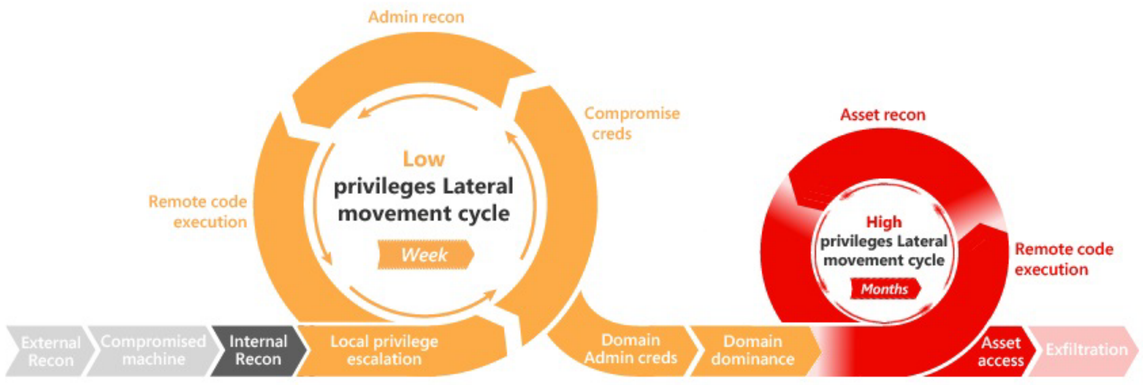
FSPROTECT

PRODUCT DATASHEET

Resilient Active Directory with Ease

FORESTALL

Active Directory is the key component for enterprise IT infrastructure and de-facto standard for identity management. 95 % of companies today use Active Directory as their main identity service worldwide. It provides authentication, authorization and configuration capabilities. Active Directory contains a database with critical information about users, computers, group policies, services etc. to perform these operations and is the essential target because of its core management features.



When adversaries gain initial foothold to a domain-joined computer, they can use built-in tools to reveal the entire Active Directory environment. This critical information provides all necessary data like Active Directory attack surface, lateral movement/privilege escalation paths, and misconfigured privileges to plan the next phase of the operation. Threat actors can use this valuable information to compromise the entire domain in days or weeks.

Disrupt the Adversaries' Active Directory Kill Chain with FSProtect

FSProtect reveals organizations' Active Directory security posture before the attacker and enables you to quickly take the necessary precautions with the continuous vulnerability assessment.

Active Directory Inventory Mapping

FSProtect collects in-depth information and relationships of Active Directory objects and endpoints with the proprietary information gathering algorithms. Some of the analyzed objects can be seen below.

- Users
- Computers
- Groups
- Group Policy Objects
- Organization Units
- Service Accounts / Managed Service Accounts
- Service Principle Names
- Access Control Entries
- Local Groups
- Local Users
- Network Shares

It presents this information in a form that can be easily searched, filtered, and exported in CSV format on the web interface. For example, the following information can be easily obtained through this interface.

- Privileged User and Groups
- Disabled/Locked Users
- Service Users
- Organizational Units with No Members
- User with Local Administrator Privileges
- Computers/Users with Most Sessions
- Group Policies with No Linked Entities

Active Directory Vulnerability Assessment

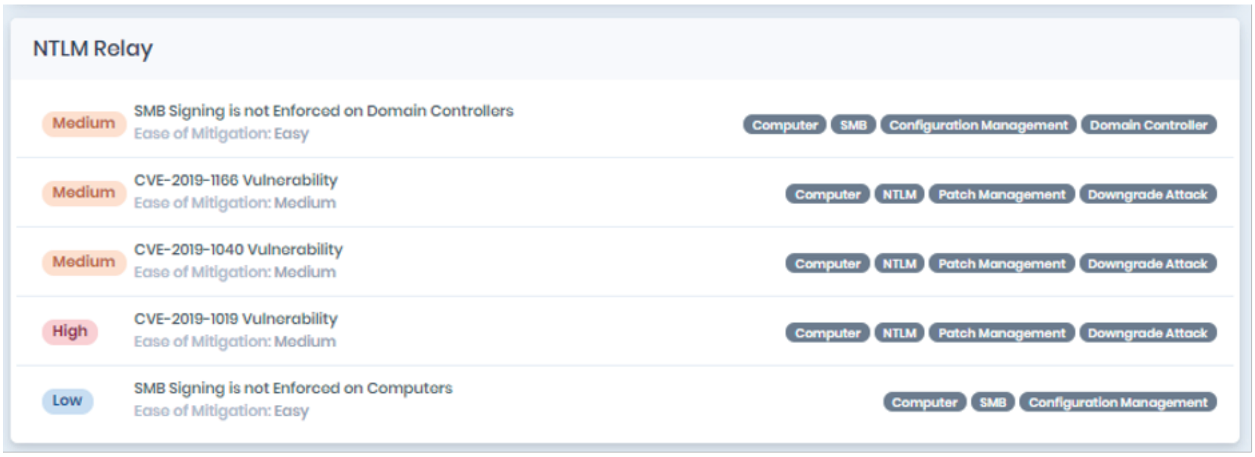
FSProtect continuously detects Active Directory Specific vulnerabilities with no false positives thanks to its Vulnerability Detection Engine. In addition, custom tags are added to vulnerabilities for easier categorization.

Vulnerability documentation contains the information below to accelerate vulnerability identification, remediation, detection, and prioritization process.

- Severity, Ease of Mitigation and Ease of Detection metrics for prioritization
- Vulnerability description, impact, and references
- Manual vulnerability identification methods
- Detailed mitigation plans and scripts for automatized remediation
- Exploitation detection methods with event log ids and attributes
- MITRE ATT&CK matrix mapping for suitable vulnerabilities

Actionable Remediation Roadmaps against Impacts

FSProtect generates a remediation roadmap by aggregating the vulnerabilities that create critical attack vectors under Impacts and reveals which attacks the organization can be affected by. In this way, measures can be taken not only against vulnerabilities but also against emerging Active Directory threats.



NTLM Relay

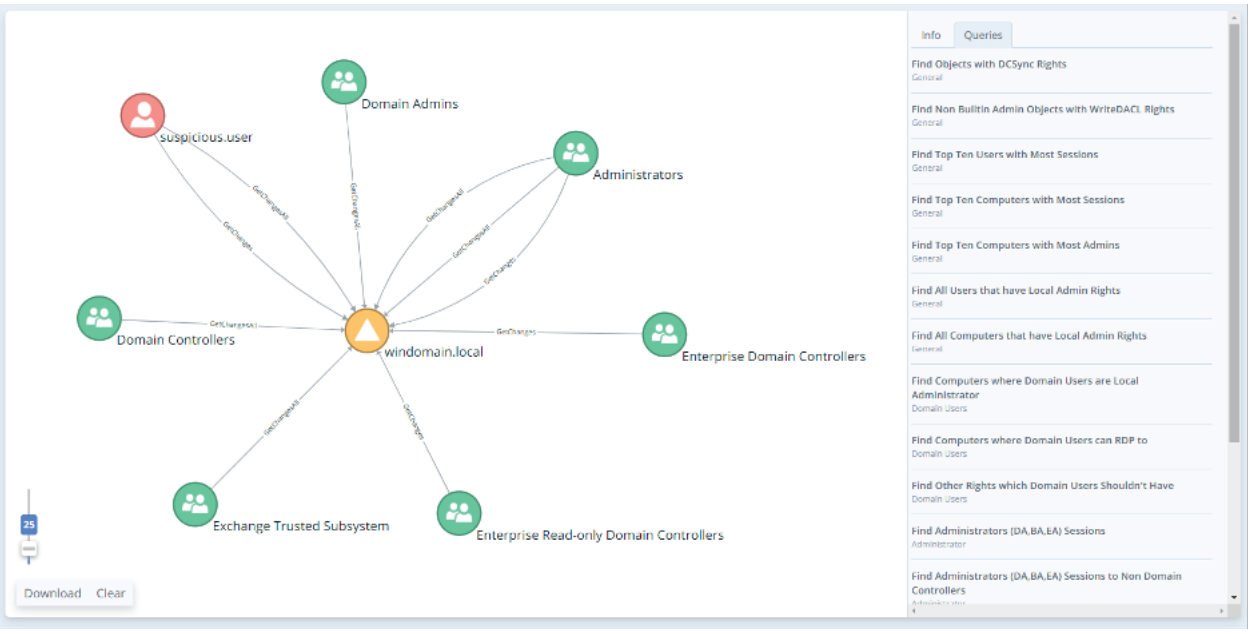
Medium	SMB Signing is not Enforced on Domain Controllers Ease of Mitigation: Easy	Computer, SMB, Configuration Management, Domain Controller
Medium	CVE-2019-1166 Vulnerability Ease of Mitigation: Medium	Computer, NTLM, Patch Management, Downgrade Attack
Medium	CVE-2019-1040 Vulnerability Ease of Mitigation: Medium	Computer, NTLM, Patch Management, Downgrade Attack
High	CVE-2019-1019 Vulnerability Ease of Mitigation: Medium	Computer, NTLM, Patch Management, Downgrade Attack
Low	SMB Signing is not Enforced on Computers Ease of Mitigation: Easy	Computer, SMB, Configuration Management

Active Directory Security Graph

FSProtect creates an organizational Active Directory Security graph when the scan is finished. This graph contains all domain inventory and their relationships in one interface. Using manual or built-in queries in the graph module, abnormal relationships, shortest lateral movement, privilege escalation paths and misconfigured access control entries can be easily detected.

Some of the Built-in Queries in the Graph Module

- Object with DCSync Rights
- Non-built-in Admin Objects with WriteDACL Rights
- Administrator Sessions to Non-Domain Controllers
- Groups with Local Administrator Rights
- Shortest Path to Admin Groups
- Abnormal Rights which Domain User shouldn't have



Find Objects with DCSync Rights
General

Find Non Builtin Admin Objects with WriteDACL Rights
General

Find Top Ten Users with Most Sessions
General

Find Top Ten Computers with Most Sessions
General

Find Top Ten Computers with Most Admins
General

Find All Users that have Local Admin Rights
General

Find All Computers that have Local Admin Rights
General

Find Computers where Domain Users are Local Administrator
Domain Users

Find Computers where Domain Users can RDP to
Domain Users

Find Other Rights which Domain Users Shouldn't Have
Domain Users

Find Administrators (DA,BA,EA) Sessions
Administrator

Find Administrators (DA,BA,EA) Sessions to Non Domain Controllers
Administrator

Automatized Reporting

FSProtect generates detailed, user-friendly, easy to understand, and instantly downloadable HTML and PDF reports when the scan is finished.

REST API Interface

FSProtect provides the REST API interface for automation and extensibility needs.

Contact Us for More Information

info@forestall.io