MVISION Cloud Security Risk Assessment

No-cost cloud security and vulnerability analysis to understand the risks associated with an 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 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

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?

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

Learn More

Learn more about cloud-native data security for the cloud era:
www.mcafee.com/cloud-security

Request Your Risk Assessment

Have McAfee Enterprise Sales help you gain visibility into your organization's cloud risk:
Request Assessment

Connect With Us

Shadow IT Assessment

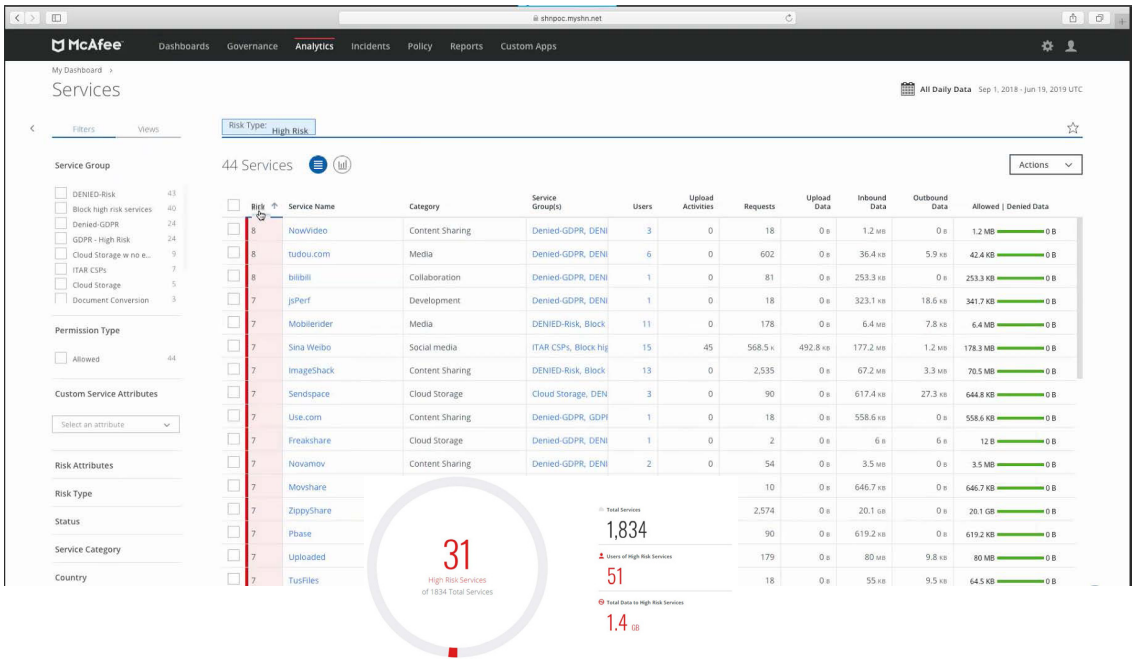
Visibility into High-Risk Cloud Services

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

Learn more about cloud-native data security for the cloud era: www.mcafee.com/cloud-security



SaaS Security Assessment

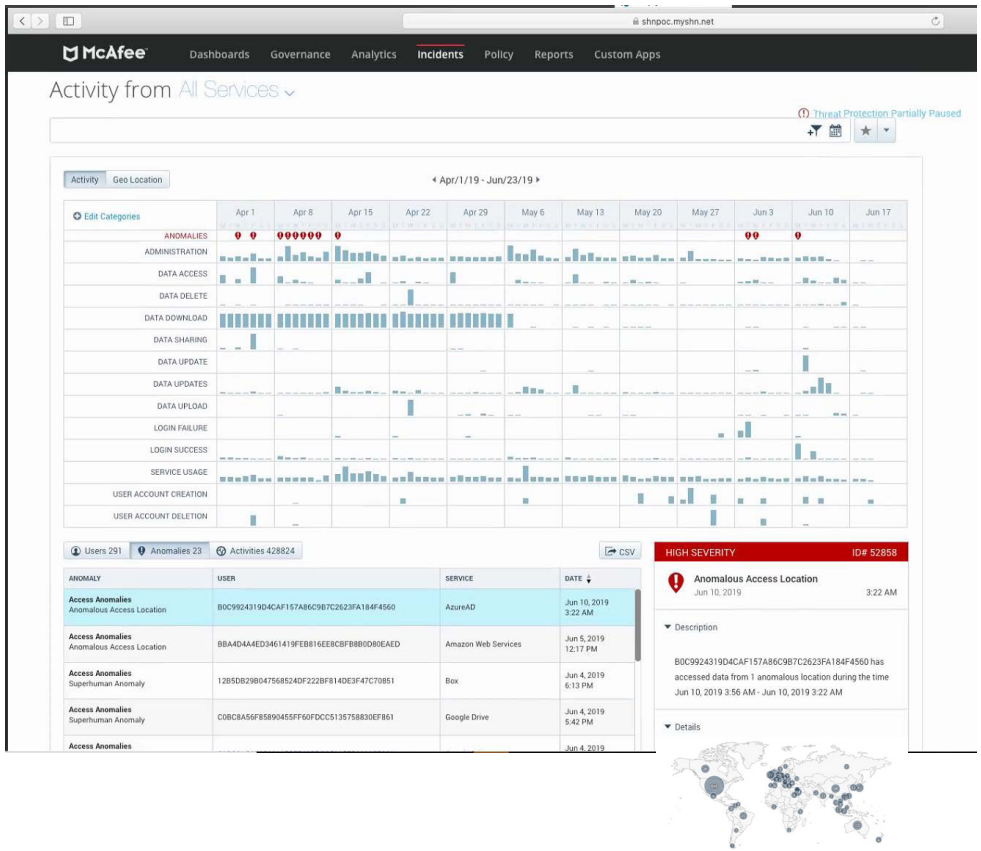
Identifying File-sharing Productions Risks

Corporate employees are using an increasing diversity of apps. In fact, 80% of workers surveyed admitted to using Software-as-a-Service (SaaS) applications, in many cases without IT approval. IT-approved apps also present a challenge. For example, threats in Office 365 grew by 63% in the last two years.

Key Findings Summary may include:

- Number of documents in OneDrive and SharePoint containing sensitive information
- Users with admin-level privileges
- Anomalous usage events indicative of threats
- Files containing the keyword “password”
- Files containing sensitive data that have untraceable links that are shareable with anyone
- Users that have access to ALL data
- Excessive user activity listing
- Unusual geographic location login attempts
- Unusual behavior analysis

Learn more about cloud-native data security for the cloud era: www.mcafee.com/cloud-security



McAfee
Together is power.

IaaS Security Assessment

Detecting and Correcting Misconfigurations

Infrastruture-as-a-Service (IaaS) providers, such as AWS, are becoming more prevalent for their ability to increase productivity and agility. However, IaaS providers also add to your organization's cybersecurity complexity. Organizations average at least 14 misconfigured IaaS instances running at any given time, resulting in an average of 2,269 misconfiguration incidents per month. Get ahead of misconfigurations before they open a major hole.

Identify misconfigurations for:

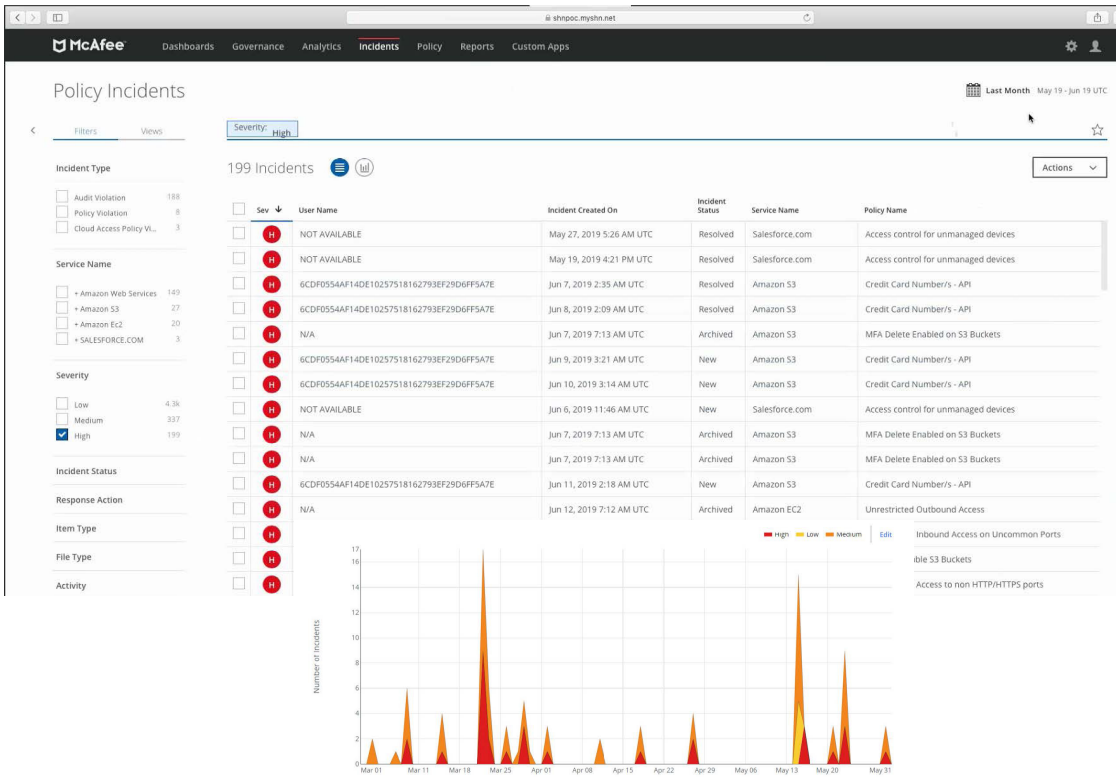
- Elastic Compute Cloud (EC2) instance
- Amazon Machine Images
- Storage services, like S3 buckets, EBS, RDS
- Identity and access management (IAM)
- Logging and monitoring series, like CloudTrail
- Network security groups and virtual private cloud (VPC) networks

Correct misconfigured services using:

- Center for Internet Security (CIS) benchmark recommendations levels 1 and 2
- Compliance recommendations for regulations such as HIPAA-HITECH, ISO, FedRAMP, ITAR, PCI DSS, or internal compliance policies

Activity reporting:

- List of managed and unmanaged AWS accounts
- Who is accessing which servers
- List of activities performed
- Geographic location and IP address
- Inactive user accounts or former employees attempting successful/failed logins



Learn more about cloud-native data security for the cloud era: www.mcafee.com/cloud-security

Little Effort, Big Benefits

MVISION Cloud Security Risk Assessment Process

Realizing the benefits of MVISION Cloud Security Risk Assessment requires very little effort, thanks to the frictionless architecture of the MVISION platform. Here's your five-step assessment process:

Step 1: Meet with the MVISION Cloud security team to determine scope of your requested assessment.

Step 2: MVISION team collects proxy (firewall) logs or sets up connection to these proxies for Shadow IT.

Step 3: MVISION team establishes API integrations for connection to SaaS, PaaS, IaaS, environments.

Step 4: MVISION team provides customer access to MVISION treatment.

Step 5: MVISION team presents MVISION Cloud Security Risk Assessment report.

Your organization will receive:

- Executive summary and detailed findings report.
- Access to MVISION tenant cloud services information and reports during the assessment.

Learn More

For more information on Cloud Security visit: www.mcafee.com/cloud-security

Request Your Risk Assessment

Have McAfee Enterprise Sales help you gain visibility into your organization's cloud risk: Request Assessment

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com