SAND2016-4096C

Exceptional service in the national interest

Sandia National Laboratories

Endpoint Hardening with Bromium Micro-Virtualization

Matt Cuellar

mtcuell@sandia.gov

Christopher Nebergall

cneberg@sandia.gov

NLIT 2016

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Outline

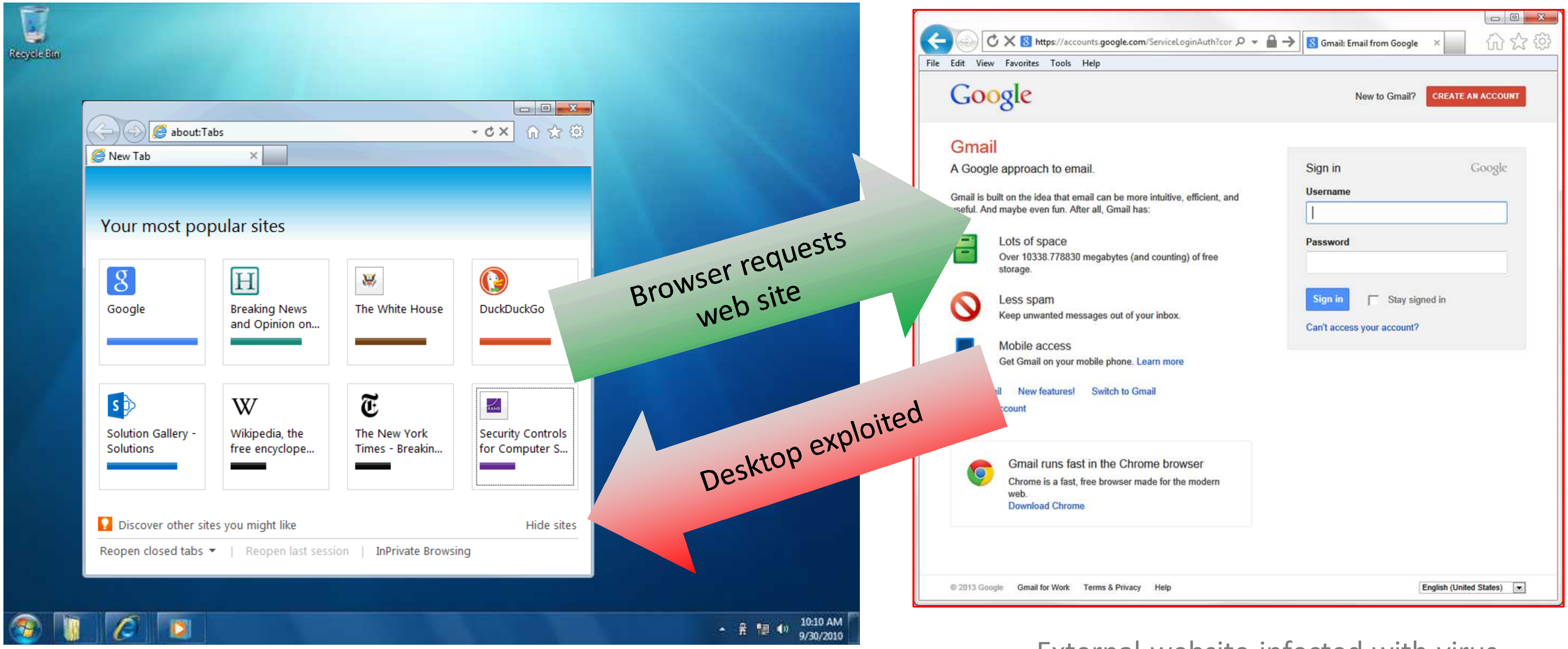
- The threat
- The Bromium solution
- How Sandia is deploying in production
- Our partnership with Bromium

The Endpoint Security Problem

- Phishing
- Internet Browsing
- Zero day flaws in applications
- Kernel Exploits

Desktop Computer - Trusted

External Web Site - Untrusted



Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Lots of space

Over 10338.778830 megabytes (and counting) of free storage.

Less spam

Keep unwanted messages out of your inbox.

Mobile access

Get Gmail on your mobile phone. Learn more

Gmail runs fast in the Chrome browser

Chrome is a fast, free browser made for the modern web.

Download Chrome

External website infected with virus

vSentry protects with hardware and software isolation

What is Bromium?

Bromium Advanced Endpoint Security

- Endpoint Protection
- Endpoint Monitoring
- Threat Analysis

Core Components Tested at Sandia

- vSentry (Software Client)
- Bromium Endpoint Controller (Management Server)

How does Bromium vSentry work?

- A separate micro-VM (uVM) container is created to host each untrusted website or supported file type
- Each Bromium uVM container isolates and restricts access to trusted resources
- Persistent monitoring on each uVM takes place with LAVA
- Malware running within the uVM is isolated from the host computer, network, and data
- Upon closing the uVM, everything within it is destroyed
- LAVA alert is sent to centralized enterprise management console

Protection and Visibility

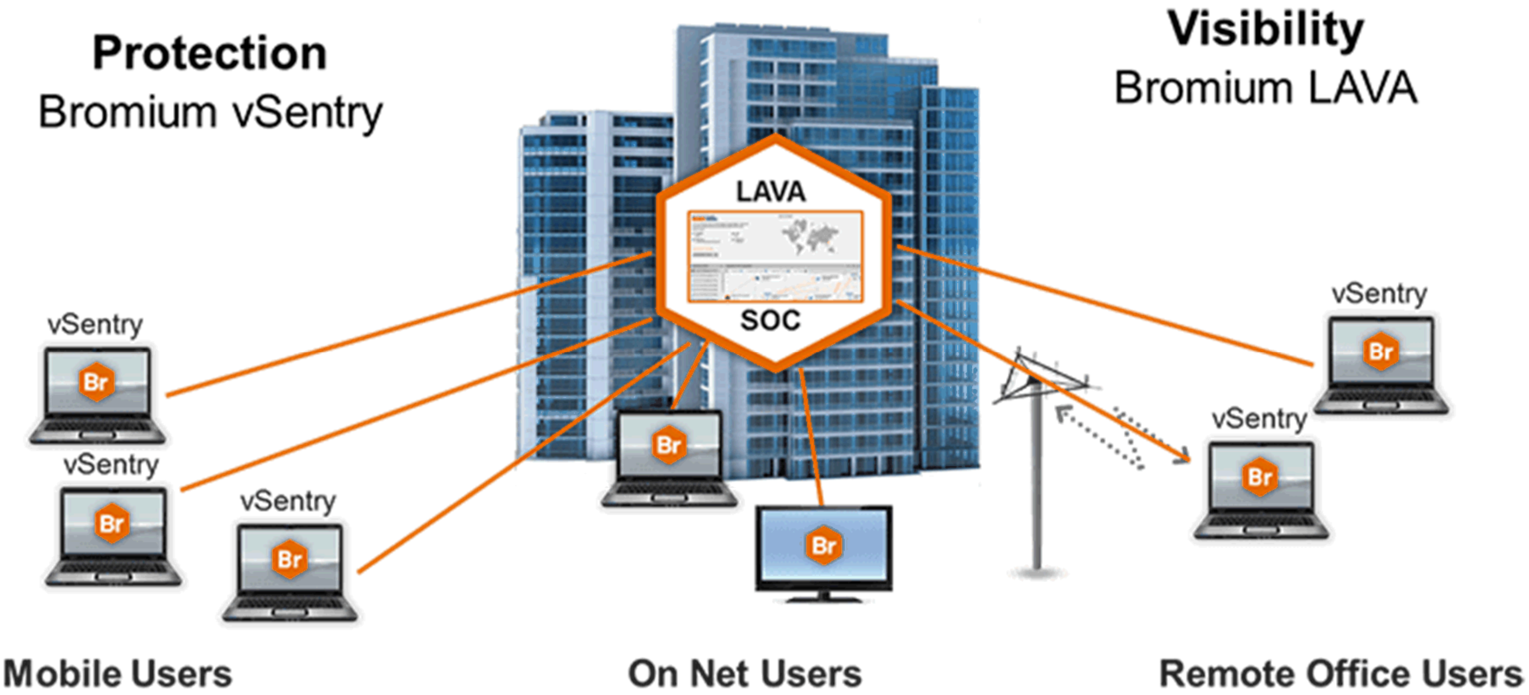
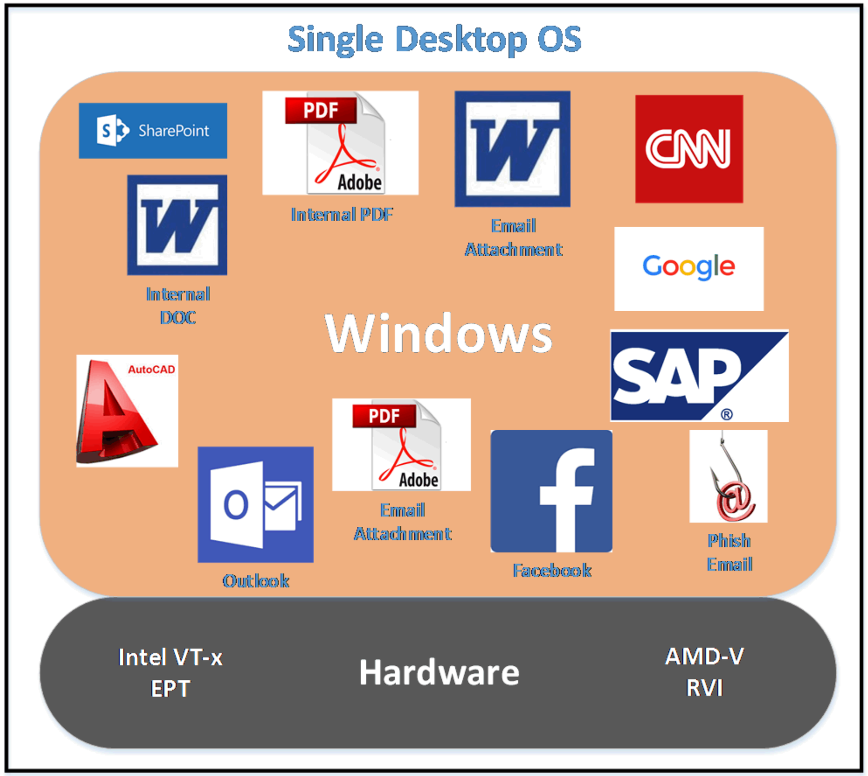
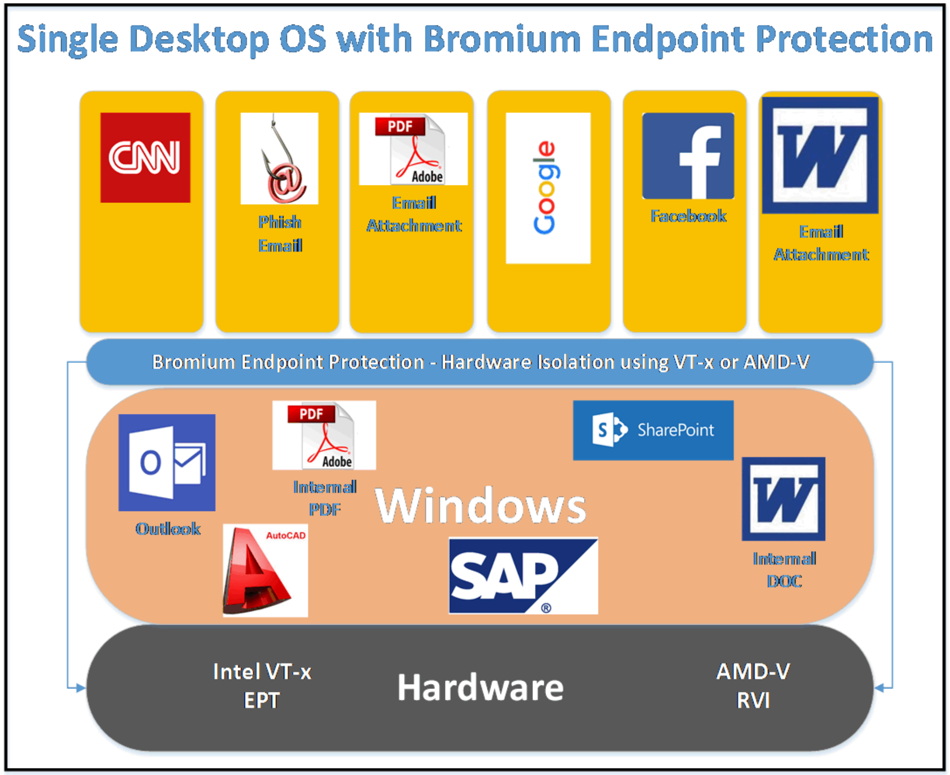


Image Credit: http://www.bromium.com/products.html

Today's Desktop vs Bromium Protected Desktop





- Slide Credit Bromium

7

How does LAVA work?

Client-Side

- vSentry LAVA engine

Server-Side

- Bromium Endpoint Controller
- Attack visualization
- LAVA manifest data
- MAEC reporting
- Syslog support
- Site to site reporting capabilities

Supported Software

- Windows 7, 8.1
- Windows 10
- Mac OS X
- Internet Explorer 9-11
- Chrome 30+
- Firefox ESR 45+
- Office 2010, 2013
- Office 2016 (beta)

- Outlook 2010, 2013
- Windows Media Player
- MS Silverlight
- Java 6-8
- Adobe Reader 9-11, DC
- Adobe Acrobat 10, 11
- Adobe Flash

Requirements for running vSentry

- Intel Virtualization Technology (VT-X) or AMD Rapid Virtualization Indexing (RVI)
  - VT-X with EPT
  - AMD-V with RVI
  - Provides CPU and memory isolation
- Minimum hardware:
  - Core i5, i7, and some i3 and Xeon processors or AMD processors with RVI
  - Minimum 4 GB RAM
  - Recommended 6 GB RAM
  - Minimum 8 GB free disk space
- Bromium Enterprise Controller
  - Policy distribution
  - LAVA report analysis

Demonstration

Deployment at Sandia

- Currently deployed to 450+ systems in production
- Scaling deployment numbers up weekly
- Currently only deploying with IE protection
- Windows 10 support in testing
- Challenges
  - Hardware requirements may not be met with older systems
  - Tuning the whitelist
  - Currently implementing many other changes

Sandia's Partnership with Bromium

- Sandia's enterprise agreement has been extended to all DOE/NNSA sites
- Sites may participate in pilots and production deployment with no upfront charges
- Requires participating in a data-sharing agreement with Sandia
- Sandia provides cyber expertise in identifying attacks against your site

Questions

- Deployment Process
  - Pre-select qualifying machines and organization
  - Notify manager
  - Manager may assign testers before deployment
  - Push installer after normal work hours