# Five Tips for Managing Host-Based Security

Host-based security represents a large surface of attack that continues to grow as employees become increasingly mobile and work from home more often. This guide will provide a few tips to make sure your vulnerability management program is covering the right bases to help mitigate some of the implicit risks associated with a remote workforce.

## 1 Workstation Image Security

Most organizations deploy laptops using a standard set of system images and configurations. Below are some questions to help you ensure workstations are secure in the event they are lost, stolen, or compromised by a threat actor:

a. Are all workstation images configured based on a secure baseline?

b. If so, are those configuration baselines managed and updated?

c. Are critical OS and application patches tracked and applied?

d. Are any applications or management scripts vulnerable to common attacks?

e. Is hard drive encryption being implemented and managed securely?

f. Has a security audit or penetration test been completed for each of our workstation images? Most organizations have more than one workstation image in use. For example, Windows 7, Windows 10, or MacOS.

## 2 Virtual Desktop Infrastructure (VDI) Security

Not all employees have physical laptops these days. Many employees and vendors access applications and desktops through solutions like Citrix. Consider asking similar questions you asked when thinking about workstations, but extend them with the following:

a. Are VDI portals and VPN currently configured with multi-factor authentication (MFA)?

b. Can users easily exfiltrate data through shared drives, the clipboard, printers, email, websites, or other common egress points?

c. Can users easily pivot to critical internal resources like database, application servers, and domain controllers?

d. Are deployed applications locked down to prevent unauthorized access to the operating system to ensure least privilege?

*Note: This one often applies to vendors or customers accessing desktop application through a VDI portal.*

## 3 Windows and Linux Server Security

While workstations and VDI portals are directly exposed to the public, once an attacker pivots into the environment it's often trivial to identify Windows and Linux servers to target. Make sure those standard deployment images and configurations have also been reviewed and hardened to help reduce attack surface. Vulnerability scanning by itself is not enough to identify vulnerabilities that could be used by authenticated attackers.

## 4 z/OS Mainframe Security

Windows and Linux servers are typically deployed using standard system images, but z/OS mainframe tend to be unique. We've found that in many environments the mainframe configurations are not centrally managed as effectively as their Windows/Linux counterparts, and those inconsistencies can lead to vulnerabilities that are often accessible to domain users. Ask yourself the questions below:

a. Are our z/OS mainframes evaluated for missing critical application and OS patches on a regular cycle?

b. Are our z/OS mainframe configurations centrally managed and implemented based on a secure baseline?

c. Are Active Directory domain users able to log into z/OS mainframe applications or directly through mediums like SSH?

d. When was the last time we did a security audit or penetration test of our deployed z/OS mainframes?

## 5 Employee Training

Simply having defensive technical controls in place isn't enough. Make sure to train your employees on how to securely access and manage your company's IT assets. Also make sure training covers easy ways to identify and avoid potential scams. Understanding how things like phishing attacks can affect you personally can be a powerful way to help people protect themselves and your company.

### About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest health care companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster. Follow us on Facebook, Twitter, and LinkedIn.

Website
**www.NetSPI.com**

Email
**Info@NetSPI.com**

Phone
**612.465.8880**

Ver 03 – 012021