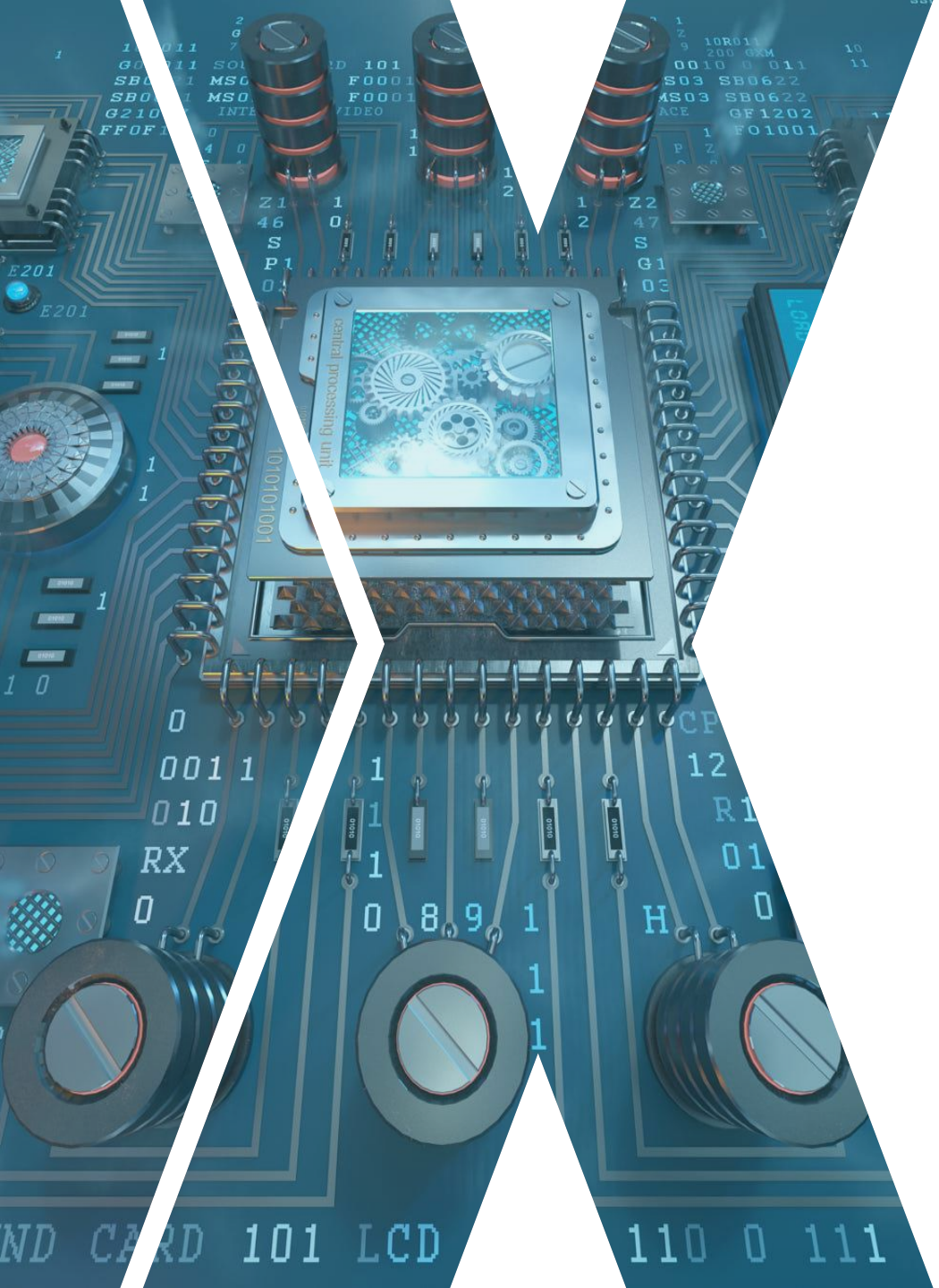
Emerging Threats, Advanced Solutions

Active Directory Security Platform



About Our Company

Forestall is a security start-up founded in 2020. Our team is focused on adversarial tactics on Active Directory. With this motivation, we are developing a multi-staged platform which comprises proactive and reactive countermeasures for emerging Active Directory threats.

BİGG BİREYSEL GENÇ GİRİŞİM

teknopark ankara "Teknolojinin Başkenti"

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

Team Achievements

Active Directory

Core Component of Authentication & Authorization

De-Facto Standard for Identity Management

Real Word Impact

A Lesson From The Pipeline Hack: Secure Active Directory Now

Written by Paul Roberts | Published 12 May 2021

Cyber

Ryuk Ransomware Hit Multiple Oil & Gas Facilities, ICS Security Expert Says

Attackers 'weaponized' Active Directory to spread the ransomware.

Active Directory Attacks Hit the Mainstream

There was a time when attacks against identity and authentication infrastructure were the domain of well-financed and, likely, state-backed threat actors. These groups crave persistence on critical networks and would invest

CrowdStrike Exec Points to Active Directory 'Structural Problems' in Senate Solorigate Hearing

By Kurt Mackie | 02/26/2021

TrickBot Now Steals Windows Active Directory Credentials

By Lawrence Abrams

January 23, 2020 04:07 PM 1

The Weaponization of Active Directory: An Inside Look at Ransomware Attacks Ryuk, Maze, and SaveTheQueen

by Thomas Leduc on October 2, 2020

Like never before, Active Directory (AD) is in the attackers' crosshairs. In this blog, we'll examine how ransomware attacks are abusing AD and how enterprises can evolve their defensive strategies to stay ahead of attackers.

Real Word Impact

https://www.darkreading.com/vulnerabilities%E2%80%94threats/researchers-explore-active-directory-attack-vectors/d/d-id/1340902

Identity Threat Detection & Response

Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

Published 20 October 2022 - ID G00765882 - 21 min read

By Analyst(s): Henrique Teixeira, Peter Firstbrook, Ant Allan, Rebecca Archambault

Initiatives: Identity and Access Management and Fraud Detection

> Conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack. To enhance cyberattack preparedness, security and risk management leaders must add ITDR capabilities to their security infrastructure.

FSPROTECT

Resilient Active Directory with Ease

Active Directory Security Assessment

Solution

Inventory & Relation Mapping

Vulnerability Assessment

Impact Analysis & Risk Scoring

Attack Path Management

Group Policy Audit

Privilege Analysis

Graph Visualization

Advanced Search & Reporting

Features

Inventory & Relation Mapping

FSProtect, collects in-depth information and relationships of Active Directory objects and endpoints with the proprietary information gathering algorithm.

Inventory & Relation Mapping

FORESTALL

Advanced Search & Reporting

Built-in Query

Built-in queries for easy reporting

- Risky Admin Users
- Service accounts with Local Admin Privileges
- Never logged on users

Custom Filters

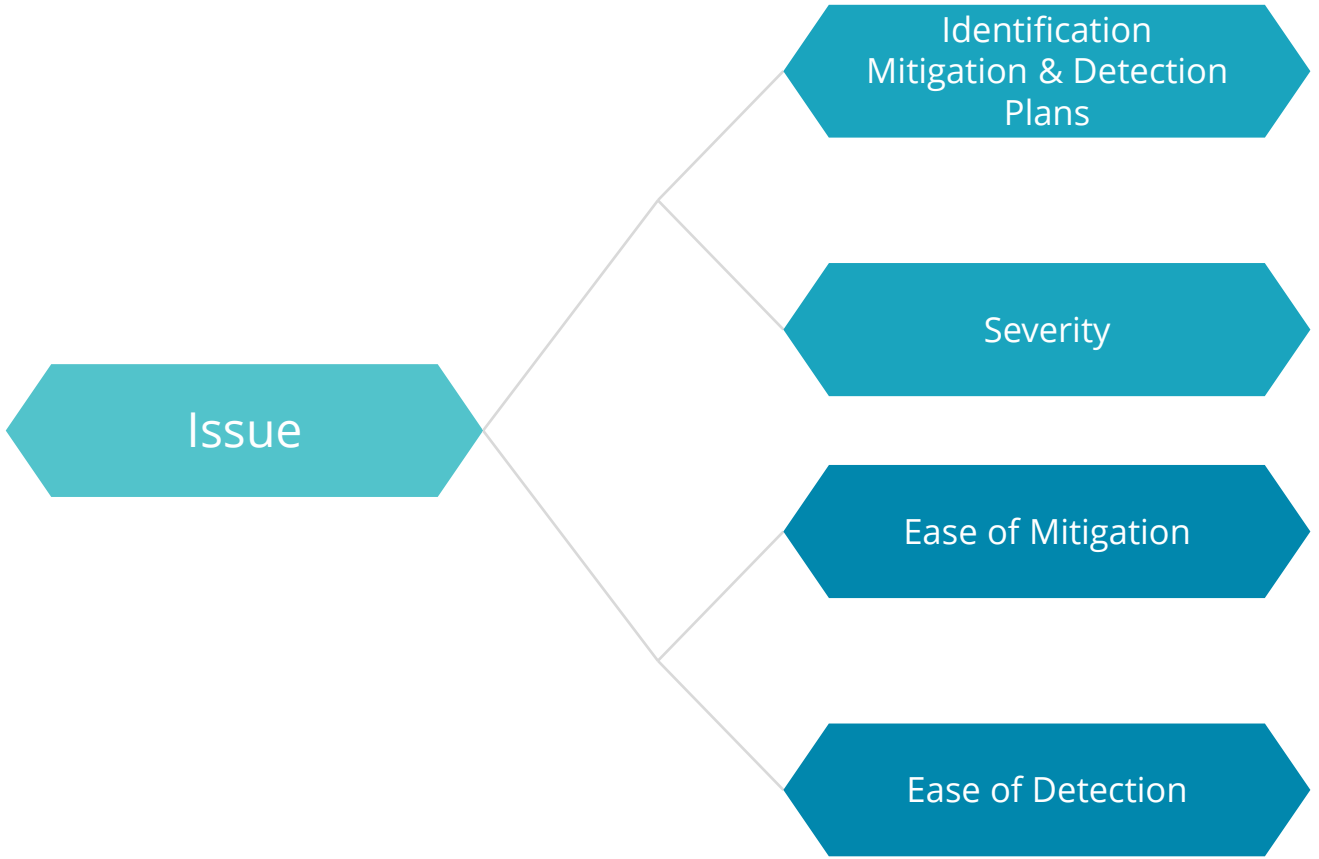
Advanced search interface with various filters

Features

Vulnerability Assessment

FSProtect continuously detects Active Directory Specific vulnerabilities with no false positives thanks to its Vulnerability Detection Engine.

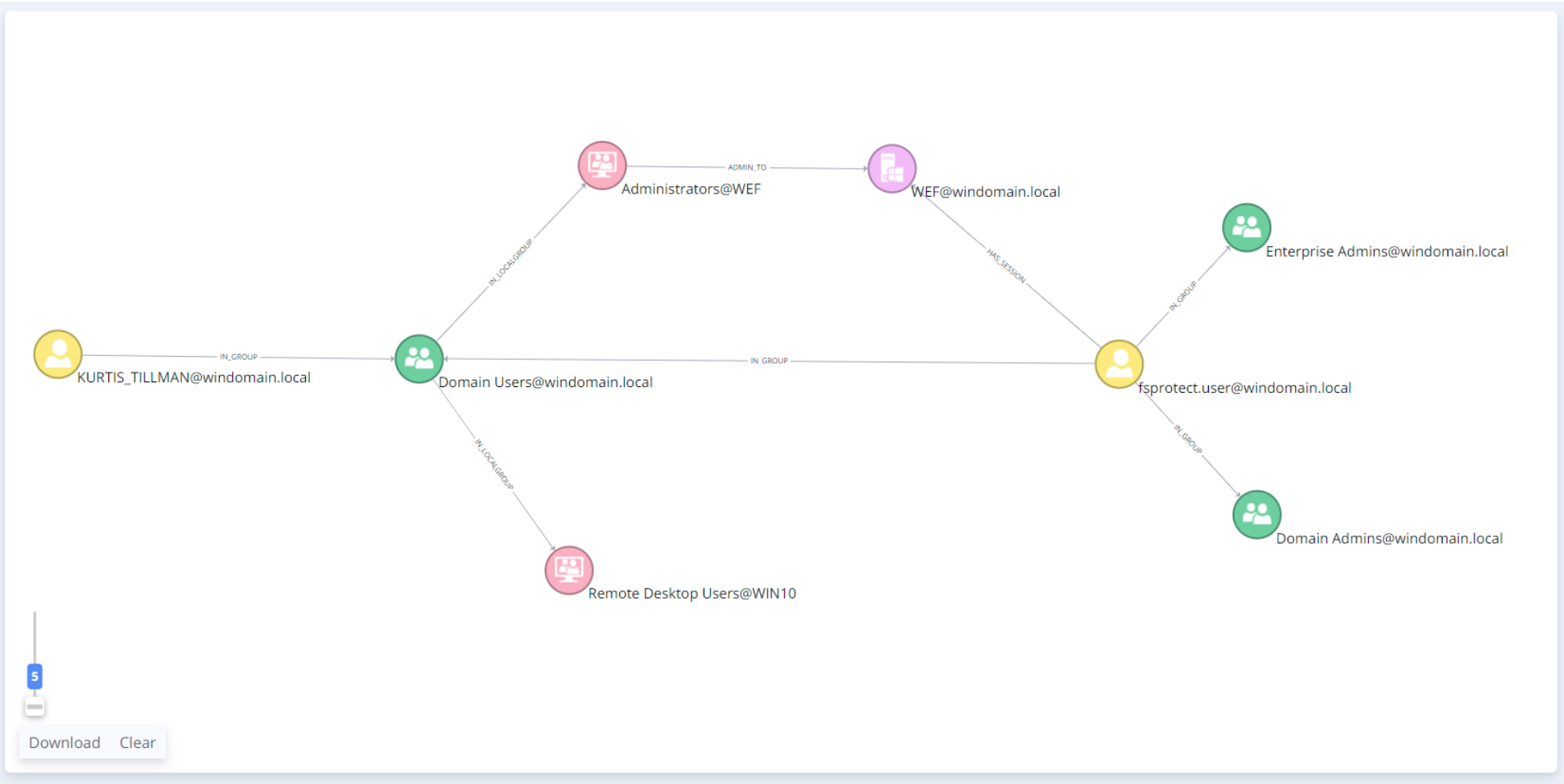
Vulnerability documentation contains the information to accelerate vulnerability identification, remediation detection, and prioritization process.



Vulnerability Assessment

Severity	Ease of Mitigation	Ease of Detection	Issue
Critical	Hard	Hard	Admin Sessions on Non-Domain Controller Servers
Critical	Easy	Easy	Dangerous Access Control Entries on Users
Critical	Medium	Hard	Plain Text Passwords in Group Policy Preferences
High	Easy	Medium	Reversible Password Usage for Users
Low	Easy	Easy	Inactive Users

Attack Path Finding with Graph Visualization



FORESTALL

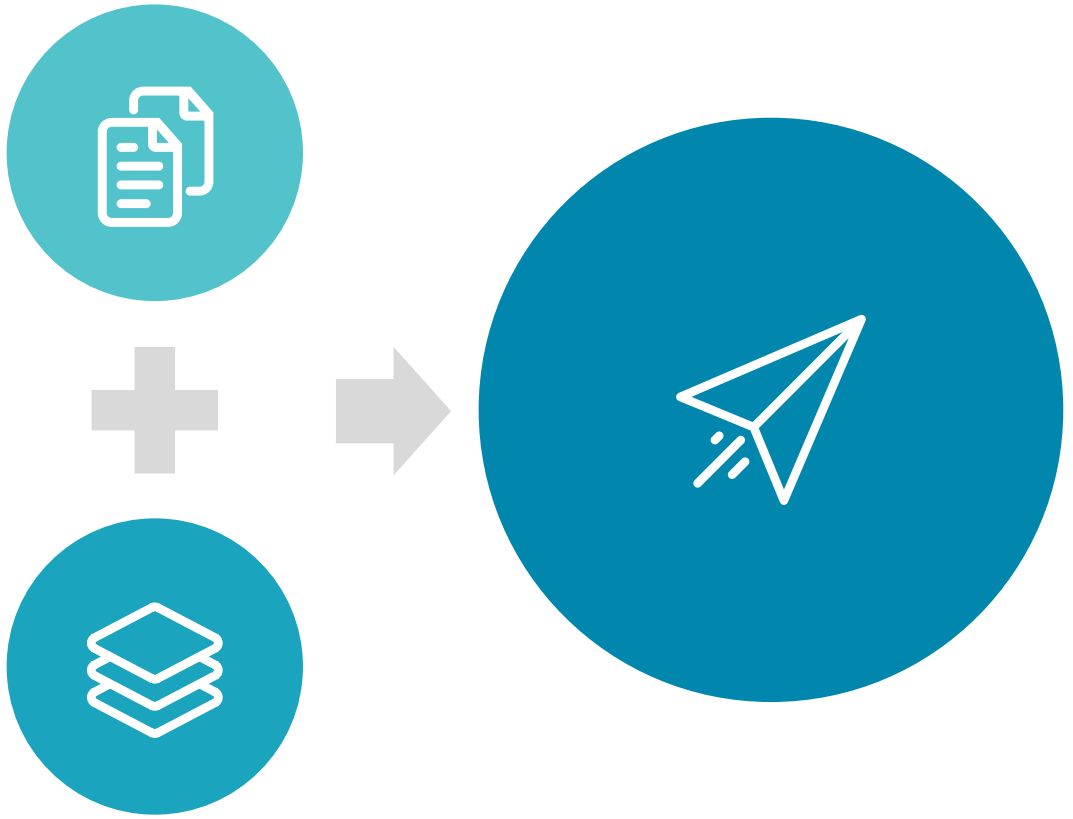
Group Policy Audit

Baseline Comparison

You can compare the GPO baselines published by Microsoft with your own GPOs.

Conflicts

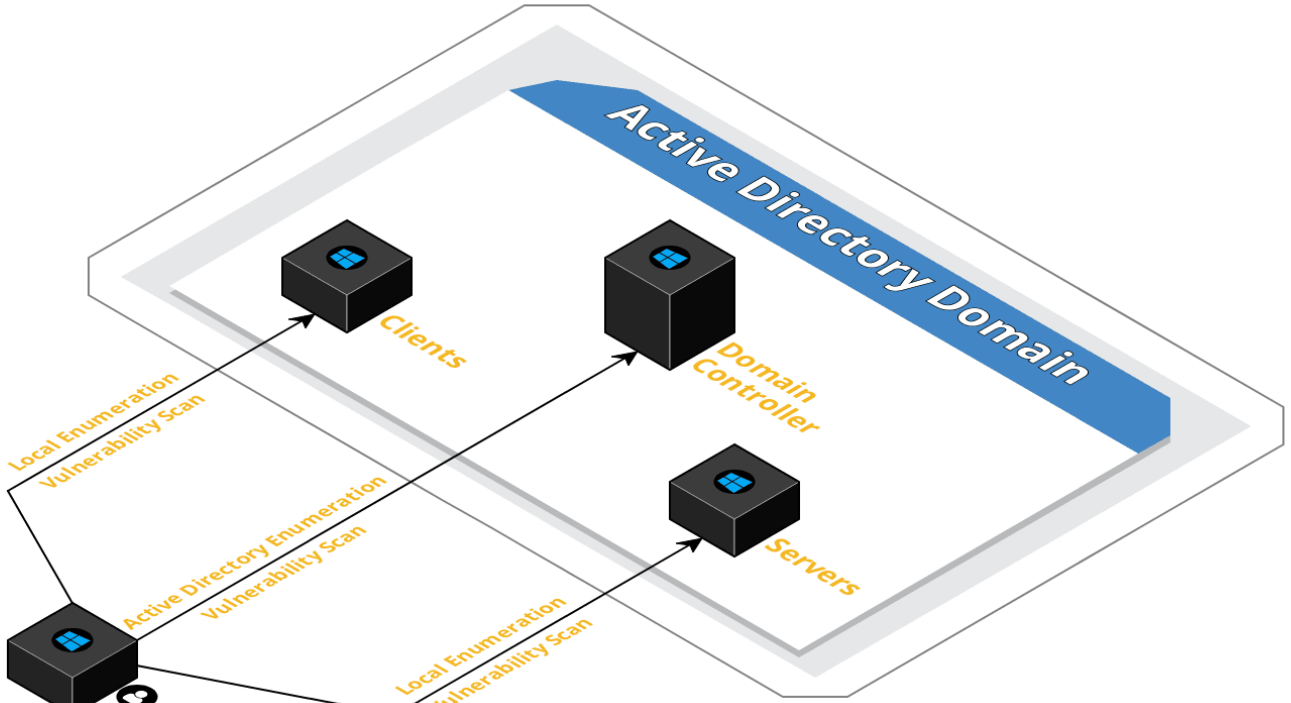
You can compare the Resultant GPO settings affecting computers, users, and OUs with our checklist.



Group Policy Audit

FORESTALL

Architecture



FSPROTECT

- No Agent Required
- No Privilege Required
- No Effect on AD & DC
- No Setup on DC

FORESTALL

FSProtect

Use Cases

- System Administrator

- Red Team

- Blue Team

System Administrator

Identity Visibility

- Unknown, risky objects
- Local inventory enumeration
- Multiple Forest & Domain enumeration

Search & Reports

- Empty groups, disabled GPOs, inactive objects etc

GPO Audit

- Vulnerable settings and Resultant Set of Policies
- Compliance scores

System Administrator – Identity Visibility

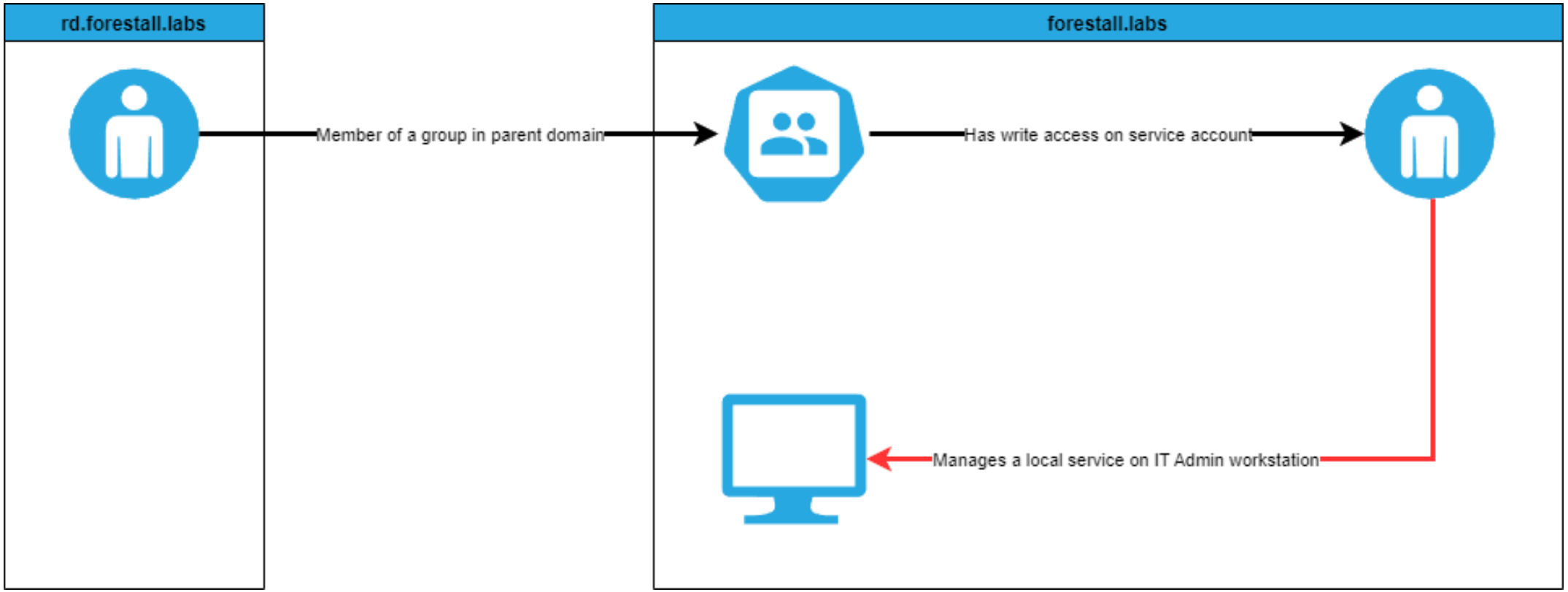
Users	Stats
Total	58300
Disabled	3316
Privileged	**10314 (%17)**
Service Account	279
Risky	**57466 (%98)**

Computers	Stats
Total	31947
Disabled	224
Inactive	**3999 (%12)**
Unsupported	527
Risky	**31556 (%98)**

Groups	Stats
Total	18232
Empty	**2774 (%15)**
Privileged	49
Admin	12
Risky	**17767 (%97)**

GPO	Stats
Total	448
Empty	**122 (%27)**
Disabled	14
Unlinked	**99 (%22)**
Risky	**126 (%28)**

System Administrator – Identity Visibility



Red Team

Vulnerability Assessment

Active Directory specific, mostly unknown vulnerabilities
- Certificate Service vulnerabilities
- Kerberos / NTLM Protocol related vulnerabilities

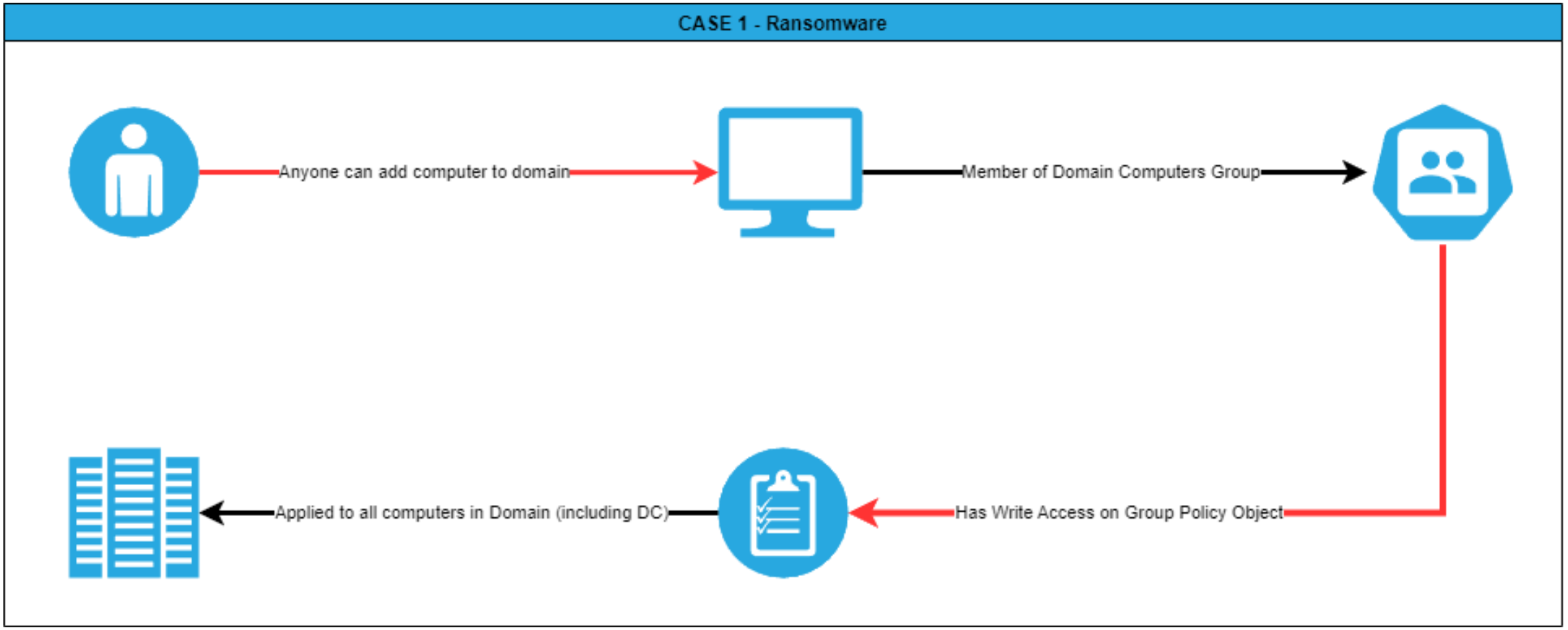
Attack Path Management

Complex and undetectable attack paths

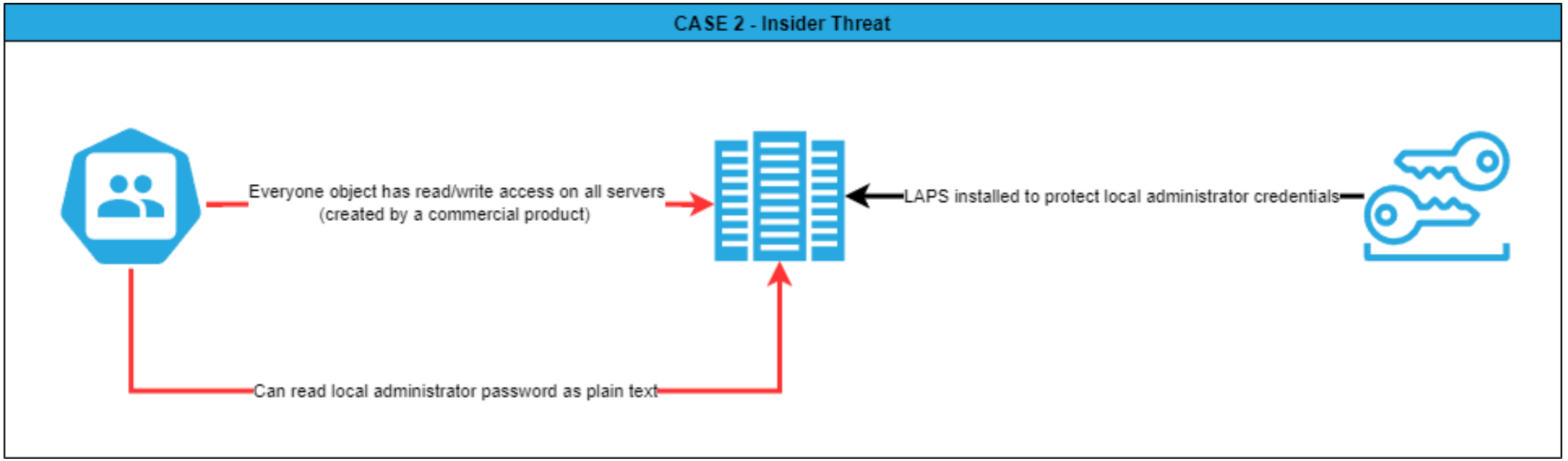
Identity Privilege Analysis

Active Directory specific lateral movement & privilege escalation paths

Red Team – Attack Path Management



Red Team – Privilege Analysis



Blue Team

Vulnerability Assessment

Active Directory specific, mostly unknown vulnerabilities

Compromise Assessment

Active Directory specific backdoors and signs of compromise

Identity Attack Surface & Risk Insight

Incident related reports and identity-based risk scores

Blue Team – Compromise Assessment

Severity	Ease of Mitigation	Eease of Detection	Sign of Compromise
Critical	Medium	Hard	Resource Based Constrained Delegation to KRBTGT
Critical	Medium	Hard	Objects with Suspicious SID-History Attribute
Critical	Medium	Hard	Dangerous ACL Entries on Admin Objects
Medium	Easy	Easy	Suspicious Accounts used as Admin Before
Medium	Easy	Easy	Computers Added by Suspicious Users

Blue Team – Identity Attack Surface

Incident Related Reports
Which users have a session on this computer?
Which objects were created/changed in the last hour?
Which objects' passwords were changed in the last hour?
Which objects have domain replication rights?
Which objects can compromise admin accounts? (Stealth admins)

Insider Threat

Advanced
Persistent Threat

Ransomware

OUR PRODUCTS

FSProtect

AD Security Assessment

AD Vulnerability Assessment, Inventory Enumeration and attack path finding

Ready

FSDetect

AD Threat Detection

AD based Real-Time attack detection

Development

FSDeceive

AD Deception

AD based deception for creating attractive decoys to lure attackers

Development

FSSimulate

AD Attack Simulation

AD based Attack Simulation for evaluating detection products and Blue Team's agility

Development

FORESTALL

Contact Us

FORESTALL
Emerging Threats, Advanced Solutions

info@forestall.io

https://forestall.io

Lateral Movement is new front

Essential target is Active Directory