iboss Feature Overview

Transparent SSO Authentication for Chromebook and Android BYOD

Introduction

Google's Chromebook has grown steadily in popularity since its introduction in 2011, and while still lagging behind Apple's ubiquitous iPad, it has been gaining ground fast. According to NPD Research, Chromebook's share of the tablet and laptop markets grew from 0.4 % in 2012 to 21.1% in 2013. A national survey studying mobile technology adoption in schools, showed that 31% of schools purchased Chromebooks in 2013 up from 14% the previous year. This rapid growth in popularity is due to several factors including cost, ease-of-use and the availability of resources.

Why Chromebook is Popular

- At roughly half the price of an iPad Air, Chromebook is an inexpensive alternative to Windows-based laptops
- Chromebook is completely cloud-based, there is no software on the device itself, rendering it relatively immune from viruses
- It provides seamless integration with Google cloud services, offering comprehensive computing and applications in the cloud
- For K-12 schools, Google offers low-cost, bundled education resources
- Because Chromebook is basically a conduit to the cloud, there's no 'heavy lifting' making them very fast with little maintenance required

Feature Descriptions

Chromebook / Android BYOD Challenges

One of the main challenges to controlling Chromebook and Android BYOD once they are deployed is applying accurate policy enforcement across all users. Chromebook has no native method for applying organization policies across multiple users because there is no way to install an agent and integrate it with directory services. This means policy enforcement is relegated to IP-based device identity only, rather than per individual user, which can have a serious impact on regulatory compliance and AUP enforcement. In the case of BYOD users, policy enforcement requires accuracy to ensure privacy rights are not being compromised. Accurate reporting across both Chromebook and BYOD requires that violations and high-risk users can be readily identified with historical logs to meet compliance and forensic investigation requirements.

iboss Offers Transparent Identity Integration

iboss offers streamlined, user-based authentication for Chromebook and Android BYOD users via transparent integration with Google OAuth to provide true single sign-on (SSO) authentication across your network. This not only provides accurate policy enforcement and reporting, it assures a better end-user experience and diminishes help desk calls.

Here's how this feature works:

- End-users are prompted once, when they access the network via Chromebook or Android BYOD and asked to share their Google ID/email and profile with the organization.
- The Google ID/email address can be used to automatically login to your organization's directory services via an AD plug-in at the gateway for true transparent SSO.
- Users now have access to the network and their individual user policies can be applied to their Internet activity.
- BYOD users who do not agree to share their Google ID/Email, can be denied access to the network per your policy.

- Chromebook and Android BYOD users are now bound to policies and part of aggregate reporting across your network.
- This provides user awareness of reporting, increases visibility for infection detection, and better manages high-risk users on devices that are not directory aware.

Additional Features

The new iboss authentication capability includes some other features that streamline authentication and policy enforcement across your Chromebook and Android BYOD users:

- You can set a cookie on the end-user's browser to avoid redirecting them to Google each time they need to login. This creates a more efficient and enjoyable end-user experience.
- Increase security by setting the cookie to timeout after a length of time you choose so that the user will have to re-authenticate with Google.
- You also have the ability to cache group information in a cookies so that a user's Google Group information can be easily retrieved.

Please Note: Android/BYOD features available Q4, 2014

> ***"The manner in which their technology was architected from the beginning makes the iboss platform very good for large deployments. Their technology has the ability to scale into high-bandwidth applications with low latency — that is a distinct competency of iboss."***
>
> ***Frank Dickson***
> *Industry Director, Network Security*
> *Frost & Sullivan*

Links to More Information

Mobile Security Data Sheet

Web Security Data Sheet

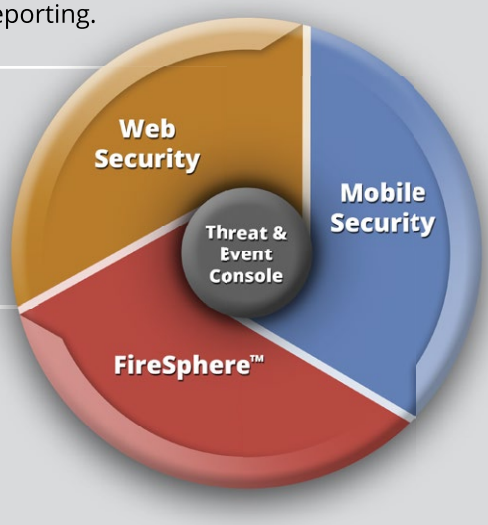
Threat & Event Console Data Sheet

BYOD Management

iboss Next-Generation Solutions

iboss patented technology protects organizations from APTs, targeted attacks and data loss with innovative Web Security, Mobile Security and FireSphere™ advanced APT defense solutions. All iboss solutions are integrated with our exclusive advanced threat SIEM single-pane-of-glass reporting.

- **Web Security with integrated BYOD and Bandwidth Management**
- **FireSphere™ for advanced defense against APTs**
- **Mobile Security with integrated MDM**



About iboss Network Security

iboss Network Security protects today's borderless networks against malware, advanced threats and data loss with innovative Web Security, Mobile Security and FireSphere™ Layered APT defense. Backed by patented technology, iboss' stream-based approach delivers unparalleled visibility across all inbound/outbound data channels and port-evasive applications, with technology that offers infinite scalability to handle the largest bandwidth demands. iboss outbound data defense includes best of breed AntiVirus, Sandboxing, data anomaly detection, and integrated SIEM-like reporting, to better detect and respond to infections already on your network. Leveraging leading threat protection and unsurpassed usability, iboss is trusted by thousands of organizations and millions of users globally.

www.iboss.com | +1 877.742.6832

iboss, Inc. (P) 877.742.6832 Sales@iboss.com U.S. HQ 9950 Summers Ridge Rd., Bldg. 160 San Diego, CA 92121
© 2014 All rights reserved. iboss, Inc. All other trademarks are the property of their respective owners.