



A security audit can help you obtain an assessment of the current security state of your Active Directory.

An Active Directory security audit is a short, systematic and methodical process that allows an organization to obtain broad high-level visibility into the attack surface and the current security posture of its organization's Active Directory deployment.

## ➤ Overview

An Active Directory security audit serves as an efficient, effective and proven means to obtain a high-level security assessment which provides a reliable foundation upon which to subsequently determine an appropriate Active Directory security risk management strategy.

It instantly delivers actionable insight into the security state of your organization's Active Directory and empowers you to obtain the executive support you may need to plan for and implement adequate Active Directory risk mitigation measures.

## ➤ Objective

The objective of the security audit is to quickly and efficiently obtain sufficient high-level insight into the security state of your Active Directory, so as to be able to determine and define an adequate, feasible and effective risk management strategy.

## ➤ Coverage

Our professional Active Directory security audit involves a systematic high-level assessment of all pertinent aspects of your Active Directory deployment, including but not limited to your enterprise design, trust relationships, domain controller placements, administrative delegation model, directory access rights, management practices, disaster readiness etc.

## ➤ Process

Our professional security audit is performed on-site and involves a variety of audit measures including but not limited to reviews of enterprise designs, delegation models and management practices, assessments of domain controller and key Active Directory configuration security policy settings, interviews and discussions with administrative personnel etc.

## ➤ Deliverables

The findings of the security audit are delivered in the form of a security audit report that presents a complete, high-level assessment summarizing the current security state of all pertinent aspects of your Active Directory deployment, including –

1. An overview of the organization's Active Directory deployment
2. An executive summary of the findings of the security audit
3. A high-level assessment of the following aspects of your Active Directory deployment (; not an exhaustive list) –
  - Enterprise design and trust relationships
  - Domain controllers and administrative workstations
  - Administrative authority delegation model
  - Management practices, policies and procedures
  - Security incident response and/or disaster recovery readiness
  - Identity, access and directory service management auditing measures
4. A high-level summary of the risks to your Active Directory deployment
5. A high-level summary of suggested security risk-mitigation measures

A summary of findings can also be presented (optionally) to an audience of executive decision-makers and stakeholders.

## ➤ Confidentiality

Our security professionals take pride in delivering world class service with absolute integrity. Your information never leaves your premises and no data is accessed or persisted anywhere without your prior knowledge and consent. You also have the option of requesting supervised security audits and/or requesting that our security professionals use laptops provided by your organization for conducting the assessment. Our security professionals completely understand and respect the need for absolute confidentiality.

## ➤ Logistics

The security assessment is performed on-site at your location by our professionals in collaboration with your IT group.

## ➤ Duration

The security assessment requires two to four business days, depending on the size of your Active Directory network.

## ➤ Benefits

Our professional Active Directory security audit service can help you quickly obtain a high-level security assessment of your Active Directory deployment and subsequently determine an appropriate Active Directory security risk management strategy.

➤ **Scheduling**

Our professional Active Directory security audit service is scheduled on a first-come-first-serve basis. A minimum of one week notice is required to schedule a security audit.

➤ **The Paramount Defenses Advantage**

Paramount Defenses Inc, a valued Microsoft partner, is a global IT security solutions company that develops and delivers innovative IT security solutions and services. It was founded by and is led by former Microsoft Program Manager for Active Directory Security and its solutions and services are deployed at and used by over 1000 organizations in 60 countries.

Our unique and professional Active Directory security services were developed by former Program Manager for Active Directory security on Microsoft's Windows Server development team, who was responsible for all aspects of Active Directory security for Microsoft Corporation.

Our security professionals possess unrivaled Active Directory security experience, and in fact only our security experts have the unique distinction of having performed a risk assessment of Microsoft Corporation's own global mission-critical Active Directory deployment.

Our experienced IT security professionals specialize in helping organizations secure their Active Directory deployments. They all possess the unique distinction of having previously worked either for Microsoft or having worked for valued Microsoft partners. Many of them earned their professional Microsoft certifications as early as 1996.

Over the last eight years, our security professionals have helped numerous organizations adequately enhance the security of their Active Directory deployments and have performed Active Directory security audits and security assessments for prominent organizations including Fortune 100 companies.

➤ **Engage**

For more information or to schedule a Security Audit, please visit us online at [www.paramountdefenses.com](http://www.paramountdefenses.com).