



Endpoint Threat Defense for AD

Protecting AD from Every Endpoint

April 9th, 2019



Pervasiveness of Active Directory



90%

**of organizations depend
on Active Directory for domain
and identity-based services¹**

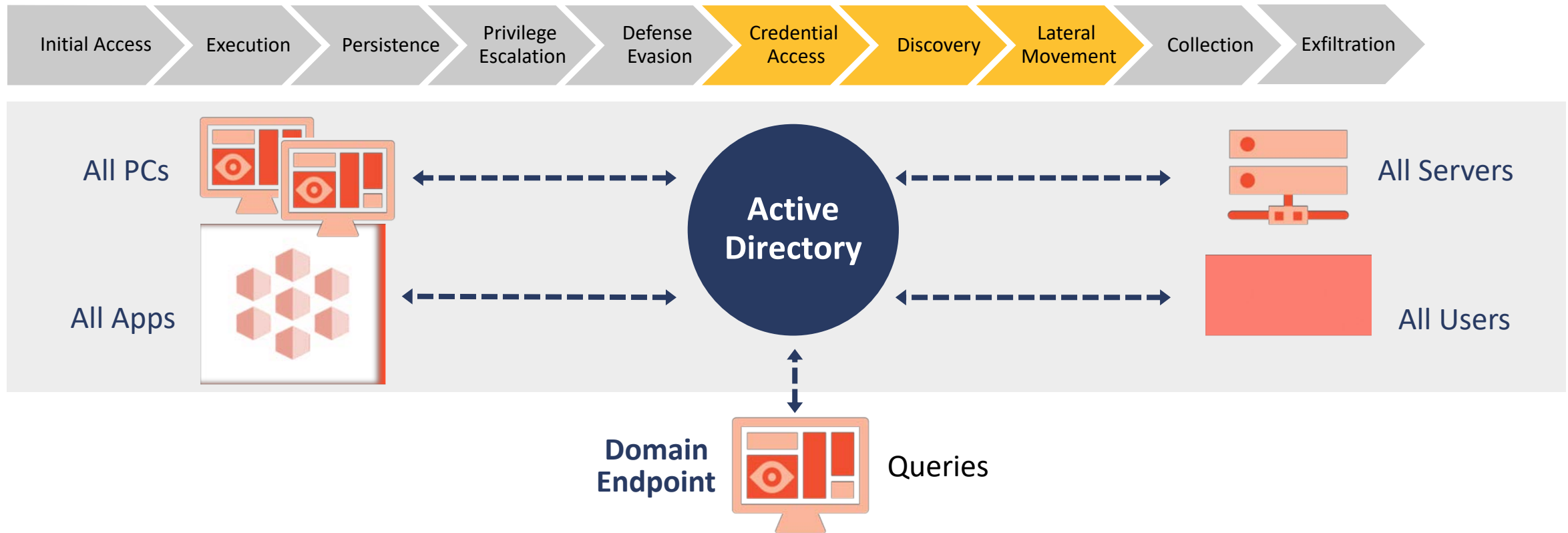
Active Directory Is a Basic Building Block of APTs*



Group Name	Alias	Credential Theft	Active Directory Enumeration	Timeframe	Origin
APT 3	Boyusec, UPS	Yes	Yes	Ongoing	China
APT 10	Stone Panda	Yes	Yes	Ongoing	China
APT 28	Sofacy, Fancy Bear	Yes	Yes	Ongoing	Russia
APT 29	Cozy Duke, Cozy Bear	Yes	Yes	Ongoing	Russia
APT 32	OceanLotus	Yes	Yes	Ongoing	Vietnam
APT 33	Charming Kitten	Yes	Yes	Ongoing	Iran
APT 34	Twisted Kitten	Yes	Yes	Ongoing	Iran
APT 35	Newscaster Team			Ongoing	Iran
Turla	Snake, Uroburos	Yes	Yes	Last Seen in 2017	Russia
Shell_Crew	Deep Panda	Yes	Yes	Last Seen in 2017	China
Dark Seoul	Lazarus Group, Hidden Cobra	Yes	Yes	Ongoing	North Korea

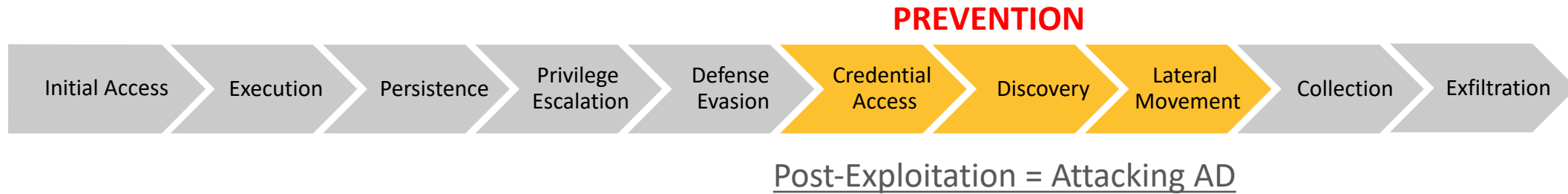
*<https://attack.mitre.org/groups/G0022/>

Active Directory Is a Primary Asset Exploited by Attackers



A few queries to active directory at the breached endpoint, an attacker can obtain all information about the corporation and move laterally

Attackers Start on an Endpoint



Protect Active Directory from Every Endpoint



Domain connected endpoints
represent a **higher security
risk to an enterprise**



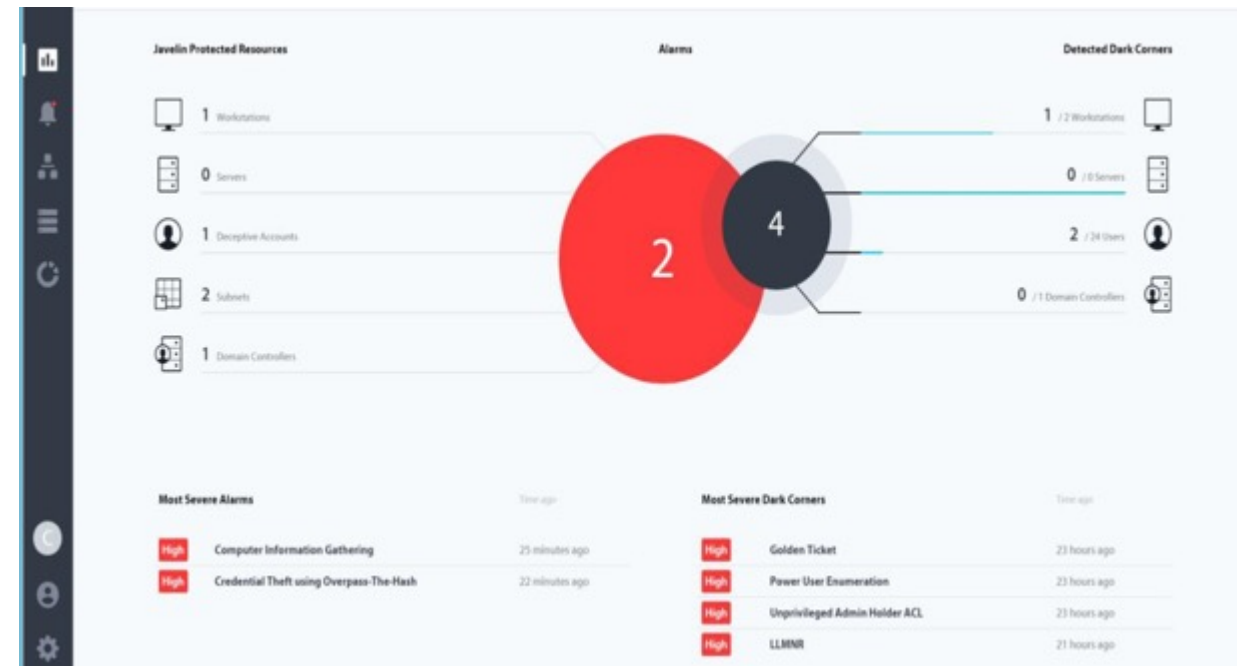
critical to protect
**Active Directory from the
endpoint to stop attackers
on their first move**

Introducing Symantec Endpoint Threat Defense for Active Directory | What it does?



AI-Driven Intrusion Detection, Investigation, and Containment


- Deploy a dissolvable in-memory code on every endpoint connect to the AD domain to obfuscate the AD reconnaissance that stops the first lateral movement attempt right at the endpoint.
- **Early into the attack cycle**, have low false positive and stop the attempt right at the point of breach.



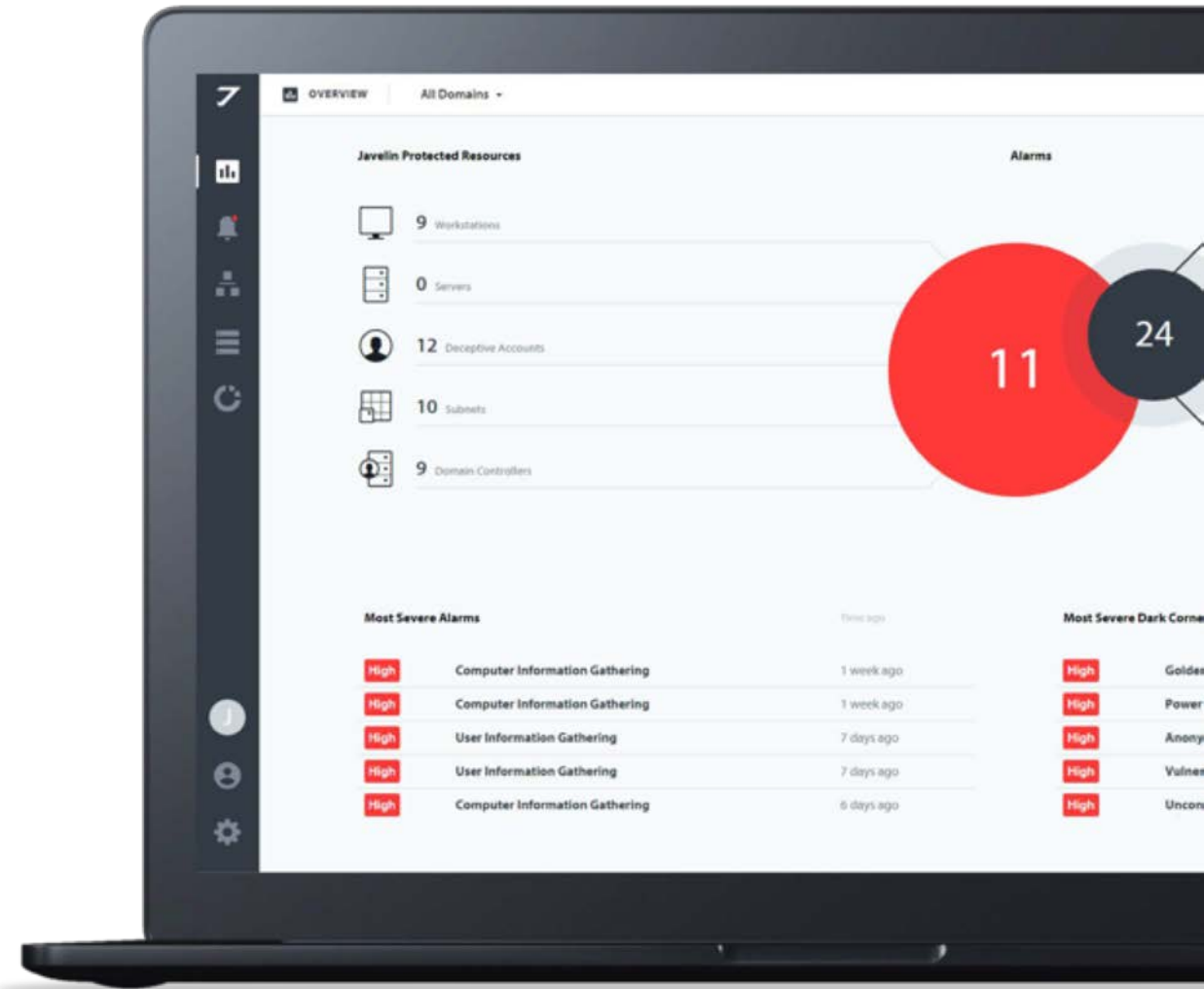
+99% success rate of stopping attackers on their first move

Simple Deployment



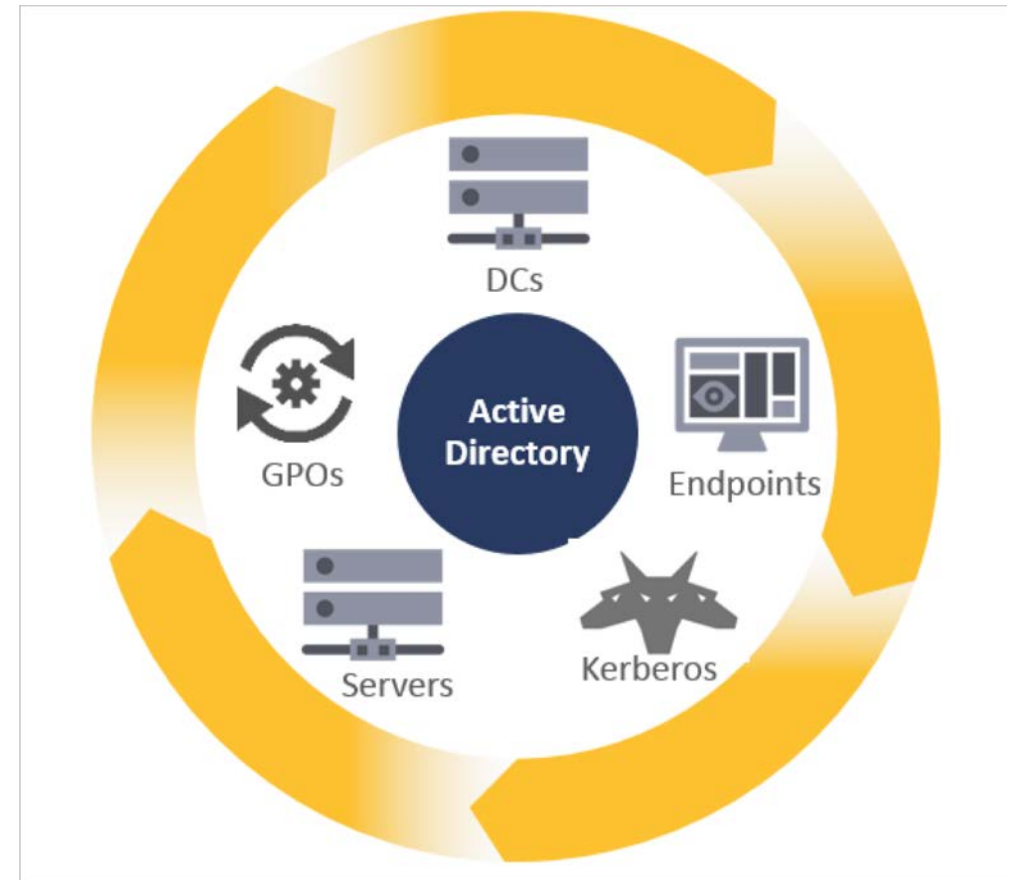
- No running process at the endpoint
- No resources consumed from the endpoint
- No network monitoring/network change
- No AD change
- No business impact
- Deploy with **SEP** or **Stand Alone**  Agentless Solution

GLOBAL AVAILABILITY | ON PRICE LIST | ADD-ON SKU



Symantec Endpoint Domain Assessment (part of TDAD package)

- Breach and Attack Simulation (BAS) to find misconfigurations and backdoors in Active Directory that lead to total compromise.
- Real-time alerts provide prescriptive recommendations on remediation
- No professional service engagements that produce only point in time threat assessments



REDUCE ATTACK SURFACE AND INCREASE VISIBILITY WITH ONGOING ATTACK SIMULATIONS

Market Landscape...



NO OTHER MAJOR ENDPOINT VENDOR



MICROSOFT ADVANCED THREAT ANALYTICS (ATA)

- Protecting AD, based on AD data only
- Unable to mitigate the attack
- Late in the attack cycle

PRIMARY BUYERS

- Endpoint Security Administrator
- Security Architect
- SOC | IR

The missing piece in the APTs security puzzle



PROTECTING THE LEAST PATH OF RESISTANCE IN THE NETWORK

- Defends primary attack surface which enables lateral movement
- 99% efficacy achieved by controlling the attacker's perception of Active Directory from any endpoint in the domain

MAXIMIZE SOC ANALYST TIME

- Intrusion detection and Automated mitigation reduces the response time.
- Automatic forensic gathering to reduce investigation time
- Fewer, high fidelity alerts reduces alert fatigue

MORE EFFECTIVE ACTIVE DIRECTORY PROTECTION

- Only solution protecting AD from the endpoint – at the origin of compromise
- Ongoing security assessment reduces number of future APTs

**SUPERCHARGE ENDPOINT DEFENSE WITH ENHANCED PREVENTION STRATEGY
USING THREAT DEFENSE FOR ACTIVE DIRECTORY**



Complete Endpoint Defense



SEP+ EDR

Symantec Endpoint Protection
Symantec Endpoint Detection and Response



AED

NEW

Symantec Endpoint Protection

Symantec Endpoint Application Isolation
Symantec Endpoint Application Control
Symantec Endpoint Threat Defense for Active Directory



CED

NEW

Symantec Endpoint Protection
Symantec Endpoint Detection and Response
Symantec Endpoint Application Isolation
Symantec Endpoint Application Control
Symantec Endpoint Threat Defense for Active Directory
Symantec Endpoint Cloud Connect Defense



CYBER DEFENSE MANAGER

(Single Smart Cloud Console)



SINGLE AGENT



POWERED BY **SYMANTEC GLOBAL INTELLIGENCE NETWORK**