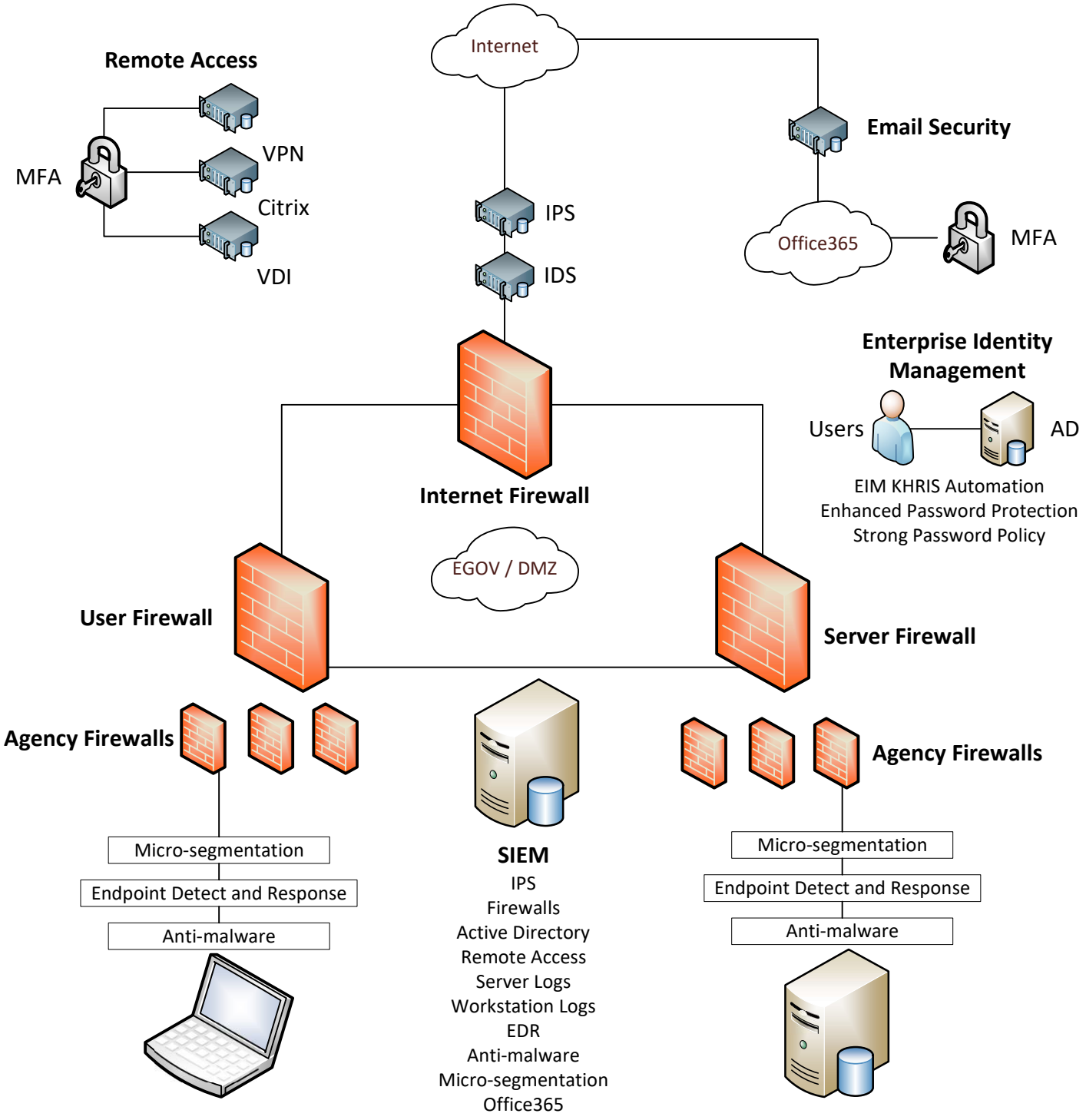

Remote Access
MFA
VPN
Citrix
VDI
Internet
IPS
IDS
Email Security
Office365
MFA
Enterprise Identity Management
Users
AD
EIM KHRIS Automation
Enhanced Password Protection
Strong Password Policy
Internet Firewall
EGOV / DMZ
User Firewall
Server Firewall
Agency Firewalls
Micro-segmentation
Endpoint Detect and Response
Anti-malware
SIEM
IPS
Firewalls
Active Directory
Remote Access
Server Logs
Workstation Logs
EDR
Anti-malware
Micro-segmentation
Office365
Agency Firewalls
Micro-segmentation
Endpoint Detect and Response
Anti-malware

CIS
Center for Internet Security
MITRE
ATT&CK

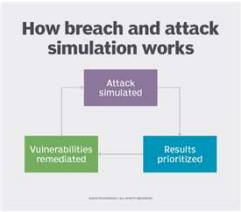
NIST
SP 800-53

EIM

SECURITY AWARENESS

COACHING
TEACHING
KNOWLEDGE
TRAINING
SKILLS
EXPERIENCE
LEARN
DEVELOPMENT

PARTNER
SHIP


How breach and attack simulation works
Attack simulated
Vulnerabilities remediated
Results prioritized

Vulnerability Management Process
1
2
3
4
Detect vulnerability
Check the quantity and nature of vulnerabilities.
Assess the risk
Examine the extent of risk.
Prioritize remediation
Set the priority of fixing vulnerabilities.
Confirm remediation
Re-scan, confirm, and report.

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK

RED TEAM
PURPLE TEAM
BLUE TEAM

Live data acquisition