In today’s security landscape—more electronic threats of increasing sophistication, more human attention from governments, terrorists, criminals, and hackers, and the increasing popularity of BYOD—it is essential to cover the basics and reduce attack surfaces wherever possible.

**Just the Basics**

What are the basics, and where can attack surfaces be minimized?

Every new revelation about security breaches, from the theft of credit card numbers and personal information to the use of Web crawlers to automate the collection of top-secret documents, touches the same issues:

- **The lack of effective enforcement and oversight at supposedly secure facilities means that the weakest link is often very weak.**

  Even the best policy is meaningless without enforcement. You cannot assume that minor or out-of-the-way branch offices are less vulnerable to attack than headquarters. USB access at sensitive sites should be restricted, if not turned off centrally, as an extra measure against security exploits and carelessness.

- **Your enemies value human intelligence as much as you do.**

  You need effective measures to prevent unauthorized access by insiders as well as intruders. The focus in the popular press on SIGINT, especially on NSA programs such as PRISM, and discussions about the legitimacy of collecting metadata tend to distract from the task at hand. The focus on SIGINT tends to minimize the role of HUMINT.

- **Portable endpoint devices, especially BYOD, continue to illustrate that “the endpoint is the weak point.”**

  No software can resolve the first two issues. Those are up to the organization’s policies. But VMware does offer very good solutions—we think the best available—to the security problems caused by unwelcome attention as well as the increasing adoption of smartphones, tablets, and BYOD in general.

**The BYOD Conundrum**

People love the power and convenience of personal devices as communication, entertainment, and access tools. For federal agencies whose personnel need access to secret data, the VMware Federal Secure Desktop enables access for a wide range of end-user devices. Unfortunately, however, access is not always a one-way street. In fact, where top-secret access is concerned, not only BYOD but all fat client devices (those that store data, passwords, user profiles) are easy prey for intruders. When devices are lost or stolen, any data they contain must be considered compromised. Even when used normally, they are vulnerable to snooping because they contain data at rest or in use. They should be considered attack surfaces.

Meanwhile, Mobile Device Management (MDM) technologies are continuing to mature and become more relevant for the heightened security needs of the federal government. Yet, even with Federal Information Processing Standards and Suite B cryptography, which is designed to protect data in motion, no portable fat client devices—BlackBerry, Android, iOS, or even PC laptops, for example—can yet be considered suitable for the most sensitive government sites. Many people who work on the SIPRNet may wish this were not the case, but it is.

---

1. VMware Horizon offers two-factor authentication and is FIPS 140-2 compliant.
Part of the Solution

For those who need to protect secret and top-secret intelligence while ensuring proper access to it, the right solution is not, for the foreseeable future, to manage smartphones and tablets, or even laptops, but to provide sufficiently safe and convenient platforms that allow analysts and others to work securely.

Today, this means:

- Hosted virtual desktops, such as VMware Horizon
- Zero clients from manufacturers such as Teradici and ClearCube
- Proper network configuration, including authentication, encryption, and vetting
- Extra security measures, including but not limited to VMware vCloud® Networking and Security™ and security virtual appliances (SVA) supplied by VMware partners

Part of the Precipitate

Defense in depth is always a good idea: as a rule, the more layers of protection, the better. But even with federal spending on cybersecurity expected to double in 2014, not everybody has the budget or the administrative authority to replace all fat client devices at once.

Hosted VMware Horizon desktops, accessed over properly configured and isolated networks, can provide relatively secure access even on otherwise vulnerable platforms, such as heritage Windows 7 PCs. But because fat client devices present weak points in an otherwise secure network—even more if any link in the network chain uses an unsecured segment—every effort should be made to reduce the size of the attack surface they expose. Disabling USB ports, for instance, places restrictions on opportunities for data theft and deliberate introduction of malware. Disabling wireless access also limits the ability of intruders to monitor live sessions. Single-wire access, of course, is best.

Continued use of outdated devices may save on CapEx in the short run, but it increases OpEx and fails to optimize security. On the other hand, temporary re-use of existing equipment as a transition to datacenter consolidation and, eventually, to the Software Defined Datacenter (SDDC), can be considered as an interim approach so long as the limitations of this approach are recognized and monitored.

MLS Sprawl

Government workers who rely on Multilevel Security (MLS) face an additional problem: the proliferation of physical devices on the desktop, which traces its origins as far back as the Cold War. Although the devices themselves have become faster and more powerful, the need for them no longer exists. In fact, their proliferation increases acquisition and maintenance costs while cluttering the analyst’s physical workspace with unnecessary equipment that generally makes intelligence work more difficult.

Instead of a separate workstation, PC, or tablet hard-wired to each network, a Horizon solution allows the analyst to access as many physically isolated networks as needed—typically three, as illustrated—from a single zero-client device.
Summary

It is up to security officers and system administrators to set and enforce access policies and to establish procedures, such as the two-person rule, to limit and contain efforts to circumvent them. Within the confines of software architecture, VMware continues to offer the best solutions available, now and into the near future. However, it is always a mistake for agency executives and security officials to regard current security measures as adequate. On the contrary, even with the most stringent security measures yet developed, there is no substitute for policy enforcement, vigilance, and HUMINT.