Application White Listing and Privilege Management: Picking Up Where Antivirus Leaves Off

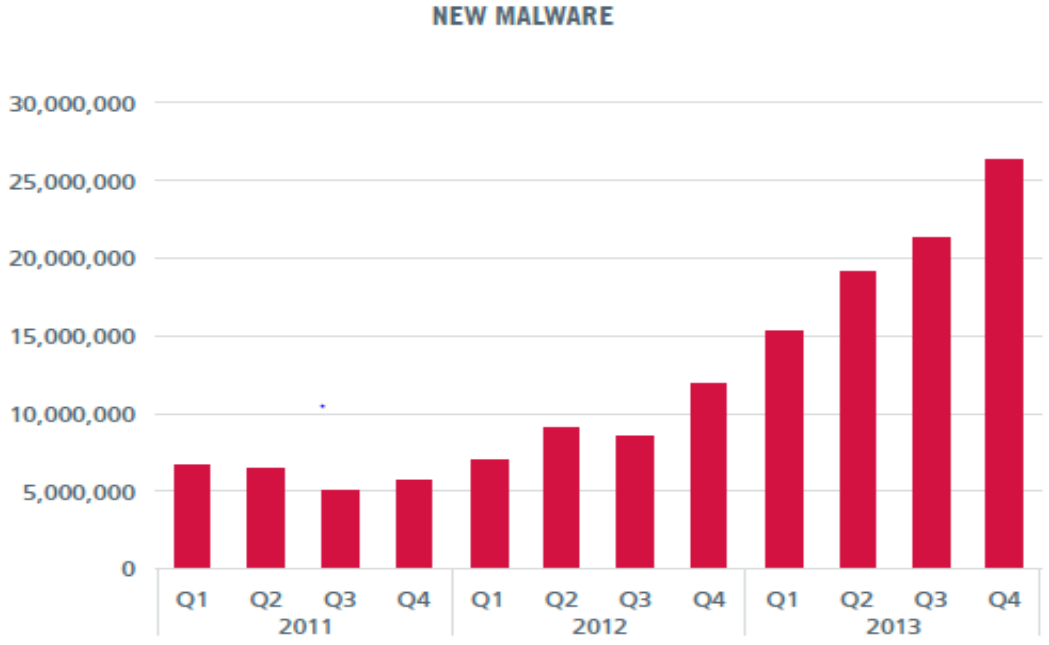
Times have Changed & A/V Executives Agree

An A/V product as your sole endpoint protection solution isn't enough.

Only about 40% of malicious code is detected by A/V products.

- "Relying solely on antivirus is a dead end—and it has been for at least 8 years now. " - Chief Technology Officer at Bitdefender, Bogdan Dumitru
- "…Antivirus signatures exist, they're still important, just not the most important. Like the seatbelt in your car; you have to have it, but it's not the most important part."- Eugene Kaspersky
- Anti-Virus "is dead"- Symantec's senior vice president Brian Dye

Malware Levels

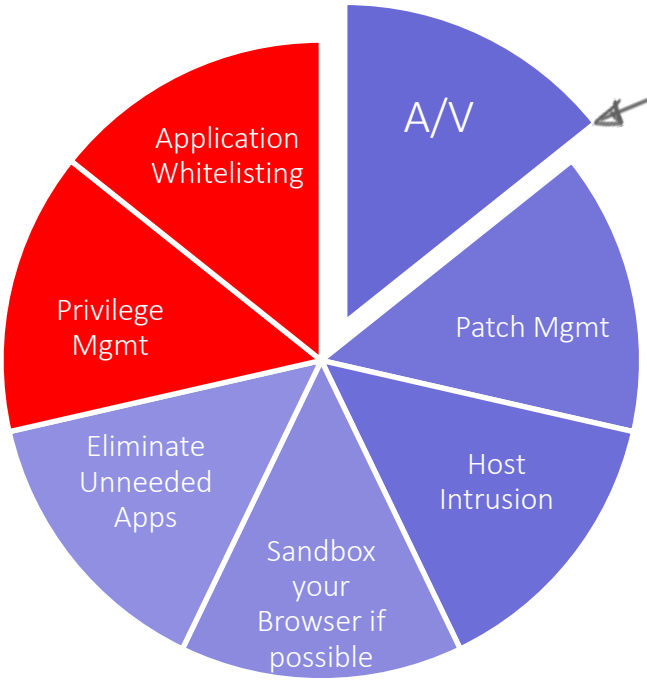


Source: McAfee Labs, 2014.

Targeted Attacks

Source: CyberFactors, a wholly owned subsidiary of CyberRisk Partners, and sister company of CloudInsure.com

Re-thinking the Endpoint Security Approach



A good A/V solution is just one element of a more balanced Endpoint security approach

Change is needed that introduces a more proactive approach to endpoint security

What is application whitelisting?

Application whitelisting comprises the following technical steps:

- identifying specific executables and software libraries which should be permitted to execute on a given system
- preventing any other executables and software libraries from functioning on that system
- preventing users from being able to change which files can be executed.

An intermediate, but still not optimum approach to application whitelisting is identifying entire directories from which users are allowed to execute programs, such as C:\Windows, C:\Program Files, or even C:\Program Files\Specific Application.

What is privilege elevation?

- Privilege elevation allows users that have standard rights to their machines the ability to selectively install programs with administrative privileges.

20 Critical Security Controls - Version 5*

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Access Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Protection

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

*In 2013, the stewardship and sustainment of the Controls were transferred from the SANS Institute to the Council on CyberSecurity (the Council), an independent, global non-profit entity. See greater detail here: http://www.sans.org/critical-security-controls

Australian DoD Top 4 Strategies to Mitigate Targeted Cyber Intrusions

At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies listed in its 35 Strategies to Mitigate Targeted Cyber Intrusions:*

1. **use application whitelisting to help prevent malicious software and unapproved programs from running**
2. patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
3. patch operating system vulnerabilities
4. **restrict administrative privileges to operating systems and applications based on user duties**

*The Top 4 Strategies to Mitigate Targeted Cyber Intrusions are mandatory for Australian Government agencies as of April 2013.
See the complete list here: http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

Mitigation strategies summary

Mitigation strategy effectiveness ranking 2014 (2012)	Mitigation strategy	Overall security effectiveness	User resistance	Upfront cost (staff, equipment, technical complexity)	Maintenance cost (mainly staff)	Helps detect intrusions	Helps mitigate intrusion stage 1: code execution	Helps mitigate intrusion stage 2: network propagation	Helps mitigate intrusion stage 3: data exfiltration
1 (1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2 (2)	**Patch applications**,eg, Java, PDF viewers, Flash, web browsers and Microsoft Office. Patch or mitigate systems with 'extreme risk' vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3 (3)	**Patch operating system vulnerabilities.** Patch or mitigate systems with 'extreme risk' vulnerabilities within two days. Use the latest suitable operating system. Avoid Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4 (4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

IAD's Top 10 Information Assurance Mitigation Strategies

IMAGINE 2014

Fundamental aspects of network security involve protection and detection measures can be grouped in four mitigation goal areas. These four mitigation goal areas target critical steps in the intrusion life cycle — creating a technical layered defense approach that supports the ability to "fight through" a contested cyber environment:

- ***Device Integrity*** — maintaining and measuring device health/integrity. Devices often represent the attack surface area or the persistent living-space for the advanced persistent threat (APT).
- ***Damage Containment*** — when intrusions occur, limiting losses of information, systems, and mission capabilities.
- ***Defense of Accounts*** — protecting credentials from misuse and enabling trusted authentication and access.
- ***Secure and Available Transport*** — maintaining the privacy and reliability of data communications.

These goal areas will support current and future cyber defense efforts, helping to set priorities, and contributing to the desired end-state of denying adversaries the ability to operate on our networks and impact our missions. Efforts that can be implemented now are listed below as IAD's Top Mitigations with goal areas indicated in the left margin. By blocking critical points in the attack life cycle, these mitigations are effective against entire classes of attacks, including new unknown variants.

1. Application Whitelisting: Application Whitelisting is a proactive security technique that allows a limited set of approved programs to run, while all other programs and most malware are blocked from running by default. Application Whitelisting enables only the administrators, not the users, to decide which programs are allowed to run.

2. Control Administrative Privileges: Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are restricted from normal users. Network owners should only grant Administrator privileges when absolutely necessary and should take steps to ensure Administrator accounts are not exposed to the internet and other sources of increased risk. More robust protections can be achieved through the use of two-factor authentications for administrators and other privileged accounts.

What application whitelisting is not:

- **Providing a portal or other means of installing approved software**

  This does not prevent users from running software not listed on the portal, and will not prevent malware from executing and compromising a system.

- **Preventing users from writing to locations such as C:\Windows or C:\Program Files**

  While this may prevent a user from installing some software, it does not prevent the execution of software residing in locations such as a user's desktop or temporary directories. These locations are commonly used by malware to infect a computer.

Why not use blacklisting?

- **Similar to AntiVirus or webfiltering tools**

  A known set of data/policies against which an application is compared to determine if it's allowed to run

- **Do you think you can think of every possible bad permutation that could occur?**

Why should admin privileges be restricted?

- Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.

- An environment where administrative privileges are restricted is more stable, predictable, and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

Privilege Management & Application Whitelisting

2 Firms : 2 Products

cohen&grigsby

McCourt

Bit9

beyondtrust
Beyond Traditional Security

Cohen & Grigsby
300 Users

Fully Deployed Since
2012

McCourt
50 Users

Fully Deployed Since
March 2014

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

IMAGINE 2014

Application white-listing:

- Has been easy to implement, but is very detailed
- Policies can be set to allow updates without new rule
- Can designate special user accounts to override rules
- Can designate network shares that are trusted
- Users can be local admins since only trusted software will run
- Allows full protection, even when disconnected
- Carbon Black adds incident response capabilities

Admin privilege elevation:

- Simple right-click on .exe or .msi and “Run Elevated”
- Allows laptop users ease-of-use
- Loss of control on application installation

Application white-listing:

- Has been difficult to implement
- Policies need to keep up with version updates
- Seriously considering abandoning the software

What about…?

- **MS Applocker**
- **AppSense / Application Manager**
- **Lumension / Application Control**
- **Others**

Questions

We'll now open it up for questions

References

http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/

http://www.sans.org/critical-security-controls

http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

http://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/

Thank You