Gold Finger

Active Directory Effective Access Auditor

Datasheet

Gold Finger

Active Directory Effective Access Auditor

At the foundation of cyber security of all organizations that operate on the Microsoft Windows Server platform lie their foundational Active Directory (AD) deployments.

Organizations absolutely require the ability to audit effective access in their foundational Active Directory deployments to maintain security, accurately identify and manage privileged access and fulfill governance, risk and compliance driven audit needs.

Architected by former Microsoft Program Manager for Active Directory Security, and endorsed by Microsoft, the *Active Directory Effective Access Auditor* from Paramount Defenses is the world's only accurate effective access auditor for Active Directory.

> *"We are very pleased to see Paramount Defenses, a valued Microsoft partner, offer an innovative security solution (in Gold Finger) that helps enhance security and compliance in Active Directory environments."*
>
> - Charles Coates, Senior Product Manager
> Identity and Security Business Group
>
> Microsoft

Active Directory Effective Access Auditor

Technical Overview

The entirety of an organization's building blocks of cyber security i.e. all organizational domain user accounts, computer accounts, and all domain security groups that protect almost all organizational IT resources, are stored, managed and secured in Active Directory.

Each one of these building blocks is represented as an object within Active Directory and is protected by an access control list (ACL), which contains access control entries (ACEs) that specify who is allowed and denied what security permissions on the object.

Together, there exist many security permissions in the ACL of every Active Directory object, granted to various users and groups, and it is the net resulting cumulative i.e. effective permissions that actually govern exactly who has what effective access on each object, and thus govern who can enact what privileged/administrative tasks on Active Directory objects.

To secure Active Directory, accurately identify privileged users, control access to privileged users and groups, maintain security and fulfill various GRC driven audit needs, organizations need to be able to accurately audit effective access on Active Directory objects.

The *Active Directory Effective Access Auditor* is unique in its ability to be able to accurately and automatically audit effective access in terms of administrative tasks in Active Directory. It can –

- ✓ Accurately audit effective access on any object in an Active Directory domain
- ✓ Audit effective access in terms of administrative tasks entitled on Active Directory objects
- ✓ Identify the underlying permissions that entitle a user to a specific administrative task

It thus uniquely enables and empowers organizations to easily perform critical audits that are required to accurately assess and lockdown privileged access and to maintain cyber security.

Active Directory Effective Access Auditor

Features

The *Active Directory Effective Access Auditor* embodies numerous thoughtful features specially designed to help IT personnel easily perform effective access analysis –

1. Accurate Effective Access Audit – Accurately audit effective access in Active Directory
2. Active Directory Privileged Access Audit – Audit who can control privileged users/groups
3. Real-time Effective Access Audit – Determine effective access on objects in real-time
4. Actionable Intelligence – Identify the underlying permission entitling a specific user
5. Effortless Audit Exports – Easily export effective access audit results

Benefits

The *Active Directory Effective Access Auditor* delivers numerous tangible benefits that have a real and measurable impact on the organization's foundational cyber security posture –

1. Accurately Audit Effective Access – Accurately calculate effective access in Active Directory
2. Accurately Audit Privileged Access – Audit who actually has what privileged access
3. Lock-down Privileged Access – Reliably lockdown all privileged access in Active Directory
4. Complete first 3 steps of PAM – Accurately identify, secure and control privileged users
5. Correctly Fulfill GRC Needs – Correctly fulfill audit and regulatory compliance needs

Active Directory Effective Access Auditor

Audit/Reporting Capabilities

The *Active Directory Effective Access Auditor* lets organizations accurately, easily and instantly generate numerous Active Directory effective access reports, such as –

1. Identify who can perform what administrative tasks on an Active Directory object
2. Pinpoint how a specific user is able to perform a specific task on a specific object
3. Determine exactly who can enact a specific task on a specific Active Directory object
4. Identify all users who can enact an administrative task due to a specific permission
5. Find out why a user is able to enact a specific administrative task in Active Directory

Audience

- ✓ IT Managers
- ✓ Domain and Network Admins
- ✓ Cyber Security Analysts
- ✓ IT and Cyber Security Auditors
- ✓ Internal Application Developers
- ✓ Pen Testers and Ethical Hackers

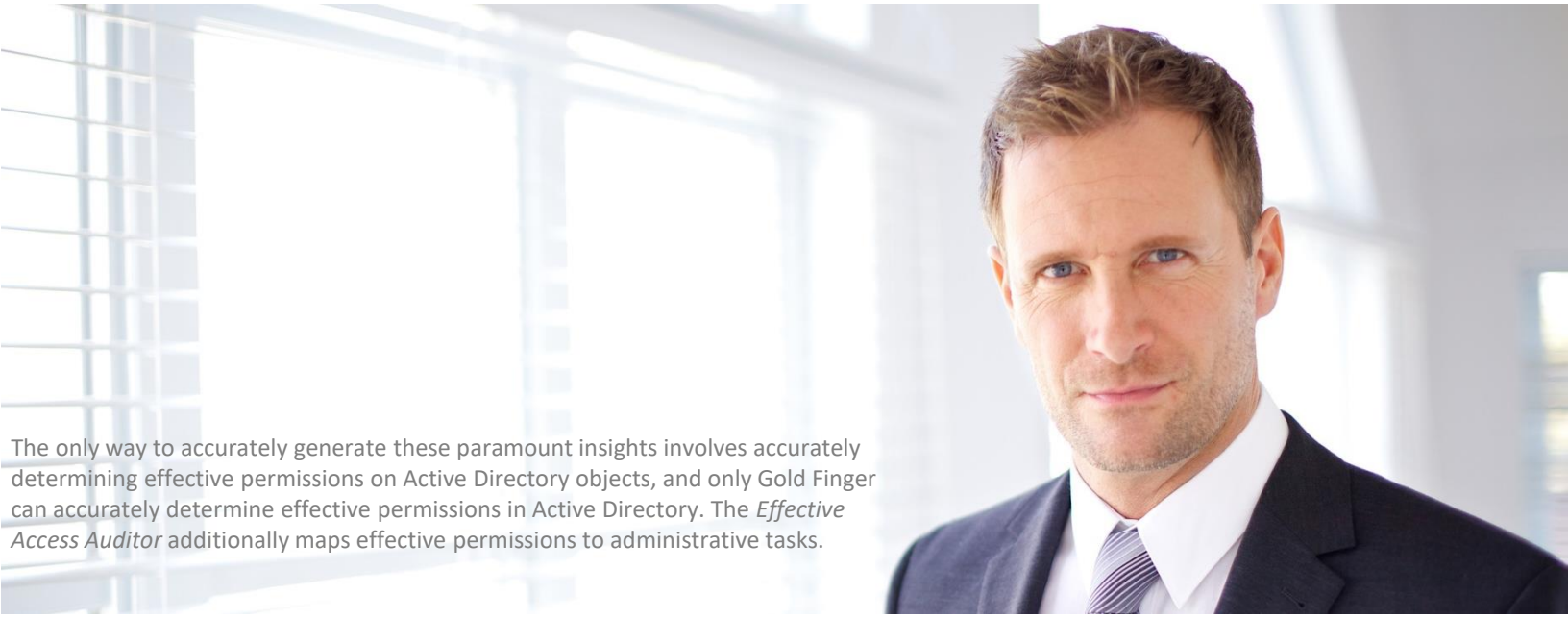
Requirements

- ✓ Any computer running Windows
- ✓ Any domain-user credentials
- ✓ Network access to Active Directory
- ✓ No privileged access required
- ✓ No installation on DCs required
- ✓ No deployment of services/agents

Active Directory Effective Access Auditor

Top-10 Reports

The *Active Directory Effective Access Auditor* uniquely empowers organizations to obtain paramount cyber security insights by generating high-value reports, such as –



The only way to accurately generate these paramount insights involves accurately determining effective permissions on Active Directory objects, and only Gold Finger can accurately determine effective permissions in Active Directory. The *Effective Access Auditor* additionally maps effective permissions to administrative tasks.

1. Identify all individuals who can change the membership of any default unrestricted privileged group in Active Directory, such as *Domain Admins*, *Enterprise Admins* etc.
2. Identify all individuals who can reset the password of any privileged user's account
3. Identify all individuals who can disable the use of Smartcards for authentication
4. Identify all individuals who can modify the ACL protecting the *AdminSDHolder* object
5. Identify all individuals who can manage any executive's (e.g. the CEO's) user account
6. Identify all individuals who can change privileged access on the domain root object
7. Identify all individuals who can change privileged access on an Organizational Unit (OU)
8. Identify all individuals who can delete accounts, groups and OUs in Active Directory
9. Identify all individuals who can change the keywords on the service connection point of a mission-critical service such as *Microsoft Entra Connect*, resulting in a DoS attack
10. Identify all individuals who can link a GPO to an OU, resulting in the modification of a security or configuration setting on all (possibly thousands of) computers in that OU

Gold Finger

Gold Finger is the world's most capable, valuable and trustworthy suite of access assessment tools for Microsoft Active Directory, and is the gold standard for Active Directory Assessment.

The *Gold Finger* Suite is architected by former Microsoft Program Manager for Active Directory Security, endorsed by Microsoft, trusted worldwide, and comprised of 8 specialized tools –

1. Active Directory Security Auditor
2. Active Directory Membership Auditor
3. Active Directory ACL Analyzer
4. Active Directory ACL Exporter
5. Active Directory Permissions Analyzer
6. The world's only accurate Active Directory Effective Permissions Calculator
7. The world's only accurate Active Directory Effective Access Auditor
8. The world's only accurate Active Directory Privileged Access Assessor

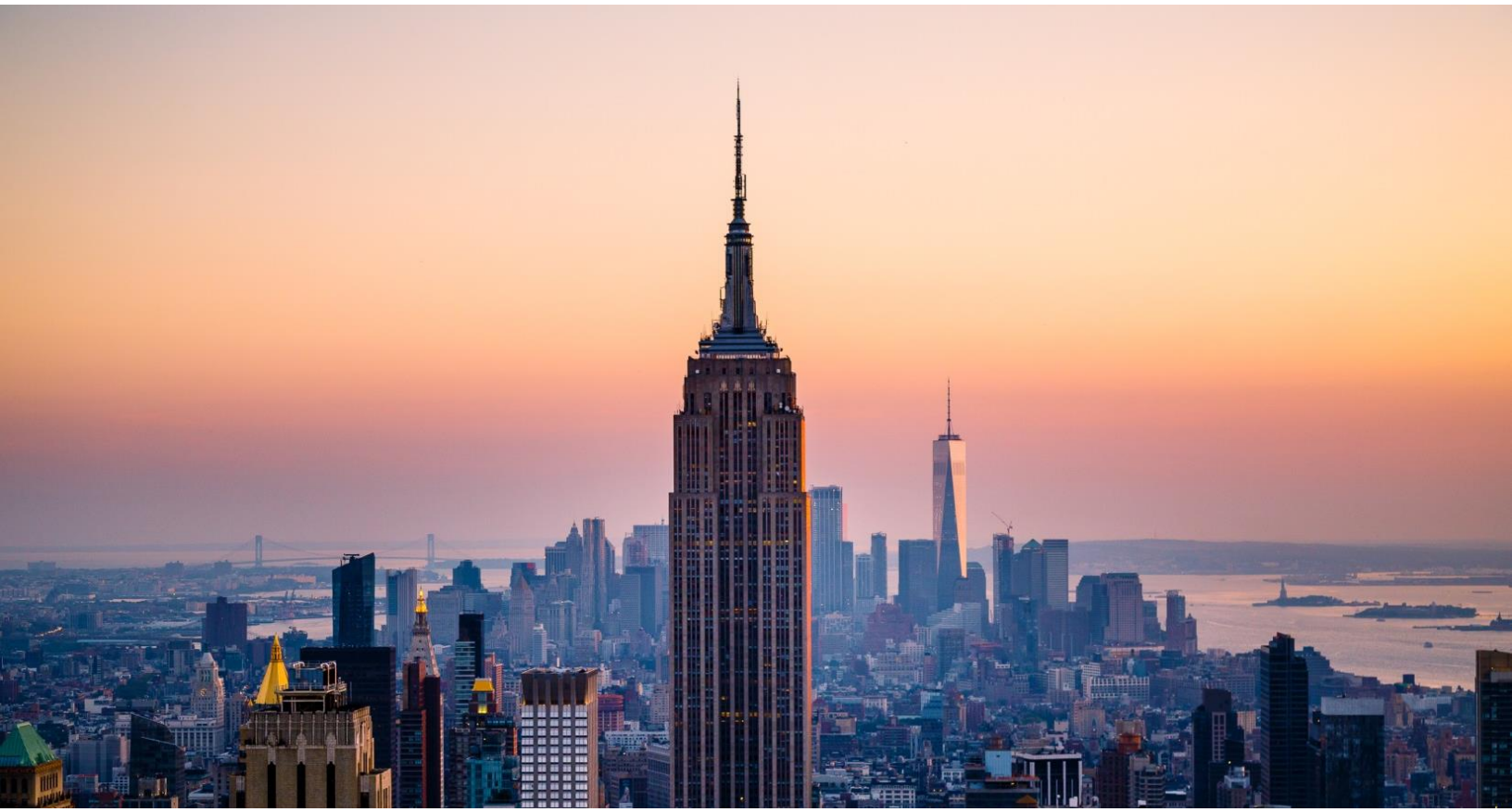
Today these tools deliver paramount cyber security insight to organizations worldwide.

Gold Finger's uniqueness is in its unrivaled ability to deliver accurate effective permissions and privileged access insight, which are paramount for Active Directory security and cyber security.

For more information, please visit – www.paramountdefenses.com/products/goldfinger

About Paramount Defenses

Paramount Defenses is the world's only cyber security company that possesses the paramount capability to be able to accurately assess privileged access in Active Directory deployments.



Microsoft Active Directory Domain Services are the foundation of cyber security and the heart of privileged access at 85% of all business and government organizations worldwide.

Paramount Defenses was founded by and is led by former Microsoft Program Manager for Active Directory Security. The company's unique, innovative, patented technology governs the accurate assessment of all access, including privileged access, in IT environments worldwide.

Its unrivaled solutions can accomplish the remarkable feat of being able to automatically and accurately assess privileged access across entire Active Directory domains, at a button's touch.

From the United States of America to Australia, its global customer base spans six continents and includes numerous prominent business and government organizations across the world.

www.paramountdefenses.com


PD