Die Cloud im Griff?

Kein Problem mit McAfee & Skyhigh!

Georg Hermann | Product Specialist Web&Data Protection
The Rise of the Cloud First Enterprise

97% of organizations use cloud services
McAfee Web Gateway Cloud Service

https://trust.mcafee.com/

Maintenance Policy
A recurring maintenance window is scheduled two times weekly on Tuesday and Thursday for improving and optimizing our service. All performed tasks are not expected to impact the service in any way. However, maintenance time will be regionalized to be least impactful for customers. Administrators or end-users impacting service updates are not part of this maintenance and will be tested explicitly including more precise information about maintenance window, i.e., start and end time.

Scheduled Maintenance #50001: ePolicy Orchestrator
Status: Planned
Start: 19th July 2017 14:00 (UTC)
End: 19th July 2017 22:00 (UTC)
Login to ePO Cloud will be disabled during this time to ensure services are back online. More details are available at support.mcafee.com.
We make the Internet faster

Cloud Infrastructure - Peering

- Reducing “Hops” = Reducing Latency
- Directly Connected to Content Providers
- https://www.peeringdb.com
We make the Internet faster

Cloud Infrastructure - Peering

- Reducing “Hops” = Reducing Latency
- Directly Connected to Content Providers
- [https://www.peeringdb.com](https://www.peeringdb.com)
- Local Browsing experience
## Some Statistics

Last 30 days - average

<table>
<thead>
<tr>
<th>Usage</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ø Bandwidth</td>
<td>24 Gbit/s</td>
</tr>
<tr>
<td>Malware Detections</td>
<td>728.76 K</td>
</tr>
<tr>
<td>Malware Detections (sec)</td>
<td>0.28</td>
</tr>
<tr>
<td>Total Requests</td>
<td>30.10 B</td>
</tr>
<tr>
<td>Traffic Volume</td>
<td>7.03 PB</td>
</tr>
</tbody>
</table>
Why us, why now?

Security is moving to the cloud - and we’re already there
- Drive down TCO and increase efficacy
- New fast infrastructure

Superior protection
- Preventing zero-day malware with machine learning (Gateway Anti Malware Engine)
- No one can touch our detection rates in Web Gateway (appliance and cloud)

Hybrid deployment
- Use your on-prem Web Gateway Policy in the cloud for your mobile users - never lose protection
- Start with web for the biggest immediate impact!
What are the package options for web?

**Appliance software (WSG+WAM) – sold as a perpetual license per user, plus support**
- Lowest cost option
- For those whose primary goal for web security is on-network protection
- Hardware sold separately (or use as virtual appliance at no extra cost)

**Cloud Service (SWE) – sold as a subscription license per user with support included**
- Mid-tier cost option
- Lowers TCO by removing the expense of purchasing and maintaining hardware
- Extends web security outside of the traditional perimeter
- Does not include appliance software

**Hybrid Web Protection (WPS) - sold as a subscription license per user with support included**
- Premier offering
- Includes both the cloud service and appliance software
- Delivers both the granularity of the appliance software plus off-network and cost-effective remote office protection with cloud
- Hardware sold separately (or use as a virtual appliance at no extra cost)
The Cloud (First) Enterprise Challenges

Data Creation and Access in the Cloud Bypasses Existing Network Security Infrastructure

95% of Network Traffic

Cloud-to-Cloud traffic

SaaS

IaaS/PaaS

Network Controls
IT'S ALL ABOUT YOUR DATA
“Data is the most valuable asset for organizations across industries.

The Economist

The world’s most valuable resource is no longer oil, but data.

The data economy demands a new approach to antitrust rules.

"Data is to this century what oil was to the last one: a driver of growth and change."
McAfee enables organizations to accelerate their business by giving them total control over their data in the cloud.
- What: Data, Apps, Users, Devices
- Who
- Where
- When

MVISION Cloud

Visibility

- DLP
- Delete/Quarantine
- Encryption
- Access
- Configuration

Control

SaaS

IaaS/PaaS

Shadow

What: Data, Apps, Users, Devices
- Who
- Where
- When

MVISION Cloud

SaaS

IaaS/PaaS

Shadow
Where is enterprise sensitive data in the cloud?

- **Salesforce**: 16%
- **Office 365**: 31%
- **Google Docs**: 7%
- **Slack**: 2%
- **Box**: 2%
- **ServiceNow**: 8%
- **AWS**: 13%
- **Custom Apps**: 11%
- **Med/Low-Risk Shadow**: 5%
- **High-Risk Shadow**: 5%

**Visibility**
Gartner CASB Magic Quadrant

Published Oct 30th 2018
Forrester CASB Wave
Published Q1 2019
Apps: Name, Configuration, Posture, Risk
Data: Classification, Tagging, Metadata
Users: Role, Activity, Collaborators
Activities: Access, Read, Write, Download, Upload...

Workloads: Details, Location, Posture
Network: Traffic, Topology
Device: Managed, Unmanaged
Location: Where, When
CASB and Web Protection
Combining forces
Secure Web Gateway and CASB convergence

Cloud Access Security Brokers
- App Risk
- API
- Reverse Proxy
- Identity
- DLP
- Malware

Secure Web Gateways
- App Control
- Forward Proxy/Reverse Proxy
- Identity
- DLP
- Malware

Synergic Efficiency
Integrated Benefits
Web Gateway CASB Integration

- Discover all cloud services in use and assess their risk against the comprehensive MVISION Cloud Registry
- Enforce acceptable use cloud governance policies based on cloud service security risk
- Upload and enforce security policies to McAfee Gateway
- Gain granular visibility into user activity and block high risk activities
- Detect and remediate policy enforcement gaps arising from proxy leakage
MVISION Cloud (CASB) Integration
Shadow IT Architecture & Closed Loop Remediation (ePO Cloud Managed)
MVISION Cloud (CASB) Integration
Shadow IT Architecture & Closed Loop Remediation (Hybrid Managed)
MVISION Cloud

Live Demo
Identify Shadow IT

My Dashboard

- **New Services**
  - 4 new services (+2, 100%) with 142 users and 14.1 MB upload data.

- **Unassigned Services**
  - 1,898 services (+111, 6%) with 327 Low, 1,550 Medium, and 21 High.

- **High Risk Services**
  - 34 services (+5, 17%) with 32 Allowed, 1 Denied, and 1 Partially Allowed.

- **Users with Uploads greater than 10 GB**
  - 19 users (+6, 46%) with 651.1 GB upload data and 520 services.

- **Torrent / Ransomware Services**
  - 0 services with 0 Low, 0 Medium, and 0 High.

- **Vulnerable Services**
  - 164 services (+15, 10%) with 949 users and 33.9 MB upload data.
Details for every cloud service – 60 security attributes

Risk Score: Last updated May 10, 2018 UTC

<table>
<thead>
<tr>
<th>Category</th>
<th>Attribute</th>
<th>Value</th>
<th>Score</th>
<th>Attribute Weight</th>
<th>Weighted Score</th>
<th>Review Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Sharing</td>
<td>File Sharing Support</td>
<td>Yes</td>
<td>80</td>
<td>12%</td>
<td>30</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Data Sharing</td>
<td>Predominant Content Type</td>
<td>Files</td>
<td>70</td>
<td>8%</td>
<td>20</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Desktop Application</td>
<td>Auto Sync of Data on User Devices</td>
<td>Yes</td>
<td>60</td>
<td>5%</td>
<td>12</td>
<td>Mar 2018</td>
<td>+</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption Strength at Rest</td>
<td>Not publicly known</td>
<td>60</td>
<td>3%</td>
<td>7</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Multitenancy</td>
<td>Encryption with Tenant Managed Keys (Data)</td>
<td>Not publicly known</td>
<td>50</td>
<td>5%</td>
<td>9</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Data Loss Protection</td>
<td>Integrated Data Loss Prevention Capability</td>
<td>Not publicly known</td>
<td>50</td>
<td>4%</td>
<td>8</td>
<td>May 2018</td>
<td>+</td>
</tr>
</tbody>
</table>
### Business Risk: 3

<table>
<thead>
<tr>
<th>Category</th>
<th>Attribute</th>
<th>Value</th>
<th>↓ Score</th>
<th>Attribute Weight</th>
<th>Weighted Score</th>
<th>Review Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Practices</td>
<td>Infrastructure Status Reporting</td>
<td>Not publicly known</td>
<td>50</td>
<td>11%</td>
<td>9</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Auditing</td>
<td>Support for Admin Audit Logging</td>
<td>Not publicly known</td>
<td>50</td>
<td>11%</td>
<td>9</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Auditing</td>
<td>Support for Data Access Logging</td>
<td>Not publicly known</td>
<td>50</td>
<td>11%</td>
<td>9</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Primarily Consumer Oriented</td>
<td>Business Type</td>
<td>Both Enterprise and Consumer</td>
<td>40</td>
<td>17%</td>
<td>9</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>EU GDPR</td>
<td>GDPR Risk Medium</td>
<td>40</td>
<td>0%</td>
<td>0</td>
<td>Aug 2017</td>
<td>+</td>
</tr>
<tr>
<td>Certifications</td>
<td>Compliance Certifications</td>
<td>SAS 70 / SSAE16 / ISAE 3402</td>
<td>10</td>
<td>17%</td>
<td>0</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safe harbor</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Legal Risk: 4

<table>
<thead>
<tr>
<th>Category</th>
<th>Attribute</th>
<th>Value</th>
<th>Score</th>
<th>Attribute Weight</th>
<th>Weighted Score</th>
<th>Review Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intellectual Property</td>
<td>IP Ownership Policy</td>
<td>SP Owns</td>
<td>70</td>
<td>23%</td>
<td>23</td>
<td>Jan 2018</td>
<td>+</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Service Adherence to Copyright Controls</td>
<td>Not publicly known</td>
<td>60</td>
<td>4%</td>
<td>3</td>
<td>Jan 2018</td>
<td>+</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Statute of Limitations</td>
<td>Not publicly known</td>
<td>50</td>
<td>2%</td>
<td>1</td>
<td>Jan 2018</td>
<td>+</td>
</tr>
<tr>
<td>Conflict</td>
<td>Dispute Resolution</td>
<td>Exclusively in SP state/county ...</td>
<td>40</td>
<td>17%</td>
<td>11</td>
<td>Jan 2018</td>
<td>+</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Privacy Policy</td>
<td>Collects and shares with 3rd p...</td>
<td>40</td>
<td>3%</td>
<td>1</td>
<td>May 2018</td>
<td>+</td>
</tr>
<tr>
<td>Geography</td>
<td>Jurisdictional Location</td>
<td>Europe</td>
<td>10</td>
<td>20%</td>
<td>2</td>
<td>Jan 2018</td>
<td>+</td>
</tr>
</tbody>
</table>
Pros:
- Known Malicious Misuse of Service: Not publicly known
- Breach Identified for Service: Not publicly known
- Support for Multi-Tenancy: Yes

Cons:
- Service Allows Anonymous Use: Yes
- Multi-factor Authentication: No
- IP Ownership Policy: SP Owns
# Get control over sanctioned apps

## Cloud Service API Configuration

Enable and monitor DLP connectivity to gain greater control and security of your data for services listed below.

**Date last updated**: Sun, 26 Aug 2018 10:26:31 GMT  
**Page refreshes every 30 seconds**.

<table>
<thead>
<tr>
<th>Status</th>
<th>Cloud Service Instance Name</th>
<th>Last Hour</th>
<th>Last Day</th>
<th>Last Week</th>
<th>Last Event Received</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running properly</td>
<td>Egnyte: Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Tue, 21 Aug 2018 11:50:46 GMT</td>
<td>Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>Tue, 21 Aug 2018 11:50:40 GMT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workplace: Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Wed, 11 Apr 2018 18:39:45 GMT</td>
<td>Disable</td>
</tr>
<tr>
<td></td>
<td>Cisco Webex Teams: Default</td>
<td>0</td>
<td>10</td>
<td>149</td>
<td>Sun, 26 Aug 2018 08:33:07 GMT</td>
<td>Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>5</td>
<td>84</td>
<td>Sun, 26 Aug 2018 08:32:57 GMT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box: skyhighdemocloud</td>
<td>2</td>
<td>42</td>
<td>415</td>
<td>Sun, 26 Aug 2018 10:00:01 GMT</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Microsoft Office 365

All Closed Incidents:
- 290
- 269 Deleted | 7 Quarantined | 14 Others

All Unresolved Incidents:
- 875
- 380 High | 327 Med | 168 Low

Setup 100% complete
- API Connection
- Policies Enabled
- Near Real Time DLP
- Email DLP for Exchange

Additional setup is required to enable DLP on Exchange emails. You will need to setup journaling, which sends a copy of the email to the DLP engine for inspection.

Setup Email DLP Learn more
“Through 2020, 95% of cloud security failures will be the customer’s fault.”

Gartner Magic Quadrant for CASB—2017
Data Exposures in IaaS—Ghost Writer

McAfee Discovers Ghost Writer – S3 Buckets Configured for Write Access open up Customers to Major Vulnerabilities
Call to Action

rethinking about your web protection
Die meisten Unternehmen infizieren sich über das Web, wie sicher sind Sie?

Was schätzen Sie, wie viele Cloud Applikationen gibt es in Ihrem Unternehmen?
Visibilität ist ein kostbares Gut.
Überblick mithilfe einer Shadow IT Analyse, bieten wir Ihnen gerne an.

O365
AWS / Azure
Gemeinsam mit Controlware helfen wir Ihnen bei Ihrer Cloud transformation