Unstructured Data Risk Assessment

Protect sensitive corporate data

As long as sensitive corporate data lives within an application, it’s protected through traditional identity and access management methods. However, with the productivity tools available today that help you analyze and present information to run your business, employees are potentially exposing critical information and creating significant compliance issues. And with the volume of unstructured data predicted to grow exponentially, organizations are being compelled to determine where all of the sensitive data is stored and put in place a strategy to adequately protect and manage it. With technologies available today, organizations can put in place a long-term plan for protecting and managing unstructured data, but evaluating the current environment and scanning for existing data is critical to establishing a solid foundation for the future.

The Optiv Unstructured Data Risk Assessment provides you with a comprehensive view of the location of your sensitive unstructured data and who is accessing it, as well as evaluating the overall health of Active Directory permissions. Using a combination of third party technologies, scripting tools and interviews, Optiv’s team of experts performs a risk assessment on your Active Directory data, infrastructure and policies and makes recommendations for reducing the risk of inappropriate access. At the end of the assessment, you will know the location of all sensitive unstructured data files, a complete analysis of your Active Directory policies and procedures, and a roadmap of recommendations for remediation and improving your approach to data security.

Who Moved that Governance?

71% of end users say they have access to company data they should not see.  
*2015 article Ponemon Institute Survey

How Do We Do It?

ACTIVE DIRECTORY RISK ASSESSMENT:
Deploy Microsoft tools and conduct interviews to analyze health of Active Directory and file share access controls and policies by evaluating group objects, user objects and permissions, and compare implementation to best practices.

UNSTRUCTURED DATA RISK ASSESSMENT:
Deploy third party technology that scans and identifies location of sensitive data files, highlighting files that are overexposed and may include regulated data, intellectual property and confidential information.

DELIVERABLES:
Summary of findings that includes an overall data security risk score based on analysis of unstructured data files that contain sensitive information, access permissions, current access controls and authentication policies and roadmap to address key areas of risk. In addition, an analysis of user activity and behavior over a 30-day period will be provided, highlighting risks associated with intrusion, privilege escalation and exfiltration.
Optiv's Unstructured Data Risk Assessment provides a review of your environment focusing on a risk assessment for both Active Directory and unstructured data. The Assessment, leveraging Microsoft tools, third party technology and Optiv Active Directory and identity governance experts, focuses on the following high-level objectives:

- Identify access security issues associated with the access controls and authorization process, privileged and end user monitoring, and Active Directory structure.

- Discover location of unstructured data files, including sensitive files that may contain regulatory data such as SOX, HIPAA, PCI, GDPR and BLG, as well as stale data files that should be archived or deleted.

- Create roadmap that defines remediation path addressing data security risk issues and establishing an approach for governing sensitive unstructured data.

**BENEFITS OF OPTIV’S UNSTRUCTURED DATA RISK ASSESSMENT**

1. **Reduced risk of a breach.** Locate sensitive corporate data contained in unstructured files and ensure appropriate permissions. Define plan for implementing tools for evaluating malicious user behavior.

2. **Better visibility and control.** Collect and analyze current state of Active Directory structure, access and authorization policies and existing permissions. Define plan for implementing tools for ongoing access governance of sensitive data.

3. **Baseline for improvements and enhancements.** Establish an optimized Active Directory structure and implementation benchmark. Set policies for controlling permissions and creation of sensitive data files.

**The Optiv Advantage**

Optiv can help businesses in every industry connect information security policies, procedures and practices with business goals. Our security leadership experts, backed by our team of consultants, can provide the experience you need to take your program to the next level.

**Expert Minds**

Optiv’s security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

**Leading Best Practices**

Our knowledge of leading best practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

**Client-First Culture**

Optiv’s passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

**Proven Methodologies**

Optiv has developed proven methodologies to help ensure superior outcomes for your projects and programs.