

Bromium vSentry Status Report

**Andres Nick Georgieff
Technology Development, 9342
Software Systems Engineer
November 12, 2013**



Sandia National Laboratories



Sandia Involvement

Sandia's involvement with Bromium has reached into the following areas of evaluation and collaborative product recommendations and bug reports:

- Security
- Server Support
- User Experience
- Application Support
- Desktop Performance
- Enterprise Scalability



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



Sandia National Laboratories



Testing Methodology

The following methods were used while testing the releases of vSentry received for review by Sandia National Laboratories.

Validate that the product:

- Works as advertised and intended
- Integrates with features and functions of the operating system or applications supported by vSentry
- Meets all security requirements
- Meets or exceeds user experience expectations
- Meets enterprise scalability requirements
- Meets enterprise management requirements
- Supports the Sandia Enterprise Desktop Environment



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Sandia National Laboratories



Current Status

- **Reviewing Version 2.0 in a light pilot**
 - Bug reports
 - Feature requests
 - Deployment/Scalability
 - Overall functionality
- **Full Pilot Preparation**



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



Sandia National Laboratories



Findings

Total Items opened with Bromium

49

Fully Resolved & Closed (as of current release)

20

Known Issues

2

Open Items

27

Version Releases

Beta 1: 1 day Beta 2: 5 days Beta 3: 40 days 2.0 GA: 57 days



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



Sandia National Laboratories



Critical Items

- Firefox ESR full support
- Ingress applications breaking internal installers
- Wider enterprise deployment support
- Training materials for end users
- (partially resolved) Safe Apps vulnerable as the whitelisting is done by process name, not by signature
- (resolved) .JS, .VBS, etc. downloading as trusted from untrusted locations
- (resolved) Save malicious files for IR team



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Sandia National Laboratories



High Priority Items

- **(partially resolved) RAM allocation for large VMs**
- **Splunk reporting & integration**
- **Integrated explorer safe viewing and editing of unknown file types (.css, .js, .vbs)**
- **Quarantine malicious files**
- **FTP support for IE**
- **WebDAV support**
- **Windows 8 support**
- **Mac support**



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



Sandia National Laboratories



Moving Forward

2.0 fixes have been positive, but not comprehensive

- Pilot will be conducted to receive feedback from a test user base to determine functionality and usability.
- Post-pilot on hold until stable release that contains critical items is released and a successful pilot with feedback is completed.

Continued technical collaboration between Bromium and Sandia

- Weekly status meeting
- Bug reports
- Optimization/Experience feedback
- Feature requests



Kudos

- **Technical Staff**
- **Engineering Support**
- **Product Development**
- **Sales Staff**



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



Sandia National Laboratories



Questions



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



Sandia National Laboratories