



White Paper

Securing Cloud apps –

BlueGem Total Privacy Google apps Edition

BlueGem Security, Inc.
440 N. Wolfe Rd.,
Sunnyvale, CA 94085
U.S.A.
www.bluegemsecurity.com

Improving Google apps security

Security in Cloud computing applications, most notably, Google apps, has long been emphasized on the server side while most hackings now target the endpoints. Proliferation of nearly-impossible-to-catch malware constantly pose serious threats, meaning that the user to know will never know whether they are at risk or not.

Google apps security should include the last mile protection that goes beyond protecting the User ID and Password. Identity protection in Google apps is centered on access security, and leverages the Secure Socket Layer (SSL) based access method, and it implicitly relies upon antivirus protection on the endpoint. This security approach leaves a very real vulnerability in the endpoint, since antivirus software is no longer effective against rapidly evolving malware such as zero day attacks.

Existing access security solutions, such as multifactor authentication, are unable to completely protect end users from these rapidly evolving threats. The following explores the challenges faced by existing access and endpoint security solutions that are typically used in conjunction with Google apps:

One Time Password (OTP) secures login credentials from malware and network spoofing attacks. However, OTP provides only limited protection for login credentials (user id and password) but other confidential information contained in emails and financial information is left with no protection. In addition, the cost of deployment and ongoing management through the life cycle of OTP poses other challenges to service providers.

Antivirus is an essential and important endpoint security solution. It is essential for detecting and removing malware from infected endpoints. However, it lags behind malware threats which have now become very sophisticated and are constantly evolving. The addition of heuristics/behavior detection only offers limited additional protection, due to the rapid increase in false positive alarms that would otherwise be created with other software applications, which in turn creates concerns amongst the end users and drives needless end user support costs.

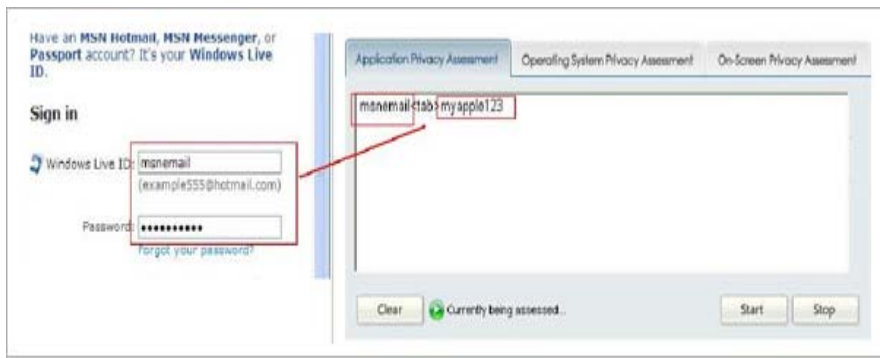
Overview of Google apps security using BlueGem solution

Identity protection in Google apps relies on network encryption technology, called SSL, however, this cannot solve the endpoint vulnerability problems caused by malware, which is the most vulnerable segment in Cloud computing. BlueGem solves this vulnerability by encrypting every keystroke using 128 bit encryption technology, thereby making it impossible for malware to intercept or steal any users' most confidential information – login credentials, ecommerce transactions, Google doc, etc. In other words, BlueGem extends network encryption from the servers in the Cloud to the keyboard on the endpoint computer, creating an impenetrable encrypted communication channel within the endpoint and in the Cloud.

In addition, BlueGem's domain-specific anti-phishing protection secures activities in Google apps and reduces the risk of information extrusion. BlueGem's multi-layer solution delivers multiple

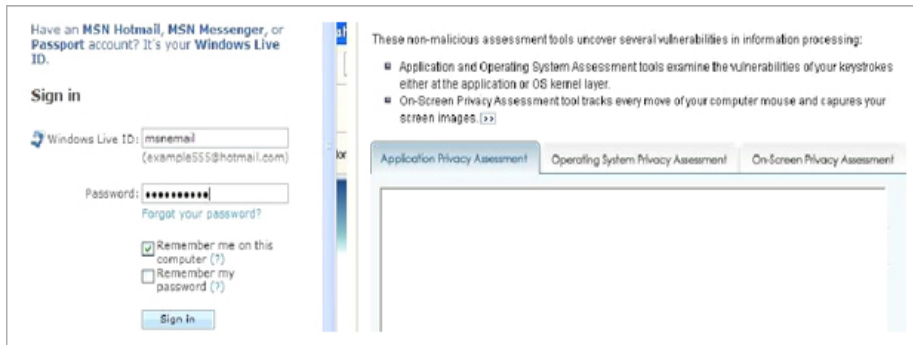
security benefits: protection from illegal screen capture on all pages as well as securing the system memory. Key security features are listed below:

- i. **Keystroke encryption:** encrypting all keystrokes that are directed to Google apps. While the user works on any Google apps application such as mail, docs, etc., BlueGem Security keystroke encryption technology blocks malware that can intercept the users' keystrokes, which is the predominant method of stealing identity information. It does this by utilizing a dual protection method: (1) a 128 bit encryption algorithm to encrypt every single user keystroke and (2) bypassing the conventional keystroke delivery channel in the Operating System where threats may reside. In other words, BlueGem Security software creates a virtual encryption channel right from the keyboard, to make all keystrokes completely invisible to both known and unknown malware.



↳ A log-in page without Keystroke Encryption applied. User id and password are captured as illustrated above

Before keystroke encryption



↳ A log-in page where Keystroke Encryption protects the user log-in. No user id and password are intercepted.

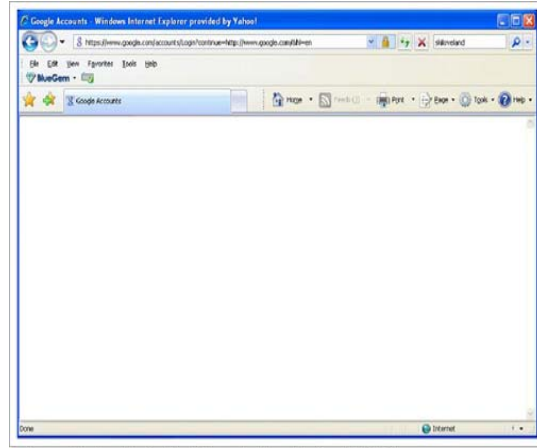
After keystroke encryption

- ii. **Screen capture protection:** this feature protects the user's information from malware that intercepts screen images. This protection feature protects against several of the toughest to catch and most virulent types of malware by preventing any information on the screen from being able to be viewed by the hacker. Some websites provide a virtual keypad, hoping to protect user log-ins from keystroke loggers, when users log on to their websites. Screen capture trojans defeat the virtual keyboard security measures by taking a screen shot every time a user clicks the virtual keyboard buttons, which can result in the

theft of user names and passwords. We completely secure virtual keyboard security logins as well as securing users from screen capture malware. BlueGem Total Privacy provides essential protection against such threats.



Without Screen Capture Protection



Screen Capture Protection takes effect by BlueGem Total Privacy

- iii. **Domain Specific Protection:** security of Google apps poses a unique set of security requirements. These include domain-specific-protection and an ability to intelligently distinguish a Google apps domain and automatically secure the user’s information while the user is on Google apps domain. When the user visits non-Google apps domains, the protection automatically goes into dormant mode.

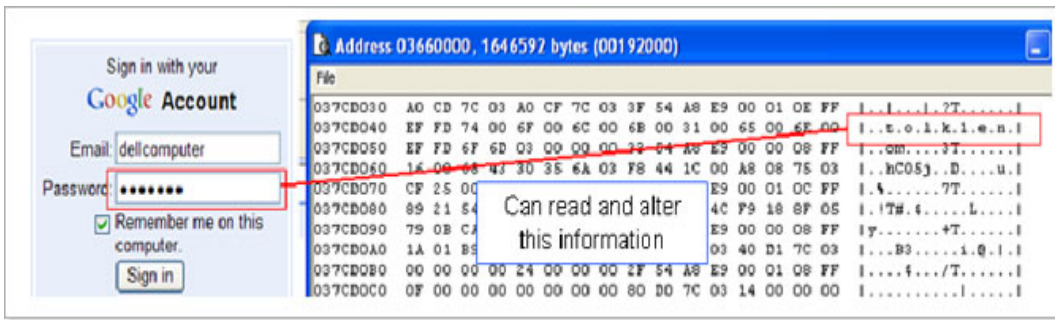
Conventional endpoint security solution, such as antivirus, operate from machine boot-up to machine turn-off and do not differentiate between online or offline activities. It also typically operates in silent mode, so that users are unaware of its operation unless they detect suspicious activities or files. However, the domain-specific-protection brings security operations to the foreground, thereby making end users aware of the presence of BlueGem’s security protection on their endpoints. This means that the domain-specific-protection for Google apps activates only when a user engages in Google apps activities for which he/she is signed up.

- v. **Anti-Phishing solution for Google apps:** the feature described above, Domain Specific Protection, helps protect against phishing of Google apps. BlueGem protection activates only when a user visits valid Google apps domains. Furthermore, BlueGem Google apps security provides visual cues, including a pop up tool tip image and a flashing tray icon that synchronously flashes with every keystroke entered, providing positive proof to the user that they are on the valid Google apps domain. This proactive reassurance feature increases user confidence that their confidential information is being fully protected. If however, the user happens to visit a phished Google apps domain, the system tray icon will not appear, so that the user will no longer see the BlueGem visual cues.

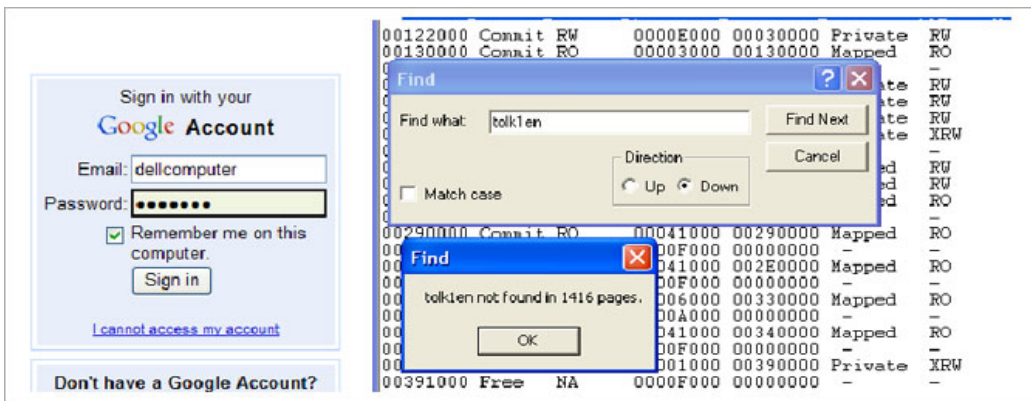


- iv. **Memory hacking protection for Internet Explorer:** when a user enters his password into the web page, whether it is a secured internet banking or non-secured site, the password is loaded in the computer system memory where the password is vulnerable to potential hacking threats. The hacker can intercept and alter the user’s password information right at the system memory as shown below. In addition, the most alarming fact about this vulnerability in the system memory is that enhanced password security tools such as OTP tokens cannot protect against this type of hacking attack, because hackers can circumvent the existing OTP protection by accessing the unprotected password in the system. This is especially vulnerable during money transfer.

In addition to keystroke encryption, BlueGem provides several additional layers of security, including a second encryption layer for your critical transactional data in the system memory. This advanced encryption technology for Internet Explorer provides the highest level of transaction security possible by protecting passwords from attack by malware, which can exploit vulnerabilities in the web browser and computer system memory where passwords are stored.



↳ Password is exposed in the system memory area. If a hacker goes directly to the memory area where the password is stored, the password information can be stolen.



↳ After encryption is applied, the password information is hidden in the memory area.

- vi. **Whitelist technology:** the whitelist technology filters and blocks unknown and malicious Browser Helper Objects (BHOs) thereby reduces the chance of the user’s Internet Explorer browser being compromised by malicious BHOs even when antivirus fails to detect or yet updated.

Value Proposition

Securing Google apps needs a unique set of requirements. BlueGem's Google apps security solution provides total privacy of user information; encrypting all keystrokes entered into Google apps, not only eliminating phishing threats using domain-specific-protection but also increasing user confidence through visual cues and being proactively able to withstand zero-day attacks.

In summary, BlueGem's Google apps security solution provides the following benefits to Google apps users.

- (1) **Securing user ID - password and protecting Google apps contents:** BlueGem uses a powerful encryption technology to encrypt the fundamental input element – keystrokes - to protect not only the Google apps log-in page but also information contents on Google apps' mail, docs, sites, Google chat, etc.
- (2) **Complimentary to existing authentication solutions:** whether or not a user has already adopted a multi-factor authentication technology for Google apps, BlueGem further enhances the level of security when accessing Google apps, by encrypting all login credentials. If a user however relies on a userID-password method, BlueGem significantly enhances the log-in credential through keystroke encryption and screen capture prevention technologies. BlueGem is an essential layer of Identity protection for Google apps.
- (3) **Zero-day protection:** whether an endpoint's antivirus protection is up-to-date or not, antivirus typically lags behind new or targeted malware attacks. BlueGem's unique security technology solves this problem and provides continuous protection to the end user.
- (4) **Single Sign-On (SSO):** SSO needs to be secured with the highest possible level of security, since it provides uninhibited access to mission critical multiple applications after login. Securing SSO with BlueGem technology would significantly increase the level of security during authentication and registration processes.
- (5) **Ease of use and deployment:** use of BlueGem Google apps security is intuitive and does not require installation or configuration on the servers in Cloud.

- END -