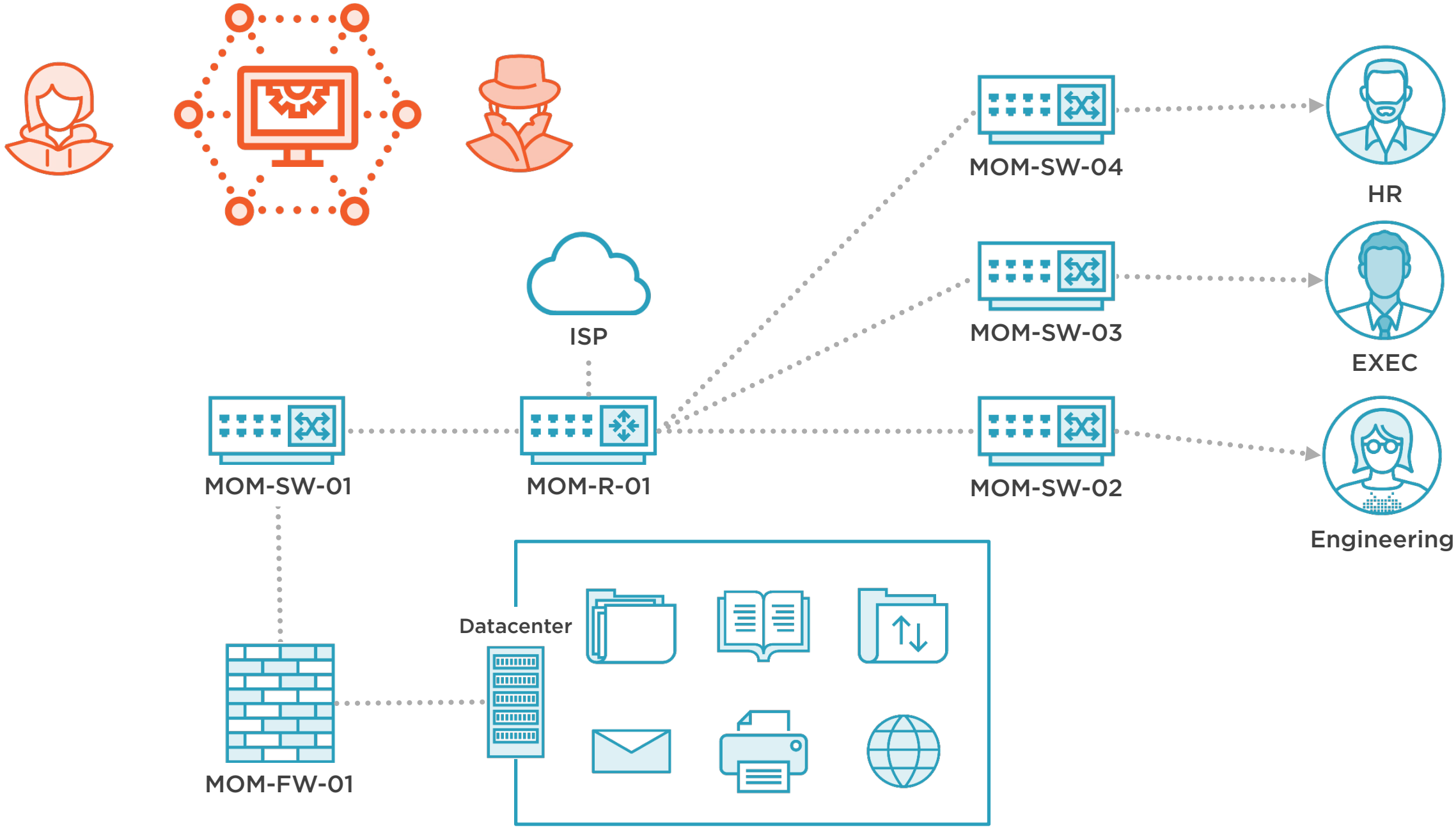
Verify explicitly

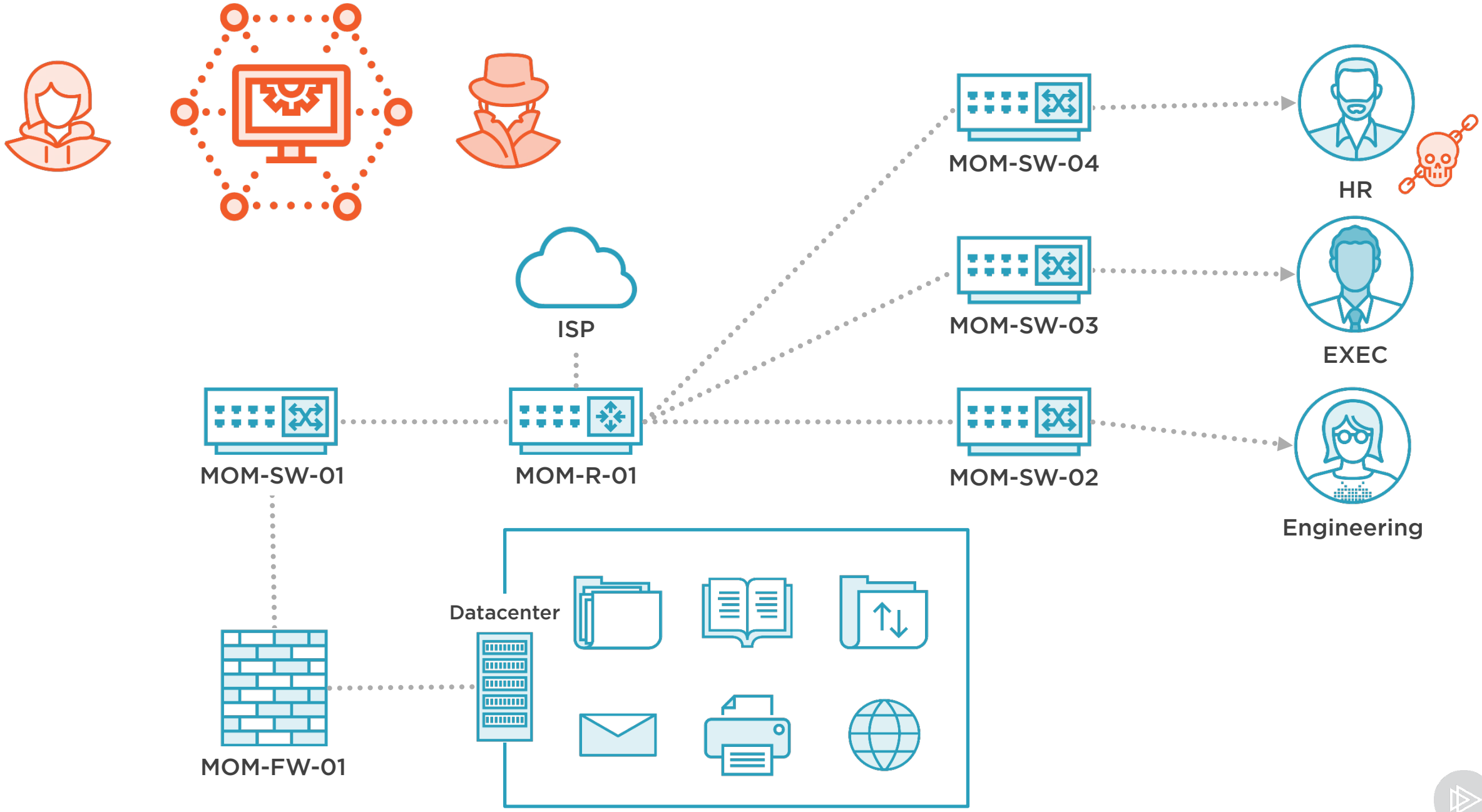


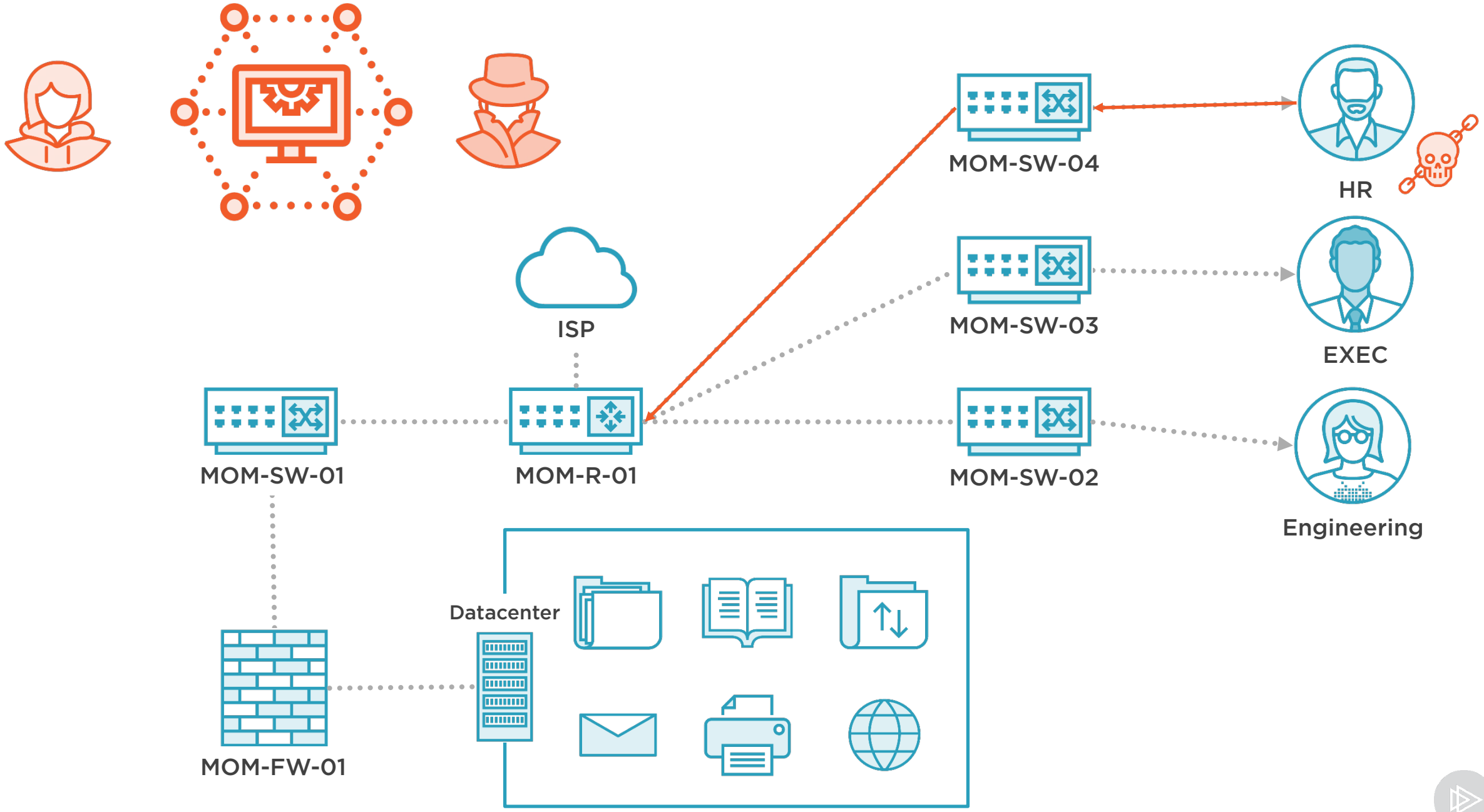
Least privilege access

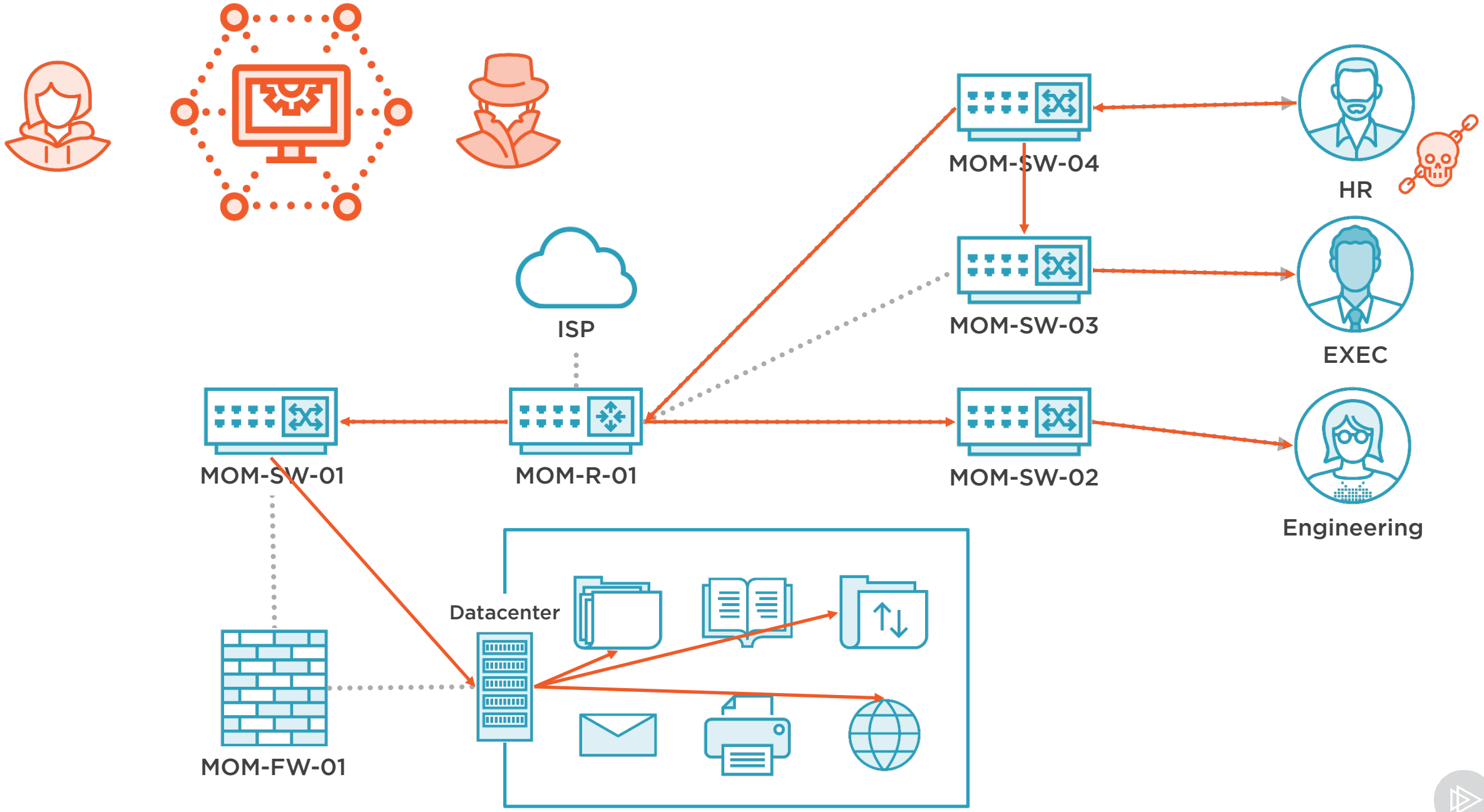
Assume breach

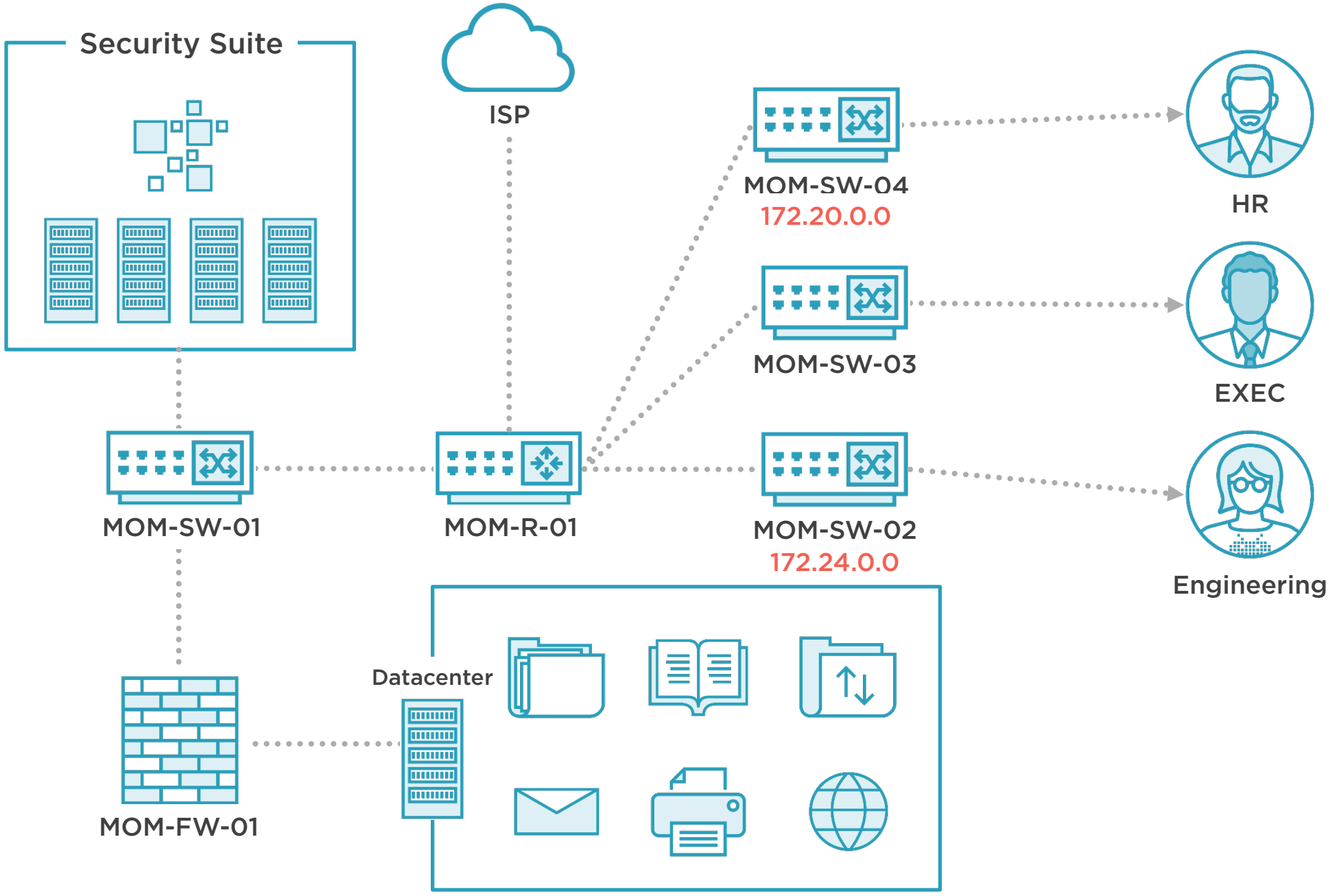

Security Suite
ISP
MOM-SW-04
HR
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01

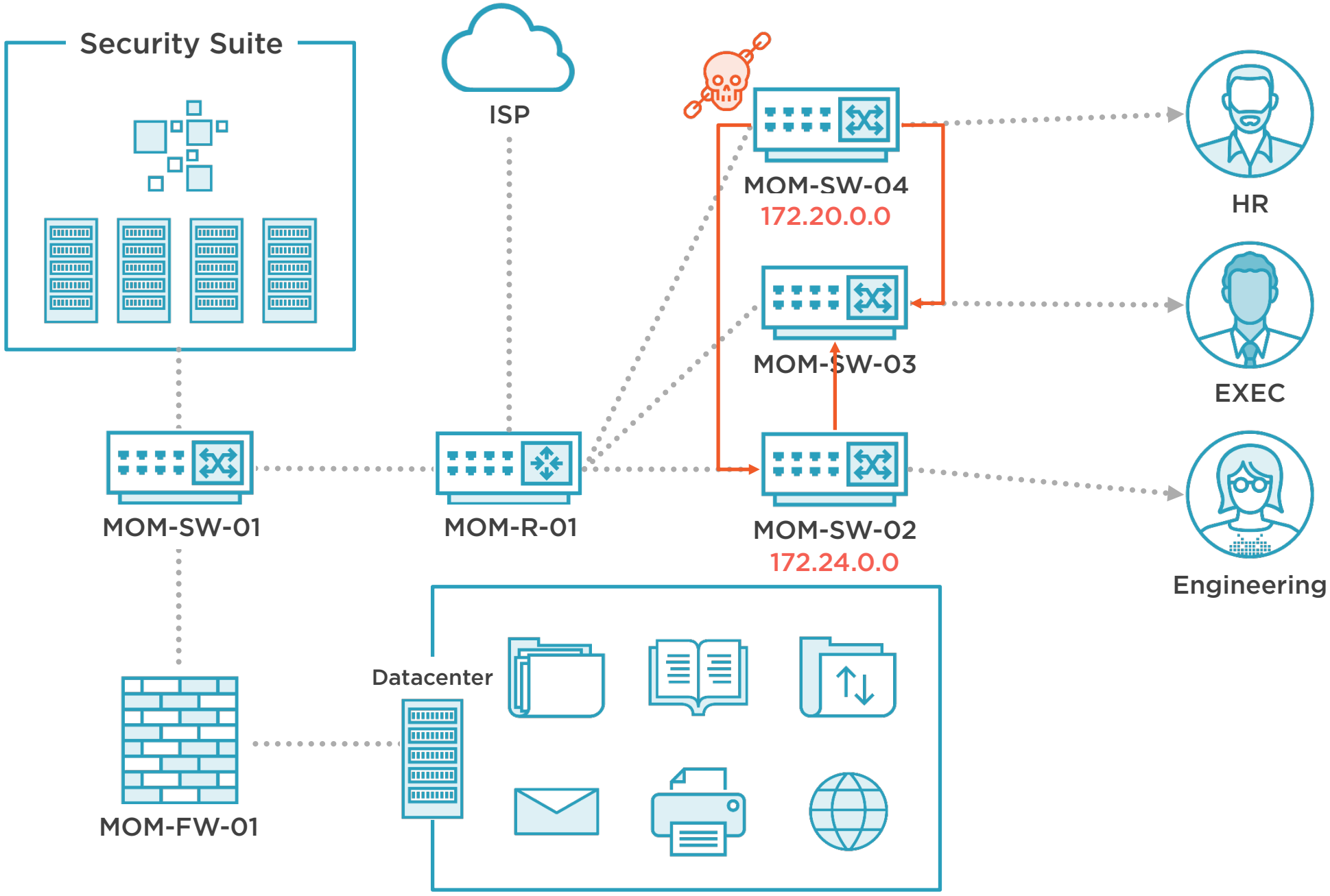

MOM-SW-04
HR
ISP
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01


MOM-SW-04
HR
ISP
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01


MOM-SW-04
HR
MOM-SW-03
EXEC
ISP
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01


MOM-SW-04
HR
MOM-SW-03
EXEC
ISP
MOM-SW-01
MOM-R-01
MOM-SW-02
Engineering
Datacenter
MOM-FW-01


Security Suite
ISP
MOM-SW-04
172.20.0.0
HR
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
172.24.0.0
Engineering
Datacenter
MOM-FW-01


Security Suite
ISP
MOM-SW-04
172.20.0.0
HR
MOM-SW-03
EXEC
MOM-SW-01
MOM-R-01
MOM-SW-02
172.24.0.0
Engineering
Datacenter
MOM-FW-01

Demo Place Holder

1. Installation Tips and Tricks

2. First use instructions & common usage syntax

3. Use of main features on live targets or in live environment

Demo 1: Lateral Movement

Demo 2: Network Segmentation