ENDPOINT SECURITY STRATEGY

January 2016

Jason Testart, BMath, CISSP
Director, Information Security Services
IST

UNIVERSITY OF WATERLOO

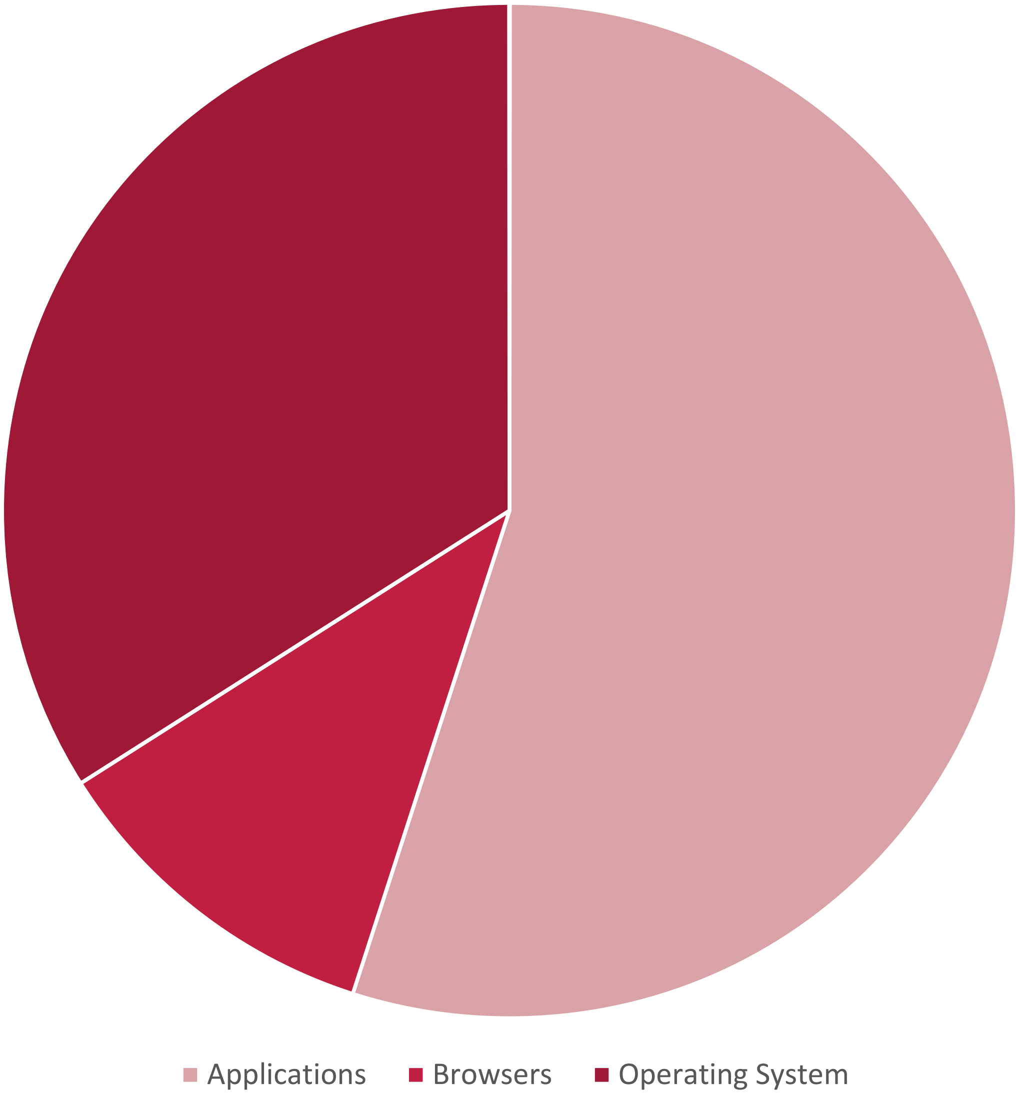
WHAT IS AN ”ENDPOINT”?

- A computer on a network that a person interfaces with directly (keyboard, mouse), and has a standard desktop OS.
- Includes:
  - Desktops
  - Laptops
  - Some tablets
- Excludes:
  - Smartphones
  - Most tablets

THREATS TO ENDPOINTS

- Malicious email attachments
- Malicious websites
- Network attacks

% of Known Vulnerabilities



From Microsoft Security Intelligence Report – Volume 19

SECURITY BEST PRACTICES

- Top 20 Critical Security Controls (CIS/SANS)
- Top 10 Security Actions (CSE/GC)
- 35 Security Mitigation Strategies (ASD/Australian Government)

CONSENSUS: TOP ENDPOINT CONTROLS

- Patch Applications
- Patch Operating System
- Restrict Administrative Privileges
- Application Whitelisting
- Secure Configuration of OS and Apps

“Over 85% of intrusions would be prevented with these controls”

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

HOW ARE WE DOING?

Control	Current State	Desired State	Next Steps
Application Patching	Limited number of applications are managed.	All applications are patched in a timely manner.	Wider adoption of Secunia CSI/PSI.
Operating System Patching	- Review of patches as released. - Emergency patches are accelerated. - Vanguard Process.	Current State.	None needed.
Restriction of Administrative Privileges	Users are given ‘!’ accounts.	More monitoring.	TBD.
Application Whitelisting	None.	Enabled in high risk environments.	Monitor market.
Secure Configurations	Some hardening.	More hardening in high-risk environments.	Reconsider CIS benchmarks for some environments.

ABOUT SECUNIA

- Corporate (CSI) and Personal (PSI) products
- In (limited) use since 2011
- Large database of vulnerabilities
- Integrates with SCCM
- Consumer version can help users keep applications up to date (no SCCM)
- May help in reducing number of redundant desktop apps.

WHAT ABOUT ANTI-VIRUS?

- Signature-based protections aren’t enough
- Behavioral (using threat intelligence and network analysis) is needed
- Sandboxing/Virtualization encouraged
- New Term: **Host-based Intrusion Prevention System (HIPS)**

HOW DOES HIPS RANK?

- CIS Top 20: 8th
- CSE Top 10: 8th
- ASD 35: 8th
  - Note: signature-based is 30th

OUR EXPERIENCE

EMAIL SECURITY GATEWAY

- Currently evaluating solutions from RFP
- Deployment planned for Spring/Summer 2016

CURRENT INVESTIGATIONS

- Behavioral with threat intelligence
  - » Webroot
  - » Bit9+Carbon Black
- Micro-virtualization
  - » Bromium
- May look at others in future
  - » Depends on market and timing

INTERIM PLANS

- Discontinue SEP effective April 30th, 2016
- Discontinue providing endpoint security software for student-owned equipment
  - » Less than 1/3 of Ontario universities provide endpoint security software to students
- Continue support for Microsoft System Centre Endpoint Protection/Windows Defender

FUTURE PLANS

- Monitor the market
- Must consider more than just malware protection:
  - Disk encryption
  - File and configuration integrity monitoring
  - Application whitelisting
  - For servers: Effectiveness in a virtualized environment.