DG TECHNOLOGY

www.dgtechllc.com

Risk Assessment

MVISION CLOUD SECURITY RISK ASSESSMENT

Our no-cost cloud security and vulnerability analysis will help you understand the risks associated with your organization's current use of cloud services.

Enterprise cloud services offer new opportunities to increase business resources and capabilities. But protecting cloud services remains a major challenge for IT environments. A McAfee® MVISION Cloud Security Risk Assessment from DG Technology provides organizations that are seeking better business results with a clear picture of their cloud security risk posture and prioritizes improvements needed to protect their organization as they adopt cloud services.

ARE YOU UNDERESTIMATING YOUR RISKS?

Broader use of the cloud is presenting an increase in opportunities as well as potential vulnerabilities to threats. The 2019 Cloud Adoption and Risk Report reveals that most organizations use approximately 1,935 cloud services, but most think they only use 30.

The MVISION Cloud Security Risk Assessment analyzes your organization's vulnerability through common workplace application usage including:

- **Shadow IT:** Unsanctioned cloud service use
- **SaaS:** Microsoft Office 365, Salesforce, and more
- **IaaS**: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform

KEY FEATURES

- Shadow IT Assessment provides visibility into high-risk cloud services
- SaaS Assessment identifies filesharing productions risk
- IaaS Assessment detects and corrects misconfigurations
- Executive summary and detailed reporting

REQUEST YOUR RISK ASSESSMENT

DG Technology can help you gain visibility into your organization's cloud risk. Contact us today!

office 813.258.0488 | mobile 813.728.4986 | deb.gannaway@dgtechllc.com

SHADOW IT ASSESSMENT

VISIBILITY INTO HIGH-RISK CLOUD SERVICES

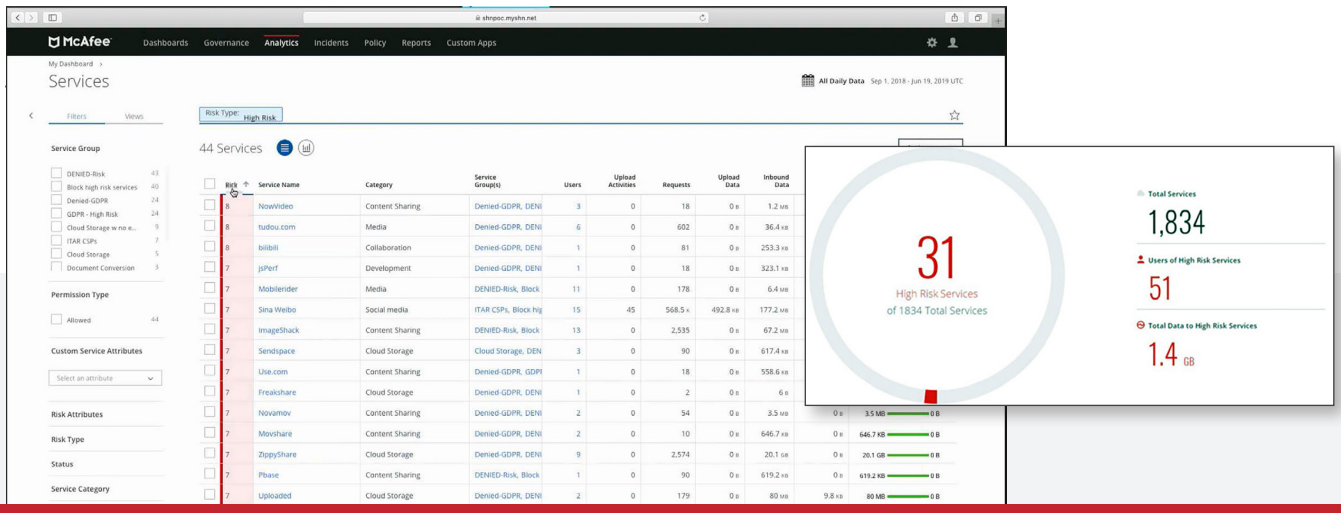
When IT assesses the use of cloud services across the organization, they generally find Shadow IT is 10 times more prevalent than they initially assumed and includes many applications and services they have never heard of before, according to a Stratecast survey. After assessing the risk of each service and its security controls, IT teams can make informed choices about which services to promote or enable.

KEY FINDINGS SUMMARY MAY INCLUDE:

- Number of cloud services in use
- High-risk cloud services
- Which services take ownership of IP
- Users who access each service
- How much data is uploaded/downloaded to each service
- Geographical location of services
- High-risk geographical locations
- Number of cloud storage services accessed
- Identify proxy leakage

ARE YOU AWARE OF YOUR VULNERABILITIES?

- Where is your corporate data?
- Who has access to it?
- What unsanctioned cloud services are in use today?
- What are the risks from unsanctioned cloud services?
- Is sensitive data being shared outside your company?
- Do you have DLP violations within cloud services?
- Are you at risk from either compromised accounts or internal misuse?
- Is your data secure when it's at rest, in motion, and in use?
- Are you compliant? (PCI, OFSI, HIPAA, GDPR, and more)
- Is your AWS/Azure/GCP configured following security best practices?
- Is your AWS/Azure/GCP configured following security best practices?



office 813.258.0488 | mobile 813.728.4986 | deb.gannaway@dgtechllc.com