Protecting high-risk environments with secure admin workstations

Security attacks are evolving and becoming more sophisticated in large organizational environments, and to say that IT teams are concerned is an understatement. Secure admin workstations (SAWs) can be invaluable in the security toolkit for any organization. Microsoft Core Services Engineering and Operations (CSEO) has discovered a particularly effective use for SAWs in protecting high-risk environments. Learn what SAWs are, how Microsoft uses them, and why other organizations might adopt them.

Understanding secure admin workstations

Secure admin workstations are limited-use client machines that are built to substantially reduce the risk of compromise from malware, phishing attacks, bogus websites, and pass-the-hash (PtH) attacks, among other security risks. Although SAWs can’t be considered a “silver bullet” security solution for these attacks, Microsoft has found these clients to be helpful as part of a layered, defense-in-depth approach to security.

Microsoft partners with manufacturers to build these devices, and what’s unique about them is what they don’t include: software, such as productivity suites and other utilities that are potentially vulnerable to malware and phishing attacks. For example, users can’t be tricked into clicking a link in an email phishing attack if they don’t have an email program running. Productivity tools and high-risk applications that aren’t required for the secure admin role are installed and used on a separate “productivity virtual machine,” which is hosted on the SAW. This configuration allows the user to access the productivity tools and applications they need without increasing risk to the secure admin environment.

Microsoft relies on “application whitelisting” for this effort, meaning that only approved software can run on the workstation. High-risk items don’t make the list. What does make the whitelist can vary, but the point of the process is to carefully vet the list and make security a high priority. The SAW can include a limited version of Microsoft Edge that is filtered and uses a proxy server to access the administrative sites the user needs.

In the context of protecting high-risk environments, SAWs are used for making secure connections to the environment and that’s pretty much their only function. As one principal IT service engineer puts it, “SAWs for high-risk environments (HREs) are like giant smart cards, identifying and authenticating that the user is allowed to get in the door.”

Who has access, and when?

Given the nature of HREs, it’s understandable that an organization would want to restrict access to SAWs and have a process in place for how these machines are assigned and distributed. For Microsoft, the sequence follows this general pattern:

1. An HRE has a designated owner. Employees who require access to the HRE request approval from the owner.
2. If the request is accepted, the owner puts in a formal request to the SAW team to create a SAW device. The SAW team coordinates with the device manufacturer.
3. The device manufacturer ships the device to Microsoft, and the SAW team adds the image to it and hardens the device to make it highly secure. Note that when Microsoft initially receives the device, the hardware is secure but the software isn’t. So, for example, it does have the UEFI passwords set and the machine configuration is already locked down, but it doesn’t have an operating system on it and it’s not software-managed and controlled. Microsoft recommends limiting the amount of time that the SAW is in this state to as short a time as possible.
4. The software-secured device is then sent to users through interoffice mail, rather than the postal system. This method ensures that the device is always in Microsoft facilities. Users can also come directly to the SAW team to pick it up if that is more convenient.

5. Users now have access to the device and can sign in using their Microsoft credentials.

6. Users can start the HRE remote access process.

After approved users have the SAW, they use it as needed to access the HREs. In practice, the SAW becomes a second device for them, with their standard machine used for day-to-day work and the SAW used for privileged work. Users experience a bit of a learning curve as they adjust to the limited functionality of the SAW. For more information about the user experience, see the Recommendations and limitations section.

How SAWs are used for HREs at Microsoft

The SAW isn’t granting rights to any actual resource; it merely provides a connection to a secure server, which itself connects to the HRE. Specifically, a SAW enables users to use two-factor authentication to make a Microsoft Remote Desktop Protocol connection through a bank of Remote Desktop Services servers for each HRE.

Figure 1. SAW enforcements

SAW devices at Microsoft serve two major purposes: to provide access to HREs and to provide access to the domain for users who have privileged admin access. There are approximately 35,000 SAW devices in use at Microsoft, with only 30 to 40 of those devices being used to access HREs, although that number is expected to grow because of increased demand for HRE access.

When users no longer need a SAW device, the SAW team typically re-deploy the device to another user in the same organization. If required, the software is reimaged and, if necessary, the hardware itself is re-baselined (such as for UEFI changes). If any device is unaccounted for, Microsoft CSEO can place it in BitLocker recovery mode, with no BitLocker recovery key available. This effectively locks down the device and renders it unusable.
Recommendations and limitations

Recommendations and limitations for organizations that are considering using SAWs as one of the layers for isolation can include:

- **Use whitelisting.** Always vet and approve anything to be put on the SAW. Users may occasionally ask for additional software or utilities to be added. IT should do a cost-benefit analysis to determine if the applications and systems are critical to the admin role or if they are simply a convenience. In most cases, high-risk applications are not needed for admin functions and can be used from the productivity virtual machine instead of from the SAW.

  This interplay or negotiation with users sometimes calls for creativity. For example, let’s say that a user requests a toolkit that requires local administrative rights on the machine when the user installs it. IT may be able to preinstall that toolkit on the system, so that it can run without administrative rights, rather than granting users the administrative rights necessary to install it themselves. Users get what they need for productivity and IT maintains the security that a SAW requires.

- **Make the connection between the manufacturer (hardware) and the provisioning team (software) as short as possible.** This is the least secure link in the chain.

- **Educate users about how to work with SAWs.** A SAW device is the only way for a user to access an HRE. There is no workaround for such a locked-down workstation. We deploy SAW laptops to mobile users who need access to HREs.

- **Carefully track SAW inventory.** Collect usage metrics on the devices to look for stale computers and devices that aren’t being used. Many IT departments practice this already for their standard hardware and will find it easy to extend this to their SAW inventory as well.

- **Understand that even SAWs are not 100 percent secure.** If persons with malicious intent gain physical access to the device, they could eventually break through its security layers and control it.

- **Realize that it’s more secure to enforce the use of SAWs to access HREs than to allow exceptions.** Microsoft uses a global enforcement mechanism, so that after a team agrees to use enforcement, everyone accessing the HRE must be using a SAW. Think of it this way: identity management is exception management.

- **Recognize that this is a relatively high-cost solution.** In this scenario, CSEO buys two machines per employee—the SAW and the standard machine—rather than one.

- **Identify the minimum hardware requirements for a device that will be used as a SAW, primarily because of the chipset needed.** Windows 10 supports these hardware requirements.

Built on a strong foundation

Windows 10 provides a strong foundation for our SAW devices with several important built-in security features.

**Windows Defender Device Guard**

Windows Defender Device Guard is a combination of hardware and software security features that, when configured together, will lock a device down so that it can run only trusted applications. If the application isn’t trusted, it can’t run—period. It also means that even if an attacker manages to get control of the Windows kernel, that attacker will be much less likely to be able to run malicious executable code after the computer restarts because of how decisions are made about what can run and when.

**Windows Defender Credential Guard**

Windows Defender Credential Guard uses virtualization-based security to isolate secret information so that only privileged system software can access it. Unauthorized access to these secrets can lead to credential theft attacks,
such as pass-the-hash or pass-the-ticket. Windows Defender Credential Guard prevents these attacks by protecting password hashes and credentials stored by applications.

**Secure Boot and Trusted Boot**
Secure Boot uses UEFI and TPM to verify the digital signature of the firmware, reducing the risk of successful rootkit attacks. Trusted Boot ensures that only verified and digitally signed operating system and application components are executed when Windows loads.

A SAW builds on the firm foundation of Windows 10, providing the level of isolation and restricted access that Microsoft needs for its high-risk environments. No single technique or even operating system is a perfectly secure solution, but combining the advantages of several techniques offers improved security overall.

For more information

**Microsoft IT Showcase**

microsoft.com/itshowcase

**IT Expert Roundtable: How Microsoft secures elevated access with tools and privileged credentials**

**Using shielded virtual machines to help protect high-value assets**

**Windows Defender Device Guard: virtualization-based security and Windows Defender Application Control**

**Windows Defender Security Center**

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.