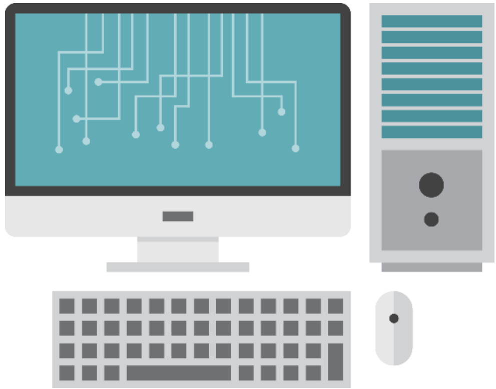
Configure Application Restriction Policies

Greg Shields

@ConcentratdGreg | www.pluralsight.com

What This Module Covers



Configure Software Restriction Policies

Configure AppLocker Rules

Configure Rule Enforcement

Blacklisting vs. Whitelisting

Your typical antimalware solution is an example of blacklisting.

"I don't want this code to execute on my systems."

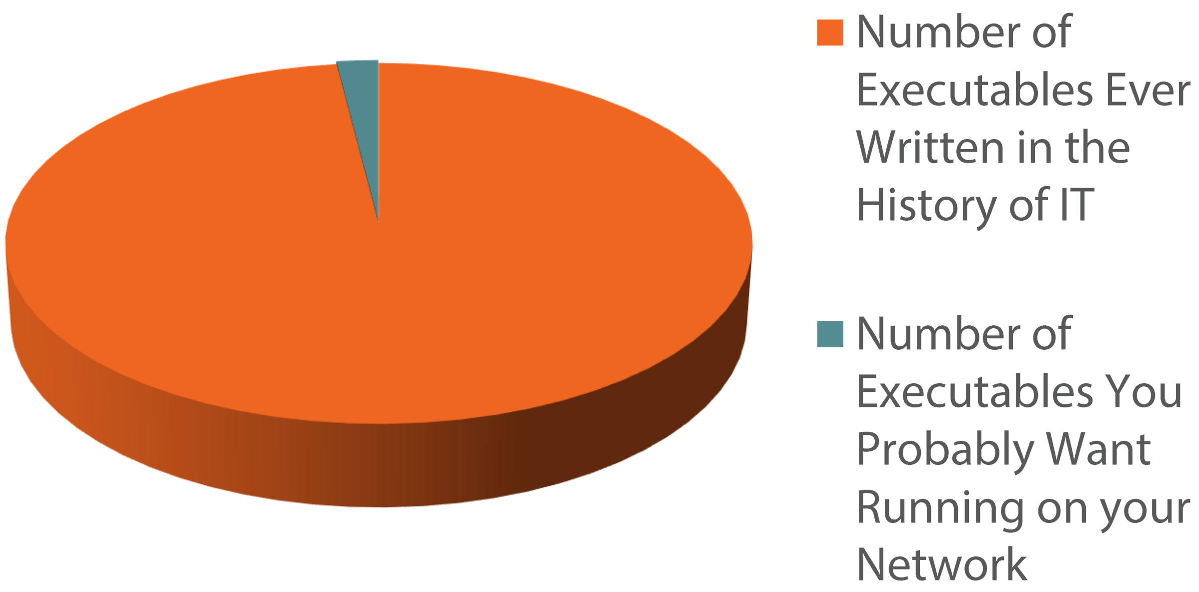
Challenge: Blacklisting requires constantly updating the blacklist.

"The bad guys are constantly evolving, so I'm constantly updating antimalware signatures."

Blacklisting vs. Whitelisting

With whitelisting, you instead identify what code is allowed to execute.

"Here is my list of company-approved applications."



Blacklisting vs. Whitelisting

With whitelisting, you instead identify what code is <u>allowed</u> to execute.

"Here is my list of company-approved applications."

Whitelisting has other uses.

"Not-quite-malware"

"License assurance"

"Version assurance"

Software Restriction Policies vs. AppLocker

Software Restriction Policies

- Introduced with Windows XP/2003
- Supported on all OS versions
- Scoped to all users
- File hash, path, certificate, registry path, and Internet zone rules
- Blacklisting and whitelisting
- Always enforcing

AppLocker

- Introduced with Windows 7/2008R2
- Requires Windows 7/8 Enterprise or Windows Server Std/Ent/Datacenter
- Scoped to specific users or groups
- File hash, path, and publisher rules
- Whitelisting only
- Enforcing or merely auditing

What This Module Covered

Configure Software Restriction Policies

Configure AppLocker Rules

Configure Rule Enforcement