ninjaOne

Endpoint Hardening Checklist

A Defender's Guide for Protecting Systems & Reducing Attack Surface

The majority of attacks still take advantage of basic gaps in security.

The cybersecurity industry is valued at $166B, and is expected to more than double by 2028. That remarkable growth has been fueled in large part by the perception that an ever-growing and increasingly complex toolset is required to combat ever-growing and increasingly sophisticated threats.

The truth is, the majority of attacks still owe their success to the same familiar lapses in basic security hygiene that IT professionals have been battling against for years. And that includes the major attacks we see in the headlines:

- Colonial Pipeline? Hacked via an inactive account without MFA.
- Irish Health Services? Malicious Excel doc.
- The LockBit ransomware gang's 5-month access to a U.S. government agency? Exposed RDP.
- The $50M ransomware attack on PC-giant Acer? Unpatched Microsoft Exchange vulnerability.

Make no mistake. Utilizing the right tools is a critical part of security, especially at scale. But, year after year, what real-world attacks show us is that the best investments aren't necessarily in new tooling — they're in shoring up the basics.

We created this checklist to help IT professionals do exactly that. It's our hope that in addition to focusing efforts, it can help serve as a basis for establishing secure baselines as well as tracking and reporting progress to management and stakeholders.

PLEASE NOTE

As with any admin work, any changes should be tested as part of a formal process, before being rolled out en masse. Some hardening techniques can have considerable impact or unintended consequences on user workflows and administration overhead.

Security, as a process, should aim to alleviate overhead where possible, and communicate these changes out to the business ahead of time to ensure user and organizational buy-in to. The higher the potential impact, the more important the level of clear communication up front.

In many cases, small and medium-sized orgs looking for the biggest bang for their buck should forget chasing shiny new tools and pour time and effort into basic system hardening, instead.

Part 1

Start Gathering Actionable Intel

Scout Ahead

Knowing (the latest threats) is half the battle. There's a lot of noise, fear-mongering, and hype out there, however, so one of the best ways to stay informed is to identify reliable sources that can provide you with measured takes and practical perspectives.

Follow these resources and monitor for changes, news, and best practices. Evaluate against your own systems, challenges, and priorities.

- [ ] **Build up a curated collection of security trusted resources and threat feeds**
    - InfoSec Twitter (start here)
    - CVE, RSS, and government feeds
    - Reputable security vendor feeds

- [ ] **Join peer communities**
  Communities can be go-to places for rapid reactions and sounding boards. Here are a few places to start:

    MSP:
    - MSPGeek
    - MSPs R Us
    - CyberDrain

    Internal IT and Enterprise:
    - WinAdmins
    - SysEngineer
    - DevOps, SRE, & Infrastructure

    Security Focused:
    - SimplyCyber
    - Cooey COE
    - Local BSides groups
    - Local Defcon chapters

Upgrade Your Hardening Process

Now that you're scouting ahead, making intel and commentary actually actionable requires developing a repeatable and engrained process.

- [ ] **Formalize the steps you take to mitigate threats and harden devices:**
    - Identify the risk
    - Scope out the likelihood and impact
    - Develop the configuration to remediate or mitigate the risk
    - Test and verify the mitigation
    - Deploy the mitigation in phases, with a backout plan
    - Document the change, and report on the exceptions
    - Monitor the mitigation to the vulnerability with your RMM

Establishing and iterating this process ensures you're working towards constantly elevating the security posture of the organization.

Part 2

Endpoint Hardening Essentials

Mitigate the Vulnerable Legacies

As Windows has evolved over the years, it has maintained backwards compatibility with several protocols and services that underpinned and supported core services. Unfortunately, with the passage of time, they're creaking at the seams and suffering from vulnerabilities.

- [ ] **Server Message Block v1**
    - Background/resource: Stop using SMB1
    - Special note: SMB1 is being removed from Windows 11, and that includes the binaries needed to use and install it.
- [ ] **Powershell 2.0**
    - Background/resource: Windows PowerShell 2.0 feature must be disabled
- [ ] **TLS 1.0/1.1, and SSL (All versions)**
    - Background/resource: Solving the TLS 1.0 Problem
- [ ] **LanMan (LM) and NTLMv1**
    - Background/resource: The LanMan auth level must be NTLMv2 only, and to refuse LM and NTLM

NOTE The following recommendations obviously aren't comprehensive. Depending on your specifics (size, infrastructure, bespoke line of business apps, etc.), some may not be appropriate for your business. Security isn't one-size-fits-all. What may be critical for some may be overkill for others. Do what's practical, take a layered approach, and remember, when implementing new controls it's always a good idea to test them first to avoid unintended disruption.

- [ ] **Digest Authentication**
    - Background/resource: WDigest Authentication must be disabled
- [ ] **Patching**
    - Background: Vulnerability management
    - Resource: Cloud-based Patch Management

OS Hardening

At the core of modern security efforts is first improving the security posture of the operating system and its configuration. Strengthening the build at this layer allows the rest of your efforts to sit on a solid, and modern foundation.

- [ ] **ASR/Anti Exploit rules**
    - Bitdefender resource: Configuration (bitdefender.com)
    - Microsoft resource: Understand and use attack surface reduction (ASR)
- [ ] **Restrict lateral movement tools and techniques**
    - Resource: Preventing Lateral Movement - NCSC.GOV.UK
    - Resource: Configuration (bitdefender.com)
    - Resource: Restricting SMB-based lateral movement in a Windows environment | by Palantir
- [ ] **Native features**
    - Resource: App & browser control in Windows Security (microsoft.com)
- [ ] **Reputation-based Protection**
    - SmartScreen for Microsoft Edge
    - Potentially unwanted app blocking
    - SmartScreen for Microsoft Store Apps
- [ ] **Secure Boot**
    - Resource: Secure boot | Microsoft Docs
- [ ] **Logging**
    - Resource: How to Optimize Windows Logging for Security (blumira.com)

- [ ] **Remove unneeded apps and features**
    - Resource/background: Remove unused and unnecessary software (johnopdenakker.com)

Network hardening

Now that you've strengthened the local operating system, turn towards the wider network, and the services exposed amongst the interconnected world. This ranges from configuring the local network to reducing the acceptable inbound traffic allowed.

- [ ] **Disable or harden RDP**
    - Resource: HOWTO: Harden Remote Desktop connections to Domain Controllers - The things that are better left unspoken (dirteam.com)
    - Resource: Methods to Enable and Disable Remote Desktop Locally | Interface Technical Training
- [ ] **Disable DNS Multicast**
    - Resource: How To Disable LLMNR & Why You Want To - Black Hills Information Security
- [ ] **Disable NetBios**
    - Resource: Disable NetBIOS in Windows networks – 4sysops
- [ ] **Disable SmartNameResolution**
    - Resource: Preventing Windows 10 SMHNR DNS Leakage | SANS Institute
      Resource: Turn off smart multi-homed name resolution (admx.help)
- [ ] **Configure the firewall**
    - Resource (Video): Demystifying the Windows Firewall – Learn how to irritate attackers

Account Protections

Restricting the attack surface available with local accounts, services, and the credential store frustrates attackers, and prevents the quick and easy elevation of privileges. This could alert you to an attack, increase the time needed to bypass the mitigations, or even prevent an attack from succeeding.

- [ ] **Remove local admin rights**
    - Resource: Least Privilege | CISA

- [ ] **Harden local administrator accounts**
    - Resource: Appendix H - Securing Local Administrator Accounts and Groups | Microsoft Docs
- [ ] **Limit logon rights for accounts**
    - Resource: User Rights Assignment - Windows security | Microsoft Docs
- [ ] **Utilize the protected users group (Active Directory joined devices)**
    - Resource: Protected Users Security Group | Microsoft Docs
- [ ] **Credential Guard**
    - Resource: Protect derived domain credentials with Windows Defender Credential Guard (Windows) - Windows security | Microsoft Docs
    - Resource: Manage Windows Defender Credential Guard (Windows) - Windows security | Microsoft Docs

Application Hardening

Attackers often attempt to exploit some of the most common tools and settings organizations rely on. These elements are widely distributed and installed on endpoints. Without further configuration they can lead to easy attacks of opportunity.

- [ ] **Office Suite**
    - Resource: Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016 | Cyber.gov.au
    - Resource: How to secure Microsoft Office Desktop Deployments – A Technical Guide. - @Precursec (precursorsecurity.com)
- [ ] **Adobe Reader**
    - Resource: Hardening Adobe Reader - Security Musings
- [ ] **Make it a process**
    - Pick an application
    - Evaluate its needs and risks
    - Work with key contacts to ensure a good balance between risk, and usability

- Research hardening techniques for that specific program
- Mitigate the risk and exposure with more comprehensive configurations

Browser Hardening

Web browsers tend to be one of the more overlooked elements in the stack. Yet, their configuration sets the scene for one of the most used programs installed on computers today. Locking down and enforcing a few basic security features can help secure this critical entry point.

☐ **Smartscreen Phishing Filter and Advanced Protection**

- Chrome: Use Safe Browsing in Chrome
- Edge: Configure Microsoft Defender SmartScreen to block potentially unwanted apps (admx.help)
- Firefox: browser.safebrowsing.phishing.enabled (admx.help)

☐ **Dedicated Sandboxing of processes**

- Most browsers now isolate the processes that form the stack we all use to experience the web, you can extend Application guard into other browsers which allows a hardware isolated browser session for risky sites.
- Edge: Microsoft Edge and Microsoft Defender Application Guard | Microsoft Docs
- Other browsers: Microsoft Defender Application Guard Extension - Windows security

☐ **Control installed extensions**

- Chrome: Managing Extensions in Your Enterprise - Chrome Enterprise and Education Help
- Edge: Manage Microsoft Edge extensions in the enterprise | Microsoft Docs
  Firefox: mozilla/policy-templates (github.com)

Part 3

Additional Resources

- [ ] **Universal Resources**
  - SecCon-Framework: Windows security configuration framework
  - CISA Insights: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses
  - CIS Critical Security Controls
  - GitHub: Defences Against Cobalt Strike
  - Embracing the Zero Trust Security model
  - 10 Immutable Laws of Security Administration
  - Endpoint Security – The Essentials – PwnDefend
  - Removing Application UAC Requirements with Shims
  - CVE Trends: Crowdsourced CVE intel
  - Proactive Preparation and Hardening to Protect Against Destructive Attacks
  - For [Blue|Purple] Teams in Cyber Defence

- [ ] **Australia**
  - Essential Eight Mitigations
  - Strategies to Mitigate Cyber Security Incidents

- [ ] **Canada**
  - Baseline Cyber Security Controls for Small and Medium Organization

- [ ] **UK**
  - Cyber Essentials
  - NCSC
  - NCSC - 10 Steps to Cyber Security
  - NCSC - Device Security Guidance

- [ ] **USA**
  - Complete STIG List
  - Windows 10 Security Technical Implementation Guide

Get More Done Confidently and Securely with NinjaOne

Find out how NinjaOne makes it easier to protect your endpoints with:

- Deep visibility across your entire network from a single pane of glass
- 360-degree monitoring and real-time alerting
- Secure remote access for disruption-free management and remediation
- Automated patch management
- Detailed asset inventory and compliance reporting
- Seamless backup and endpoint security integration

LEARN MORE

Contact Us Today
(888) 542-8339 | sales@ninjaone.com | www.ninjaone.com

ninjaOne