SANS Institute

InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Simplifying Cloud Access Without Sacrificing Corporate Control: A Review of McAfee’s Integrated Web and Identity Solutions

Copyright SANS Institute
Author Retains Full Rights
For enterprises deploying and making use of cloud-based services, the security landscape is changing rapidly. Traditional security tools such as endpoint antimalware and access controls are still relevant, but the increasing reliance on resources hosted by cloud-based service providers is adding new layers of complexity that require businesses to take a different approach. More applications and data than ever before are using cloud provider APIs, data is stored in the cloud without a second thought, and application architectures and use cases are relying on many layers of integration that simply didn’t exist previously. Web filtering and data loss prevention (DLP) controls must adapt to cloud access models, and identity management and authentication requirements (e.g., single sign-on, multifactor authentication or application integration) must evolve as well.

In this review, we examined several new releases of McAfee's web security and identity products, including McAfee Web Gateway version 7.3, McAfee Cloud Single Sign On (CSSO) version 4.0 and McAfee One Time Password version 4.0, with Pledge Software Token (Pledge) version 2.0. For our work, McAfee set up a test environment with a simple architecture that encompasses all the core security capabilities in a streamlined fashion. This architecture is illustrated in Figure 1.

We evaluated the products in a number of common enterprise use cases that fall into three major categories. The first category—“Controlling Access”—delved into single sign-on, multifactor authentication, context-aware authentication and application controls. The second —“Protecting Data”— focused on antimalware, encryption, data loss and leakage protection, web and URL filtering, and threat intelligence. The final category—“Monitoring and Security Management”—focused on user and application configuration, activity monitoring and event logging. This review will describe both the security team and end-user experiences (where applicable) throughout these use cases.
Many cloud services are user and group centric and, thus, need strong authentication and authorization services and capabilities that mirror those of internal security and identity systems. As the authentication processes of cloud-based services become more streamlined and integrated, the likelihood that sensitive credentials will be protected when using such services increases. Unfortunately, many of these authentication mechanisms are incompatible with existing authentication controls, or simply less robust, offering minimal or no support for multifactor authentication capabilities that are commonplace in corporate IT.

The use cases in this category represent a broad list of different scenarios that are increasingly found in business. For our testing throughout the evaluation, we alternated between the roles of the administrator tasked with enforcing access rules and ordinary user “Bill Smith” (username bsmith), who is onsite (or connected via VPN) and who wants to access one or more cloud applications (e.g., Salesforce, LinkedIn or Dropbox) with or without prior permission.

**Use Case 1: Cloud-Based SSO with Two-Factor Authentication**

The first use case is simple, but covers several core elements of how many businesses and their employees will benefit from improved security when accessing cloud applications. In many such situations, each user has a login that is distinct from their corporate identity, and few cloud providers offer multifactor authentication, opting only for usernames and passwords. Users, therefore, have to remember each set of credentials, write them on a sticky note or store them in the browser. Furthermore, the lack of multifactor authentication can lead to account compromises if the cloud application provider is breached, as with the June 2012 LinkedIn password breach.¹

How can “Bill” access these cloud-based applications more securely? After logging into his enterprise network with IT-issued credentials (for our testing, stored in Microsoft Active Directory), he opens his browser, and McAfee Web Gateway directs him to the CSSO portal. The portal loads and prompts him to create a one-time password (OTP), as seen in Figure 2.

![Figure 2. OTP Prompt for the CSSO Portal](image-url)

¹ [www.computerworld.com/s/article/9227869/Hackers_crack_more_than_60_of_breached_LinkedIn_passwords](www.computerworld.com/s/article/9227869/Hackers_crack_more_than_60_of_breached_LinkedIn_passwords)
Controlling Access (CONTINUED)

This is done easily through the McAfee Pledge application, which runs on a mobile device or, as in our testing, on “Bill’s” desktop; it appears in Figure 3.

![Figure 3. Generating a Pledge OTP](image)

After entering the Pledge-generated OTP, the CSSO app portal appears, as shown in Figure 4.

![Figure 4. The McAfee CSSO App Portal](image)

From here, logged in as bsmith, we were able to easily access LinkedIn, with no additional authentication required. Behind the scenes, the entire authentication process and all resulting transaction data were monitored and protected by McAfee Web Gateway as well, preventing malware or other attacks.
Use Case 2: Service Provider–Initiated Login

The second use case is similar to the first: Users browse directly to specific applications (such as LinkedIn, Gmail and others) versus navigating to them from the CSSO portal. When “Bill” went directly to an application site (Gmail in our test case), the authentication was redirected to the CSSO portal. Instead of entering Gmail or enterprise credentials, “Bill” was simply prompted to enter a Pledge-generated OTP. Once the OTP was entered, the CSSO portal forwarded him back to Gmail, but with IT-approved authentication. As with the first use case, the session was monitored and protected by McAfee Web Gateway.

Use Case 3: Two-Factor Authentication to a Site with Dynamic URL

Some cloud applications, such as Dropbox, can generate dynamic URLs from Web forms and other methods; handling these can be difficult (if not impossible) for simple identity and access management solutions. Because McAfee Web Gateway tracks all HTTP traffic, dynamic URLs can be monitored and authentication redirected to the CSSO portal for proper, directed access to the application or acquisition of a second authentication factor. When we tested this case (using Dropbox), the session was directed back to the CSSO portal, thus ensuring proper policy application and strong authentication.
Several potential opportunities exist where business users can unwittingly reveal sensitive authentication data or expose data stored in the cloud. Users often log in to remote sites with account information, transmit account details across untrusted channels, and work with applications and services that may not fully integrate the provider’s authentication with internal authentication and authorization mechanisms. Even more pressing is the need to maintain policy continuity for encryption and DLP tools, thereby preventing users from deliberately or unwittingly storing data in cloud provider environments lacking proper protection.

The unrestricted use of cloud applications and social media, or even worse, the dissemination of malware and malicious code via cloud-based applications is a huge security concern that needs to be addressed by organizations allowing this access. How can organizations detect threats to users coming from social media networks or cloud services? With a security offering that includes threat intelligence and access control for specific applications and services, organizations can begin mitigating such threats.

**Use Case 4: Encrypting Files Stored in the Cloud**

Certain types of sensitive data should be monitored and protected when sent to cloud-based applications. Many varieties of encryption can be applied to data at rest and in transit between secure network locations, but the most effective tend to be the simplest and most transparent. In this case, “Bill” needs to upload a file to Dropbox. The file *test123.txt*, containing a single line of text (“testing the encrypt for dropbox”), was used for this test. After logging in with normal enterprise credentials, we opened a browser and navigated to the CSSO portal, entering an OTP. From the portal, we clicked the Dropbox icon to access the service.

Once logged into Dropbox as *bsmith*, we then uploaded *test123.txt*. The upload worked as expected: While the file uploaded, it was automatically encrypted by McAfee Web Gateway, which we verified by logging into Dropbox from a system outside the protected network (a machine outside our test environment). The file could be accessed in Dropbox, but the contents were encrypted, as illustrated in Figure 5.

![Figure 5. Unencrypted (left) and Encrypted (right) Dropbox File](image-url)
Use Case 5: DLP Policy Control for Sensitive Files

In some cases, data should not be permitted to leave the organization at all, even when encrypted. In most enterprises, DLP tools are employed to identify specific pattern matches within data at rest, in use or in transit. In this case, “Bill” wants to upload a file containing credit card numbers to Dropbox so that he can access it later and process customer accounts from home (or worse, sell these numbers to criminals). This is a violation of the organization's policy as well as PCI DSS requirements and should be explicitly forbidden.

McAfee Web Gateway can perform DLP functions and policy control for all content exiting the network. When “Bill” accesses Dropbox (as in Use Case 4), he attempts to upload the file `Credit_Card_Numbers.csv`. After proceeding through the Dropbox upload sequence, he receives a DLP error message in the browser, as shown in Figure 6.

![DLP Block Message for Credit Card Data](image)

**Figure 6: DLP Block Message for Credit Card Data**

Use Case 6: Controlling Access to Cloud Apps and Social Media

Controlling and restricting access to potentially dangerous online sites and services is a standard enterprise information security function. In this case, “Bill” wants to access Twitter, which is normally allowed, but the information security team has learned that Twitter has been compromised. For this reason, access to Twitter is temporarily disabled to prevent account information from being leaked or potentially malicious content from affecting enterprise users.

Blacklisting or whitelisting Twitter, or other cloud applications, is a simple task for McAfee Web Gateway. An administrator creates an Application Control rule that controls access to one or more specific sites, applications or categories; rule creation takes a minute or two in many cases. In our example, “Bill” attempts to access Twitter in the browser (which also leverages CSSO to provide strong authentication) and is presented with the message shown in Figure 7.
When the Twitter breach has been resolved to the organization’s satisfaction and the rule disabled, users can once again access the service with no hindrance.

**Use Case 7: Enable Threat Intelligence, Detect/Prevent Malware**

Site reputation and threat intelligence are also important capabilities for any web/cloud security platform. The McAfee Global Threat Intelligence service provides malicious code intelligence, reputation analysis and general threat categorization information to many of McAfee's products, including Web Gateway. In this case, we simulated the download of a malicious file by accessing a URL at the malware test site CSM-Testcenter.org, as shown in Figure 8.
When we clicked the URL, McAfee Web Gateway identified the content as malicious, blocked it and caused the browser to display the error message shown in Figure 9.

![Figure 9. McAfee Web Gateway Blocking Malicious Web Content](image-url)
For security teams, the ability to capably and easily configure and establish security policies and controls for cloud services is paramount. In addition, managing services such as web content filtering, SSO and robust authentication control must be as simple as possible, with all or most capabilities accessible from a single console. It should also be possible to manage logging and monitor identity and security services from a single console.

**Use Case 8: Monitoring Cloud-Based Single Sign-On**

Monitoring the use of cloud services is important to a number of organizational groups, including IT operations, information and compliance teams, and business units that are provisioning services without IT's involvement (sometimes, without IT's knowledge). By monitoring the use of cloud identity services in real time and analyzing usage logs, organizations can create a baseline of how cloud accounts are actually used, along with other useful information for security and compliance efforts.

We tested the monitoring of cloud account use by logging into the CSSO Management Console, which provides several ways to monitor and review logs and login information. The first is the Activity Dashboard, where login activity can be monitored in real time. In Figure 10, two separate logins within five minutes of one another can be seen in the graph on the left.

![Figure 10. SSO Activity Monitoring](image)

Audit logs are also easily accessible, by clicking on the Logs tab and then choosing specific filters for what is to be monitored, as seen in Figure 11.

![Figure 11. Audit Logs](image)
Finally, login history can be viewed in the Monitoring section, shown in Figure 12.

Figure 12. Login History

Several other types of alerting and monitoring are available within the CSSO Management Console, but these were not reviewed as part of our evaluation. In general, we found the number of event and log types, as well as the flexibility of searching and downloading the events, to be more than adequate for most security and compliance teams.

**Use Case 9: Configuring CSSO Connectors**

When a new cloud application is provisioned by a business, integrating it with existing user repositories and identity standards is important, and it should be possible to restrict access to particular users and groups. In the case of McAfee’s tools, a “Cloud Connector” enables CSSO to connect to and provide identity and SSO services for a specific cloud application such as Salesforce.com or Google Apps. Similarly, an “Identity Connector” enables CSSO to connect to and communicate with an identity source, such as Microsoft Active Directory or another authentication service. Once created, the Identity Connector allows CSSO to authenticate the user against the identity source. Both connector types may be configured through the CSSO console’s Cloud Connectors tab, offering policy control and strong authentication. We found configuring new CSSO connectors on our test bed to be simple and straightforward.

After clicking the Identity Connector radio button, the list of existing connectors displays; by selecting the New Identity Connector button, administrators can create new ones. Connectors can then be edited to specify their type, such as a chain of authentication components, Lightweight Directory Access Protocol (LDAP), Active Directory or other credential stores, as shown in Figure 13.
CSSO’s wizard-driven interface enables administrators to set authentication type(s), login page specifics (if desired), additional options and policy controls, such as time/date or IP address-based restrictions for certain users and groups, as shown in Figure 14.

Using the wizard, we were able to easily edit and configure Identity Connectors that flexibly handled different user repositories and authentication types.
Use Case 10: Configuring One-Time Passwords

Configuring specific connectors for cloud-based applications is the second piece of the CSSO puzzle. With existing identity repositories and specific authentication criteria defined, organizations can develop connectors that logged-in users can easily and transparently utilize through the CSSO portal. The use case we explored focused on adding an OTP to cloud connectors.

Clicking the Cloud Connectors button presented us with the list of defined connectors, which we could modify by clicking the Edit icon. Identity Connectors can be added here (including features such as OTPs), and Security Assertion Markup Language (SAML) attributes can be specified. Finally, specific authorization enforcement rules (e.g., time, date and IP address) can be added, as shown in Figure 15.

We found the process of creating and editing Cloud Connectors to be simple and intuitive (although the SAML options were not evaluated). In particular, the connectors’ authorization rules use clear Boolean syntax and rule elements that were easy to create, and one can get as granular as desired.
Use Case 11: Account Provisioning for Cloud Policy Control

Provisioning user accounts for the various cloud services defined in and accessed through CSSO is a critical task that could be complex if approached clumsily. Fortunately, McAfee provides the Provisioning Studio tool to help administrators more easily configure accounts and provision them within cloud applications. (We did not thoroughly test this tool or its capabilities during our evaluation.) Figure 16 shows this console in its Salesforce Provisioning mode.

Use Case 12: Web Access and Content Management

In our final use case, we evaluated the ability of security administrators to view any activity relating to CSSO and cloud applications coming through McAfee Web Gateway. This is a simple use case, as McAfee Web Gateway offers robust alerting and monitoring, with granular filter sets that can accurately and easily monitor these events.

First, we logged into the Web Gateway management console and then selected the Errors filter on the dashboard under Alerts. As implied, this shows any error messages regarding applications and their communication with Web Gateway and the CSSO platform, as shown in Figure 17.

Figure 16. Salesforce Provisioning with McAfee Provisioning Studio

Figure 17. CSSO Alerts in the McAfee Web Gateway Dashboard
Another view of activity can be seen on the dashboard by choosing the *Charts and Tables* view; admins selecting *Single Sign On Statistics* can view more granular information about SSO logins and traffic, as shown in Figure 18.

![Figure 18. Granular SSO Login and Traffic Statistics](image)

To configure which events to monitor and how the McAfee Web Gateway will manage traffic to and from CSSO, we selected the *Policy* tab and then clicked *MCSSO Authentication* under the *Complex Login* category. Here, all controls specific to how McAfee Web Gateway functions with CSSO will be set, as shown in Figure 19.

![Figure 19. Configuring CSSO Authentication in McAfee Web Gateway](image)

We did not make changes to this group of settings, so as not to disrupt the shared test environment.
Overall, the combination of McAfee Web Gateway version 7.3, McAfee Cloud Single Sign On version 4.0 and McAfee One Time Password version 4.0 provides a strong set of controls for enabling safe use of cloud and online applications. The web protection features include inbound traffic control and protection incorporating antimalware, attack protection for cloud applications, McAfee Global Threat Intelligence for reputation assessment, DLP and encryption for outbound traffic, and fundamental application access and policy controls. McAfee's newest identity and access management products provide SSO, directory and cloud application integration, account provisioning/deprovisioning, strong authentication with OTP, and capable monitoring and management features.
Among the nine threats identified in the Cloud Security Alliance’s “Top Threats to Cloud Computing” research, account hijacking is one of the most serious on the list, and abuse of credentials is not far behind.\(^2\) Examples abound of cloud service user accounts being hacked and used maliciously. To combat this threat, organizations need to focus on the implementation and nature of identity and access management standards and tools when employing cloud services, and carefully monitor the use of those services thereafter.

Traditionally, IT security teams have found it difficult to implement identity and access management tools that are poorly integrated with more traditional security controls such as content filtering, DLP and network monitoring. McAfee’s combination of identity management and multifactor authentication with web monitoring and filtering is designed to help organizations overcome those challenges.

Throughout the evaluation, we found the products to work as advertised, and the ease of use for all management consoles and configuration options was top-notch. The integration between the products was also self-evident, which will certainly make the lives of security and operations teams easier as they look to define policies and provide a sound level of protection for cloud application users, all while minimizing any impact to the rapidly changing needs of business users.

Dave Shackleford is the founder and principal consultant with Voodoo Security, a SANS analyst, instructor and course author, and a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert, and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft and CTO for the Center for Internet Security. Dave is the author of the Sybex book Virtualization Security. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.
## Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>