

Bromium vSentry Status Report

Andres Nick Georgieff
Technology Development, 9342
Software Systems Engineer
October 9, 2013





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



Testing Methodology

The following methods were used while testing out 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



Current Status

- **Reviewing Beta 3 of Version 2.0.**

- Bug reports
- Feature requests
- Deployment/Scalability
- Overall functionality

- **Pilot Preparation**



Findings

Total Items opened with Bromium

48

Fully Resolved & Closed(as of current release)

17

Known Issues

2

Open Items

29

Version Releases

Beta 1: 1 day

Beta 2: 5 days

Beta 3: 40 days

2.0 GA: N/A



Critical Items

- **Firefox ESR Full Support**
- **Ingress Applications breaking internal installers**
- **.JS, .VBS, etc. downloading as trusted from untrusted locations.**
- **Safe Apps and Ingress apps vulnerable to attack as the whitelisting is done by process name**
- **Save malicious files for IR team.**



High Priority Items

- **RAM allocation for large VMs**
- **Splunk Reporting & Integration**
- **Safe viewing and editing of unknown file types (.css, .js, .vbs)**
- **Quarantine malicious files**
- **FTP support for IE**
- **Wider enterprise deployment support**
- **Training materials for end users**
- **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 beta fixes have been positive, but not comprehensive.

- Pilot held off until version 2.0 GA is released with expected fixes.
- Post-pilot held off 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.



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