The Myth of the Secure Virtual Desktop

Avoid a false sense of security with your VPN or VDI endpoints

Key Takeaways
- Virtual Private Network (VPN), Virtual Desktop (VDI), and Remote Desktop (RDP, RDS) strategies can be effective components of an information access and security strategy.
- These implementations cannot be solely relied upon as a security measure to protect network and endpoint computers from security risks.
- Security is only as strong as its weakest link; a virtual endpoint implementation on a poorly secured endpoint is hazardous.
- Layers of security are required, and conventional endpoint security is still valid in ensuring protection from outsider threats.

Synopsis
There is a lot of misinformation about the security of virtual desktop technology. No one security tool is 100% secure and because of the complexity of technology and how we use it, layers of defence are necessary. You are only as secure as your weakest link. Effective security in your virtual strategy is not automatic or straightforward. IT professionals must also consider the security of the associated endpoint.

In this paper, we will outline why keeping data off the endpoint is harder than you think, and examine issues around passwords and intrusion detection, security software, VPN security, connections and user behaviour.
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Virtual Desktop Illusion and Reality</td>
<td>3</td>
</tr>
<tr>
<td>Keeping Data Off the Endpoint is Harder Than You Think</td>
<td>3</td>
</tr>
<tr>
<td>Passwords and Intrusion Prevention</td>
<td>4</td>
</tr>
<tr>
<td>Security Software</td>
<td>5</td>
</tr>
<tr>
<td>VPN Security</td>
<td>5</td>
</tr>
<tr>
<td>The Weakest Link</td>
<td>7</td>
</tr>
<tr>
<td>No Connection, No Production</td>
<td>7</td>
</tr>
<tr>
<td>Conclusion</td>
<td>8</td>
</tr>
<tr>
<td>Bibliography</td>
<td>10</td>
</tr>
<tr>
<td>About the Authors</td>
<td>11</td>
</tr>
<tr>
<td>About NPC</td>
<td>12</td>
</tr>
</tbody>
</table>
“Personally (and in principle) I’d rather advocate a sound combination of defensive layers than advocate the substitution of one non-panacea for another.”

— David Harley – CITP FBCS CISSP
ESET Senior Research Fellow

Introduction

David Harley said this as he was dismissing the contentious reports that anti-virus software was no longer required, due to its allegedly poor detection rates, while taking the sensible position that nothing in data security is perfect. While we agree with him that AV detection rates are often misunderstood and misreported, and that AV software is still required as part of a solid security posture, his comment is instructive about all data security.

No one security product or tool is 100% secure; layers of defence are essential. While the security weaknesses outlined below can be made secure, any one of them unaddressed can cause the loss of data. The complex technology and networks we use today require layers of defence, and redundancy, to assure data protection. No solution on its own should be relied upon as companies evolve their data management and access strategies.

Endpoint security salespeople are often told “we don’t worry about endpoint data protection because nothing is on them. Everything comes in through the secure VPN and is on the server.” That’s wishful thinking. Unless the user is on a secured diskless terminal with carefully managed multifactor credentials, all endpoints present a variety of risks that need to be dealt with.


2 Endpoints refer to all end-user computing devices including laptops, notebooks, ultra-books, netbooks, desktops and tablets.
It’s easy to believe that a computer is safe because it was set up not to store important data, but nothing is that simple, especially in data security. New threat vectors and methods emerge daily, product updates and patches (or lack thereof) can create risk, and users are notorious for out of policy activity that can place information where it clearly should not be.

The high efficacy and “quality” of today’s threats are also an issue. Today, cybersecurity is a big business and because it is so lucrative, criminal organizations make huge investments in the illicit technology they create. Yesterday’s threats were often obvious to their victims. Infected endpoint computers behaved unpredictably and servers crashed, as attackers showed off their prowess. The thrill for them was in the attack, and in showing their peers how clever they were.

But those days are gone. Today’s threats don’t make themselves known. Instead, it’s to a cybercriminal’s benefit to remain invisible as long as possible, harvesting data that can be sold or used in future attacks. They come in quietly through social engineering trickery, assisted by the collection of key information about staff or the company on social media websites, or through a security hole so small it is near impossible to detect. Their pinnacle of achievement is to have free run of the corporate data, through the VPN, looking like an authorized user from an authorized location and device.

That tactic of staying silent works. In the now infamous Winners breach, after breaking in through poorly secured Wi-Fi that was using only WEP level security built into the access points, the attackers looked like authorized users and stole data directly from the server, undetected for what amounted to years.

User credentials, intellectual property, credit card numbers, banking information, or access to sensitive systems are infinitely more valuable than bragging rights, so today the criminal strategy is all about stealth. Today’s threats are not about disruption, they are about profit. The criminal’s profit, and your loss.

Those concealed threats, such as rootkits which turn computers into components of criminal botnets controlled by attackers, are difficult to detect and even harder to eradicate. That’s why the IT security market is expected to grow at a rate of about 12 percent per year through 2016, according to analysts at International Data Corp.

---

3 Wired Equivalent Privacy (WEP), sometimes incorrectly called Wired Encryption Protocol. An outdated security algorithm for 802.11 wireless networks. Part of the original 802.11 standard it soon became irrelevant due to its numerous security flaws, although it is still in use on unmanaged and outdated networks.


Virtual Desktop Illusion and Reality

There is no question that VPN’s (Virtual Private Networks), VDI (Virtual Desktop Infrastructure) and RDP’s (Remote Desktop Protocol or Services) can increase the security of corporate information and in some instances lower endpoint support and management costs. When corporate data resides in a manage repository, which requires users to work directly on a centralized server through a secure link, that bulk of data is more easily secured. But overestimation of the completeness of the security of this strategy, as a panacea for endpoint security, abounds.

Like the emperor in the children’s story, companies relying solely on just one strategy and believing that they are adequately protected, can in fact be naked to attackers. They can create even more risk than there was before the endpoint virtualization, thinking they can ignore other critical endpoint security practices, as after all, there is supposed to be no data on the endpoints.

That centralized data, set up to be accessed remotely through the endpoints, offers an enticing treasure-trove to thieves, thanks to new ingress points via inadequately protected endpoints. A VPN agent, anti-malware and a strong password policy or multifactor authentication may have been installed on the endpoint, but if just one of many other attack vectors is left unattended, the crooks are in the data. Attackers make a career of thinking of every possible avenue to exploit. Endpoints are in the hands of users, most in the field, and the attackers only need to find one hole.

Let’s look at a few problem areas.

Keeping Data Off the Endpoint is Harder Than You Think

Some companies argue that their data is secure because they require employees to store it only on company servers. The fallacy here is believing that the data exists only on those servers. In fact, even if the user does not do it deliberately, software often saves data, even server-based data, on the local machine in temporary files of various sorts to perform its functions or improve computer performance. It may store user names and passwords, spreadsheet data or pieces of documents, and it may not erase the information when the user exits the program.

If the endpoint is shutdown improperly or experiences a crash, it creates a file of system information to help it properly recover or for system error analysis and volumes

---

"Security is an asymmetric business. Attackers have to be right only once. We have to be right every time." 

– Francis deSouza, Symantec Corp.

---

of data can be exposed. That data can be harvested and used by attackers. This cache, temporary file, working file, and crash-file data may have valuable information itself, or it may also contain clues as to how to access server data to further penetrate the target organization. While it can appear to be deleted at the end of a remote access session, hacker recovery tools can effectively undelete those files.

**Passwords and Intrusion Prevention**

While passwords are a necessary part of any security regimen in virtualized endpoint strategies, they too can be problematic, creating risk when poorly managed. Companies may, for example, implement BIOS hardware passwords as an extra layer of protection and to help lock system configurations. But for convenience they will use the same password on all machines that are not changed when employees leave. It just takes one incautious or disgruntled current or former employee to let that password fall into malicious hands. This, or lack of a BIOS password altogether, can leave a lost device vulnerable to Operating System bypass attacks, and if the data or drive of the device is not encrypted, could provide access to or clues to access the corporate network.

Logon passwords, even if the user doesn’t do foolish things like writing them on sticky notes attached to a monitor or stuffed in the pocket of their computer bag, can also be a major risk. Companies with good password policies requiring regular changes and sufficient complexity may still be compromised if an attacker manages to gain access to a machine via malware, and accesses the file in which the passwords are stored. If the logon passwords are not encoded or encrypted, an OS bypass attack can make for an easy kill. Even if they are encoded, some algorithms do not provide true encryption, but simple storage obfuscation strategies that even a limited-talent hacker can decode.

Since user login credentials give access to shares on servers, once an attacker has endpoint credentials, any files protected by that user name and password are also compromised.

The use of additional authentication factors such as biometric fingerprint readers or access code-randomizing authentication devices like RSA keys is strongly recommended in a virtualized endpoint deployment, when not using a diskless device, on top of strong password policy management. These methods and technologies
provide a critical additional layer of intrusion prevention that can cover for password mismanagement.

**Security Software**
Anti-malware and other forms of security software are a requirement in every security posture, but they can also comprise part of the risk. Unless the products are properly installed and configured, and kept up-to-date and monitored, they too can provide a false sense of security.

The user frequently is unaware when a security product has ceased to function properly. In an effort to be unobtrusive and minimize their impact on operations, anti-malware programs often don’t report their status clearly and visibly. If an update fails, the program simply writes an entry to a log file rather than warning the user that he or she is potentially unprotected against new threats. In enterprise installations, where security staff receives reports of those failures, they can at least be detected and remedied – if the security staff regularly monitors the reports and has the time and resource to deal with them. In a smaller business without central control, problems can go undetected for weeks or months, until an incident prompts inspection of the computer. By then, the machine is often compromised.

**VPN Security**
One huge illusion that bears greater examination is the notion that a connection to the network over a VPN (virtual private network) is impenetrable. Nothing could be farther from the truth. While a VPN is a critical part of an organization’s security arsenal, it is not the be-all and end-all that keeps data safe.

VPNs themselves can provide a false sense of security, not because of flaws in the concept, but because of poor implementation and maintenance.

Most remote gateways are configured by default to report make, model, and even firmware and software versions, on their login screens, and that display is often not anonymized by IT. VPN client software also contains this data, sometimes in unencrypted form. That information is a goldmine for attackers, who have studied the products on the market and know their every weakness; it helps them choose the best way to infiltrate an organization.
VPNs have their own security, but to make things more convenient for users, IT often either stores the credentials on the endpoint, or ties VPN access to computer login credentials. Those credentials may be stored (or transmitted) in an unsecure form, perhaps in plain text. If the computer is not properly encrypted and secured, it can thus become an attack vector for the entire network.

SSL VPNs, also known as clientless VPNs, work through a Web browser that supports the SSL protocol, or its successor, Transport Layer Security (TLS), to secure communications. They do not require a separate client on each endpoint to establish a secure connection. They eliminate the need to install, configure and maintain the client software, and allow users to choose their favourite browser. However, the user may save credentials in the browser, unless it is explicitly configured to prevent this. In addition, any of the security vagaries of the browser can become vulnerabilities for the VPN.

SSL VPNs, according to networking and VPN vendor Cisco Systems (Steven Song, Security Architect for Corporate Security Programs, Cisco Systems Inc., 2010), are vulnerable to man-in-the-middle attacks in which the attacker creates a fake SSL VPN site, which intercepts the user connection, records credentials and then passes the traffic through to the legitimate site. It may also perform other malicious actions, for example, installing a key-logger to harvest other information. These attacks succeed when users either are not aware of how to verify that an SSL certificate really belongs to their intended destination, or have browser settings that don’t flag certificate errors.

Although it provides a secure tunnel into a corporate network, a VPN does not protect the network from malware on the connecting endpoint. An infected machine will, securely, pass its malware on to other vulnerable systems over the VPN. A properly secured endpoint using the VPN is the best defense.

A network access control (NAC) solution that checks connecting computers to ensure they comply with specified levels of anti-malware software and OS patches before they are allowed to access the network can provide an additional layer of protection, however costs for acquisition and administration may be prohibitive.

Finally executives who travel cannot rely on VPN use being permitted in every country. Some governments block their use (Iran is the most recent, prohibiting any but “legal

---

“VPN technologies (SSL VPN included) come with their own security issues. These issues must be dealt with appropriately to ensure the confidentiality and integrity of data and information, as well as overall corporate network security.”

– Steven Song, Architect for Corporate Security Programs Organization at Cisco Systems Inc.

---

and registered VPNs—run by the government, so easily monitored—because they allow users to access unapproved sites on the Internet. Thus travelers who rely on VPN connections may unexpectedly lose that security blanket in some regions, such as China and the Middle East, making a secure endpoint their only defense.

The Weakest Link
Putting technology aside, user behaviour is often the most significant security risk in endpoint deployments. In an effort to do their jobs, or just for convenience’s sake, where they can users will bypass security protocols if they impede the way they like to work, inhibit access to necessary files, or for that matter access to the Internet.

Users will copy data to their computers, regardless of rules, if they find the server connection too slow. While cut and paste features can sometimes be controlled, other methods of copying data such as screen caps and file copies to portable media like USB sticks while inside the firewall, or other inventive ways, like sending themselves files on emails, can be problematic. Stories are plentiful of an organization’s sensitive information being found on the Internet or in the hands of a competitor, and a server hack is immediately blamed. Often it is found that the files were actually plucked off an employee’s home computer, because that computer allowed the employee faster, local tools to do his or her work, off the VPN.

Users are, in fact, the weakest link. They will save credentials on their computer, and find small utility programs which are often not secured, to do so. They will click on dubious links in emails, possibly infecting their systems with malware in the process. If they can’t access needed resources on the corporate network, they may surf the Internet or connect to public wireless networks without launching the VPN. If the computer itself is not secure, it, and the company network resources, are all put at risk.

No Connection, No Production
One of the key challenges of a virtualized endpoint strategy is that when you are not able to connect satisfactorily to the network, you are not working. There are many instances when this occurs, from employees sitting in airports and on airplanes (slowly changing with inflight Wi-Fi), or when sales and field staff are on the move. We say here “connect satisfactorily” as not just any connection to the Internet is robust enough to provide a useful connection. The number one complaint by users as to why

---

7 User behaviour is often the most significant risk in virtualized endpoint deployments.

---

they dislike using the VPN is speed and availability. One or two instances of not being
able to get on the VPN at a critical time motivates them to squirrel away data on their
computer for that big meeting “just in case they can’t connect”, creating risk.

The need for constant connection can drive other dangerous behaviours that may
also bring risky activity to the endpoint, especially prior to or when the VPN is not
yet loaded. To save a trip back to the office or to access a piece of critical information
needed for the next meeting while on the road, a user may dodge into a coffee shop
that offers free public Wi-Fi or use airport Wi-Fi, both notoriously unsecure ways of
connecting. They may also ask a client for guest access on their network, an inappro-
priate request that can expose your company to the client’s security risks, and your
risks to them.

3G/4G/LTE telco wireless are all highly recommended for increased security while con-
necting on the move, as they are inherently encrypted and offer users roaming access
without the need to beg or borrow Wi-Fi. But they too can have coverage, connection
and cost issues.

Conclusion
Certainly all of these risks can be addressed with proper policy and configuration, but
it’s a big job, not to be missed or misunderstood.

Virtualizing the endpoint or relying on the protection of a VPN connection is only one
step in securing corporate data, and it is critically important to employ a full range of
other conventional protections. No one thing can secure a computer or network. Even
security vendors acknowledge that and recommend a layered approach:

• The endpoint device Operating System should be correctly configured and
  patching kept up-to-date.
• Web browsers should be patched and securely configured.
• Anti-malware is critical; it must be properly configured, kept up-to-date and
  constantly monitored for efficacy.
• Hard disk data should be encrypted even if the configuration is designed not to
  store data on the endpoint. If there is a disk present, encrypt it.
• Sophisticated intrusion prevention and password policy management is critical.
• All security components must be monitored to ensure they continue to
  work correctly.
Above all, considering how users work, where they work, and their performance experience is critical. Forcing changes to their operating methods, poor endpoint performance, or cumbersome security will drive them to undisciplined, often dangerous behaviour. All these tasks, and others, combine to secure the endpoint. Although security experts agree there is no such thing as a completely secure computer, virtual or otherwise, the goal is to make it so hard to penetrate that attackers will look elsewhere for easier targets.

It’s a daunting task. IT staff, stretched to capacity, may not be able to keep up with the work involved, tracking and applying updates to installed products, managing encryption keys, and monitoring server and endpoint logs.

One alternative is managed endpoints. Used in combination with your VPN, they are supplied, secured, monitored, backed up, and maintained through managed services by their supplier, providing a security and management alternative. These products are security hardened and configured for high performance and usability. The supplier takes care of vetting and installing patches and updates, and may provide additional services such as remote wipe management of lost or stolen machines and real-time security monitoring. With those burdens removed, IT staffers are freed to innovate and add value to the infrastructure, to work on more strategic projects of the corporate information and technology strategy, and the company is assured that its endpoints are protected by dedicated resources, capitalizing on the benefits of the VPN, without the risks indicated above.
Bibliography


About the Authors

Lynn Greiner

Lynn Greiner is a freelance journalist specializing in information technology and business topics. She is also an IT professional, giving her real-world experience that allows her to cut through the hype and address topics that are relevant in the business world.

Her articles and white papers have been published in both print and online publications, including The Economist, The Globe and Mail, itWorld Canada, Computer Dealer News, CIO.com, Canadian Security, Security Matters, GlobeTechnology.com, Canadian Technology and Business, Computing Canada, and many others.

Lynn holds a Bachelor of Administrative Studies degree from York University.

Larry Keating

Larry Keating is president and CEO of NPC. He is recognized as Ontario’s first Ambassador for Privacy by Design by the Information & Privacy Commissioner of Ontario. Larry has also served as founding chairman of the Ministers’ Technology Advisory Group for the Province of Ontario; member of the Chair’s Advisory Council on e-Government and currently serves as a technical advisor to the Lieutenant Governor of Ontario for the Aboriginal Computer Literacy Program.

He is a speaker and author on a variety of topics including technology trends, data security and embedded privacy, and economic opportunity through the adoption and deployment of new technologies. Larry also founded Keating Technologies, which has been recognized as one of Canada’s 50 Best Managed Companies on three separate occasions, bringing more than $1.3 billion in technology and services to Canadian businesses and consumers.

Peter Giannoulis

Peter Giannoulis specializes in deploying network and security technologies.

Over the last decade Peter has been involved in the design and implementation of client defenses using many different security technologies. He is also skilled in vulnerability and penetration testing having taken part in hundreds of assessments.
About NPC
NPC offers secure, professionally managed computers featuring a suite of backup, wireless, security and customer support services, controlled and supported by a sophisticated support and data centre strategy, for one low monthly payment.

Every NPC device features biometric access with professionally managed encryption and is automatically backed up each day. All systems are constantly monitored for security and backup compliance, malware attacks, physical unauthorized intrusion attempts and system performance. Lost, stolen or defective systems are replaced within 48 hours, with data and applications restored.

NPC provides the benefits of sophisticated endpoint security and management infrastructure without a large financial investment, and keeps pace with rapidly changing privacy and compliance demands, security threats and industry trends to provide certainty and control of confidential information.

For more information, visit www.nopaniccomputing.com, email info@npcmail.net, or call 1-855-667-2642.