Gold Finger

Active Directory Security Auditor

Datasheet

Gold Finger

Active Directory Security 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 require the ability to frequently inventory their foundational Active Directory and perform basic Active Directory security audits to maintain security, operate a healthy Active Directory and fulfill various governance, risk and compliance driven audit needs.

Architected by former Microsoft Program Manager for Active Directory Security, and endorsed by Microsoft, the *Active Directory Security Auditor* from Paramount Defenses helps organizations fulfill all their basic Active Directory inventory and security audit needs.

> *"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 Security 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 the domain security groups that protect almost all organizational IT resources, are stored, managed and secured in Active Directory.

Since the entirety of an organizations identities (user accounts) are stored in Active Directory, Active Directory is the focal point of numerous basic security audits that involve assessing and maintaining the state of all the domain user accounts that represent these identities.

In addition, because Active Directory also stores all domain computer accounts, security groups, published printers, and various other objects such as service connection points, organizations periodically need to perform Active Directory inventories and clean-ups.

Thus, to ensure the basic security of all organizational identities (domain user accounts), maintain a secure and healthy Active Directory and fulfill various GRC driven audit needs, organizations need to be able to perform basic Active Directory security and inventory audits.

The *Active Directory Security Auditor* fully enables organizations to easily, efficiently and cost-effectively perform basic Active Directory security and inventory audits. It can –

- ✓ Automatically inventory all Active Directory content.
- ✓ Generate numerous basic, customizable Audit Directory security audit reports that cover various essential reporting aspects of domain user account management, such as true last logon reports as well as various domain user account state and status reports.

It thus enables organizations to easily perform basic yet essential Active Directory security and inventory audits needed to maintain security and fulfill audit and compliance needs.

Active Directory Security Auditor

Features

The *Active Directory Security Auditor* embodies many thoughtful features specially designed to help IT personnel easily perform Active Directory inventory and security audits –

1. Fully Automated Audits – Inventory Active Directory at the touch of a button
2. 100+ Built-in Reports – Instantly generate 100+ audit and inventory reports
3. Fully Customizable Audits – Easily customize any audit report using LDAP filters
4. Instant Data Exports – Easily export the results of all reports to CSV files
5. PDF Generation – Create professional-grade audit and inventory PDF reports

Benefits

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

1. Inventory Active Directory – Inventory entire Active Directory domains at a button's touch
2. Perform Active Directory Cleanups – Use inventory data to perform periodic cleanups
3. Perform Account Management Audits – Audit the state and status of all domain accounts
4. Fulfill Audit Needs – Fulfill various essential regulatory compliance and audit driven needs
5. Get Peace of Mind – Rest well knowing you have essential insight into Active Directory

Active Directory Security Auditor

Audit/Reporting Capabilities

The *Active Directory Security Auditor* lets organizations accurately, easily and instantly generate and export many Active Directory inventory and security audit reports, such as –

1. Generate a list of all domain user accounts, including status, state and last-logon data
2. Identify all active, inactive, locked, disabled, expired and stale domain user accounts
3. Identify all domain-joined computers and domain controllers, and their account states
4. Enumerate all domain security groups, organizational units (OUs) and other content
5. Audit and list the complete contents of any OU or the entire Active Directory domain

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 Privileged Access Auditor

Top-10 Reports

The *Active Directory Security Auditor* lets organizations easily obtain basic yet essential cyber security insights by generating Active Directory inventory and security audit reports, such as –

1. List of all domain user accounts, domain computer accounts and security groups.
2. List of all active, inactive (stale), enabled, disabled, locked and expired domain user accounts
3. List of all domain accounts and security groups marked “administrative” by Active Directory
4. List of all domain user accounts, computer accounts, security groups, organizational units, containers, published printers, GPOs, service connections points and contacts created, deleted or modified in the last 24 hours as well as in the last 7, 30, 60 and 90 days
5. List of all domain controllers in an Active Directory domain
6. List of all domain user accounts that have logged on in the last 24 hours
7. List of all domain user accounts that have failed a logon attempt in the last 24 hours
8. List of all domain user accounts that do not require passwords to logon
9. List of all domain user accounts that are not marked “*Sensitive and cannot be delegated*”
10. List of all domain computer accounts that are trusted for unconstrained delegation

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

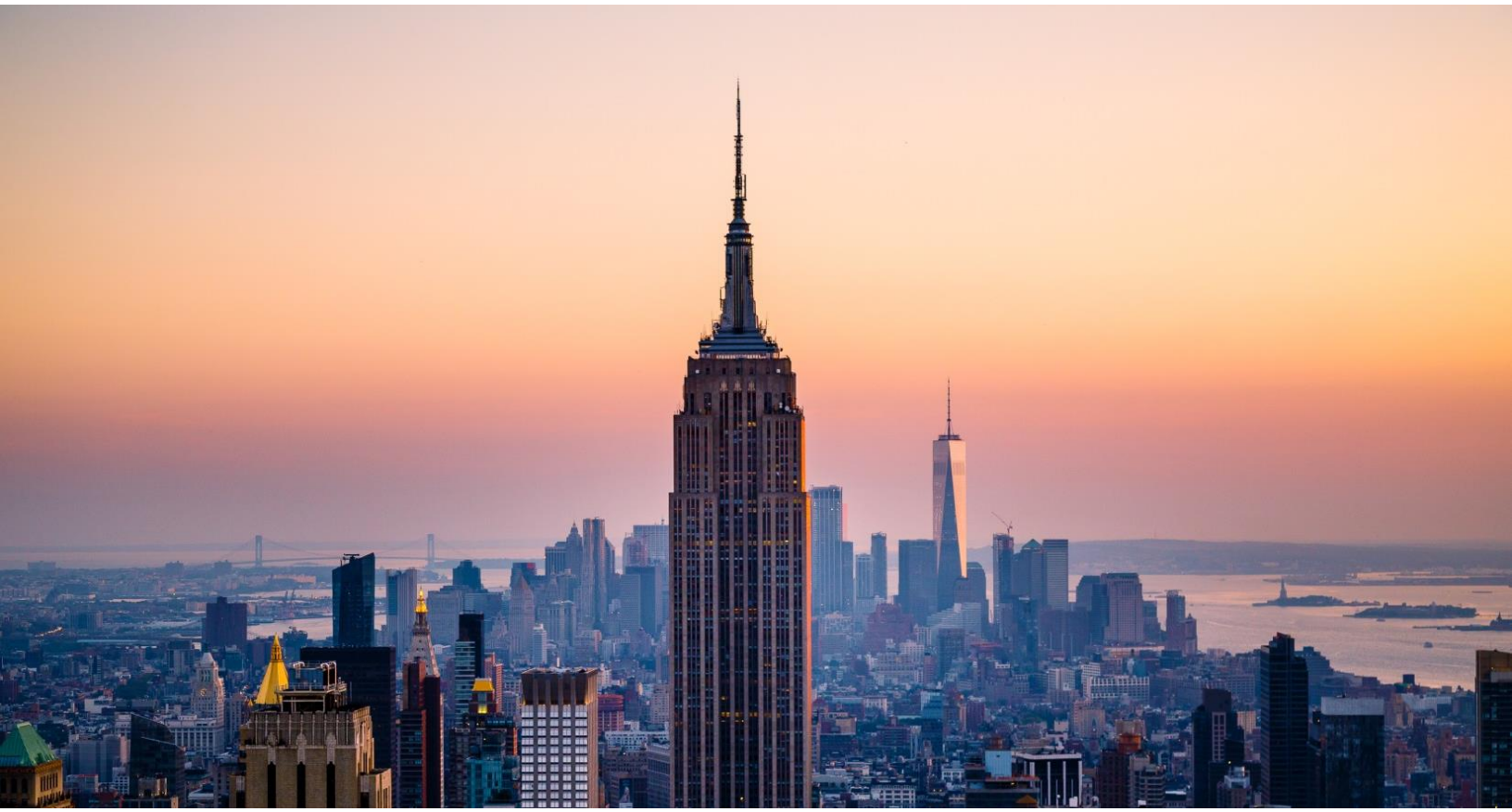
Today these tools deliver paramount cyber security insight to organizations worldwide.

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