SAND2015-2937C

Exceptional service in the national interest

Sandia National Laboratories

Endpoint Hardening with Micro-Virtualization

Andres Georgieff

angeor@sandia.gov

Christopher Nebergall

cneberg@sandia.gov

2015 DOE Cybersecurity Training Conference

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

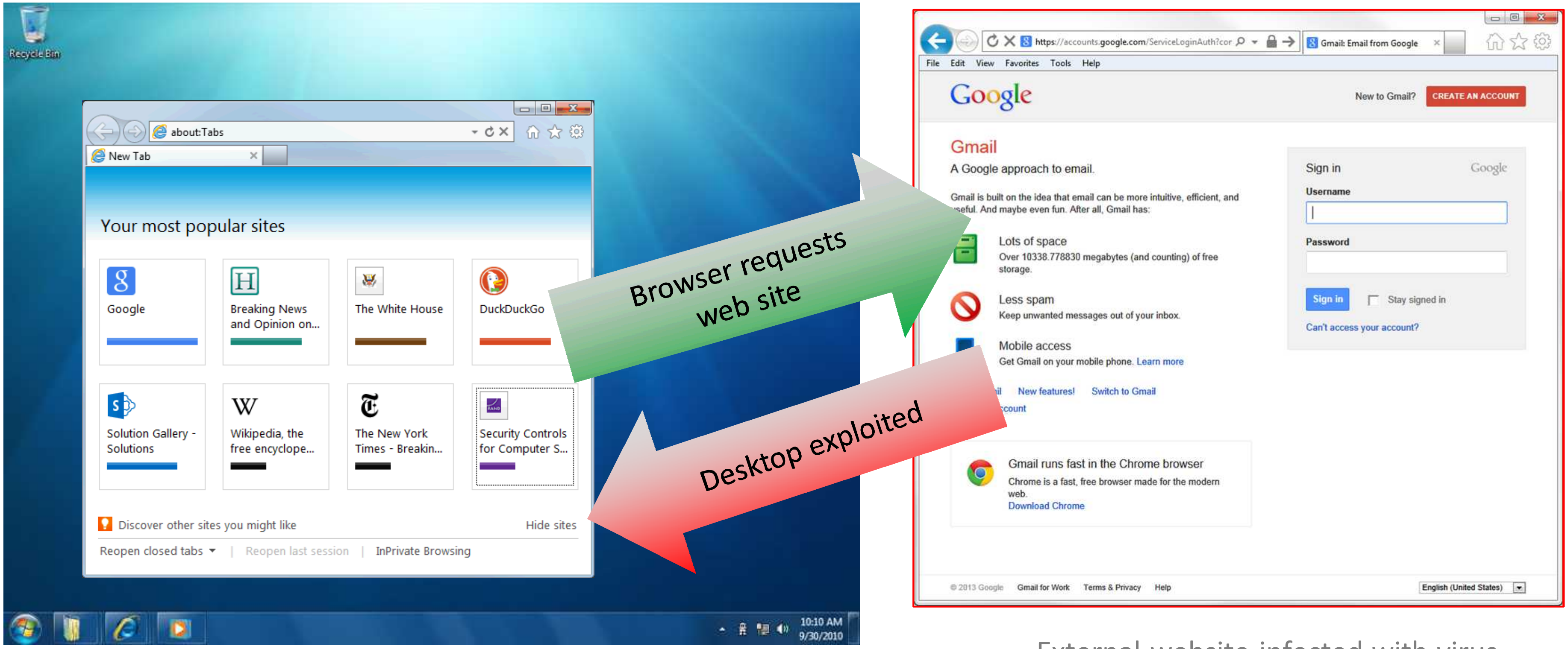
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

The Endpoint Security Problem

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

Desktop Computer - Trusted

External Web Site - Untrusted



Browser requests web site

Desktop exploited

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?

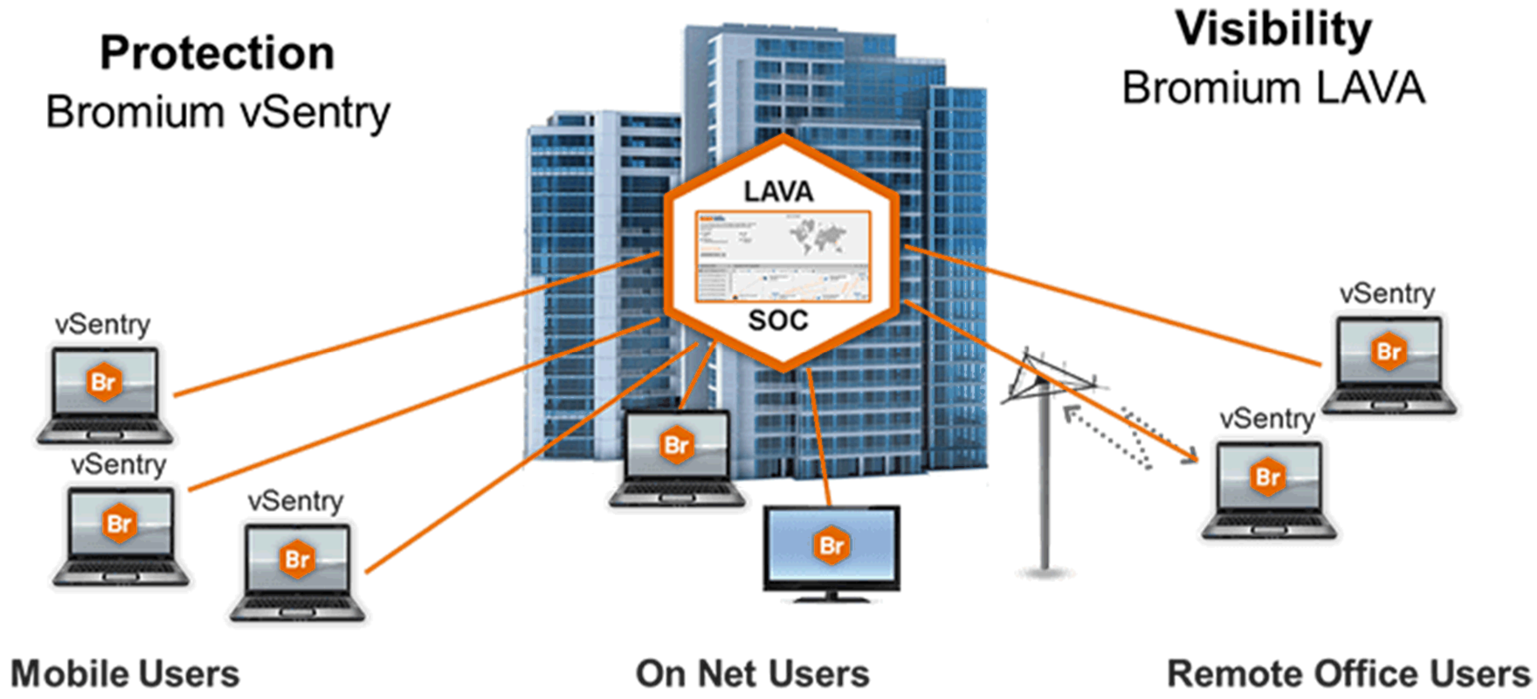


Image Credit: http://www.bromium.com/products.html

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

How does LAVA work?

Client-side

- vSentry LAVA engine

Enterprise Management Server

- Attack visualization
- LAVA manifest data
- MAEC reporting
- Syslog support
- Developing DOE Enterprise sharing capabilities

Requirements for running vSentry

- Intel Virtualization Technology (VT) or AMD Rapid Virtualization Indexing (RVI)
  - Provides hardware-level isolation
- Minimum hardware:
  - Core i5, i7, and some i3 and Xeon processors or AMD processors with RVI
  - Minimum 4GB* RAM
  - Minimum 10 gigabytes free disk space
  - Windows 7 x64

**We recommend 8 GB RAM*

- Bromium Enterprise Console
  - Policy distribution
  - LAVA
- vSentry-supported applications
  - Internet Explorer
  - Google Chrome
  - Microsoft Office 2010 & 2013
  - Acrobat Reader & Professional
  - Flash
  - Java
  - Silverlight

Demonstration

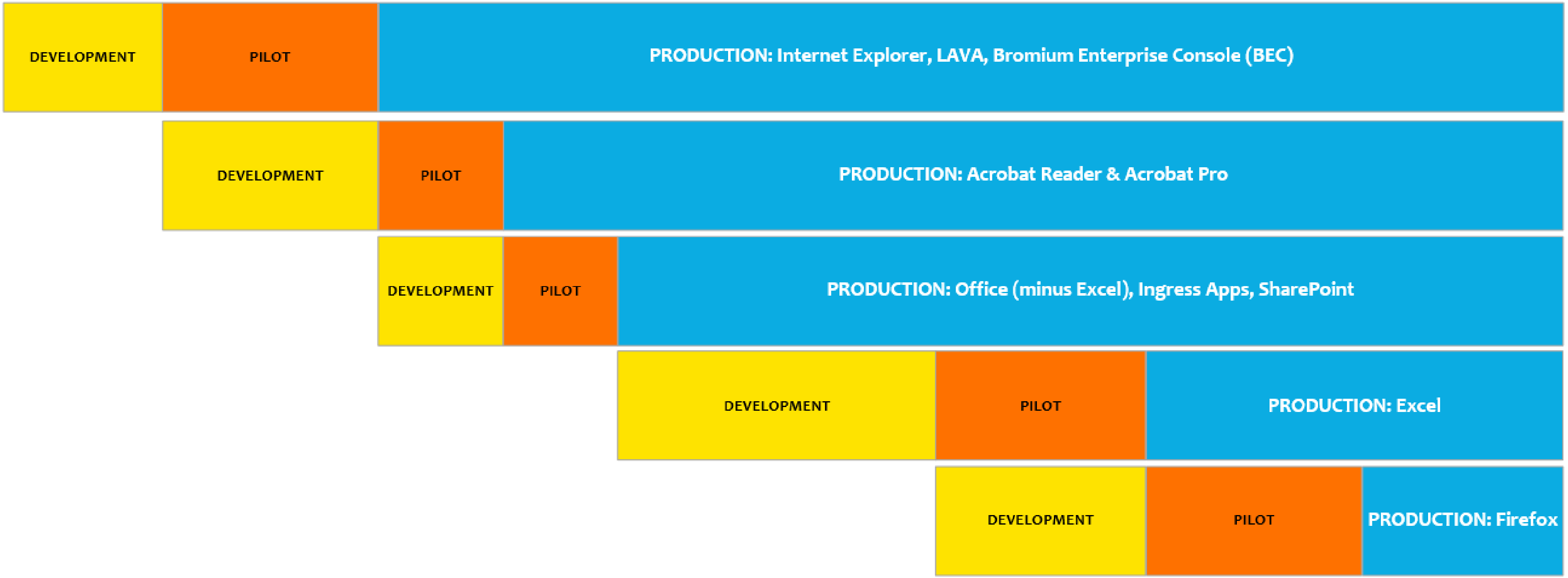
Criteria for Success

- Effective
  - Malware isolation, LAVA detection engine is accurate
- Enterprise Ready
  - Deployment, policy management, device management, and flexibility of management
- Usable
  - Ability to do work without vSentry getting in the way
- Embraced
  - Did pilot participants feel safer, more secure, and willing to adopt the new product

Phased Deployment

- Pre-Production Group (currently engaged)
  - One phase ahead of production group
  - Tests applications releases
  - Stabilizes the build
  - Determines readiness before going to production
- Production Group (not live)
  - Receives stabilized build

Our Plan for Phased Deployment



DEVELOPMENT | PILOT | PRODUCTION: Internet Explorer, LAVA, Bromium Enterprise Console (BEC)

DEVELOPMENT | PILOT | PRODUCTION: Acrobat Reader & Acrobat Pro

DEVELOPMENT | PILOT | PRODUCTION: Office (minus Excel), Ingress Apps, SharePoint

DEVELOPMENT | PILOT | PRODUCTION: Excel

DEVELOPMENT | PILOT | PRODUCTION: Firefox

Current Phase – Pre-Production

- Pre-production group:
  - Verified eligibility of machines via SCCM
  - VT on processor remotely enabled via script
  - Installer advertisement for new install and upgrades
- Using typical Incident Management and ticket escalation procedures to handle support
- Measuring metrics against normal, quantitative success criteria
- Make the go/no go decision

Pre-Production Numbers

Contact Events	30
Tier-3-escalated	4
Bromium escalated bugs	17
Bromium open bugs	14
Total sites added to trusted sites list (unsupported sites)	11

Challenges

- Policy management being handled through SCCM/Orchestrator/Bromium Enterprise Controller
- Hardware and operating system compatibility limited the number of qualified users
- Difficulty reproducing bugs with vendor
- Tuning the whitelist

Upcoming Features

- Windows 8.1/10
- Mac OS X
- Office 365
- Firefox ESR
- Least privilege
- Enterprise scalability improvements
- Licensing Agreement & Deployments

Questions