Threat Protection and Security

How Your IT Team Should Respond To Recent Headlines

By Jeff McNaught
January 20, 2017

A failure of imagination often leads IT professionals to take half-measures when it comes to protecting corporate data from malware attacks. It's an honest mistake however, since it can be difficult for CIOs or IT professionals – anyone really – to visualize why they might need to invest in yet another security solution or an additional layer of network defenses, just to keep things humming.

After having explored and then purchased the "latest and greatest" option, the challenge these days is to recognize that the bad actors out there are not standing still or creating malware to take on yesterday's solutions. The malware race never stops and can still surprise even the most experienced IT engineers and network managers who do security for a living.

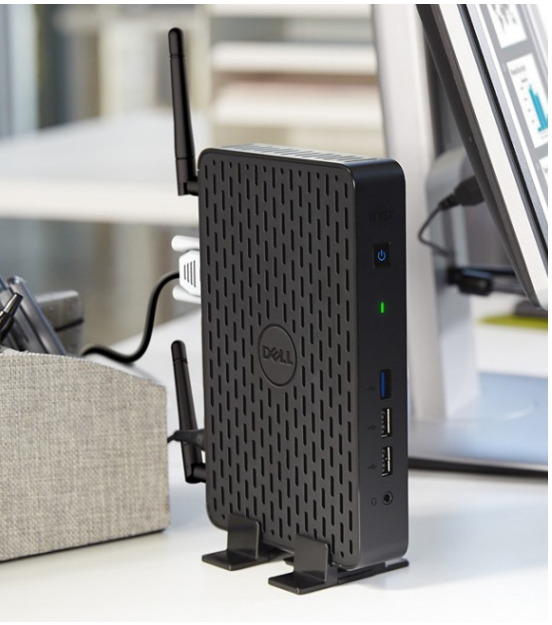
For example, in October 2016, a denial-of-service attack originating from thousands of Web-connected IoT devices impacted several major Web sites in the U.S., including Twitter and *The New York Times*.[1]

1 *The New York Times*, "A New Era of Internet Attacks Powered By Everyday Devices," by David E. Sanger, October 22, 2016

What was novel about this event was that it did not spring from the typical vector: a coordinated linking of bot-nets or zombie computers. That such an attack could be mounted from static nodes in people's homes may have escaped IT professionals focused on the traditional threat landscape of social engineering or phishing-related spam. After all, few would have thought that household devices that lack a traditional operating system such as routers, thermostats, and Web-connected refrigerators could be rallied to create a denial-of-service attack.

More recently, on January 19, more than 700 computers at 16 branches of the St. Louis Public Library were rendered inoperable by a "ransomware" attack.[2] While it is too early to say how the computers were infected, a widespread outage of this sort can be the result of only taking the standard preventive measures against modern malware: The estimated 400,000 new malicious codes registered every day create a relentless ocean tide of "zero day" attacks that are a perpetual threat to every network since they can have a devastating effect on the enterprise.

2 *New York Daily News*, "All 700 Computers In St. Louis Public Library Go Down," by Jason Silverstein, January 19, 2017



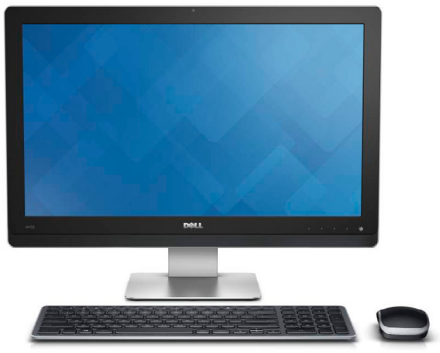
Traditional signature-based solutions will not catch a majority of these variants, creating a false sense of security despite the virus definitions gap. This weakness in the traditional anti-virus paradigm is what has allowed virulent ransomware to bypass defenses at hospitals, law enforcement agencies, and other institutions and negatively impact productivity.[3] Each new malware strain is often just different enough to fly under the definitions radar.

While many enterprises may have "disaster recovery" options in place for remediation, recovering from a true data disaster can be expensive and more disruptive than anyone realizes. By some estimates, the majority of small businesses hit by ransomware face at least two days of downtime, not to mention the effort and new hardware cost of restoring and migrating data to unaffected systems. As a result, the bumper sticker adage about the high cost of education may be apt in this situation: *"If you think doing everything to avoid malware is expensive, try remediation and data recovery."*

Indeed, just when everything may be moving along at a calm and steady state is when a new attack vector can reveal how dynamic the persistent threat has become. Newspaper headlines routinely announce the unfortunate results of having enterprise defenses remain static and focused on previously known attack vectors and already-identified blind spots.

Even so, some IT professionals may be skeptical and even frustrated at the thought of having to add yet another layer of virus protection. Having recently adopted a Cloud Client-Computing architecture which was ostensibly the be-all, end-all as far as endpoint security goes, it is understandable that an IT manager might be annoyed with the suggestion that they consider another, better-still "last line of defense."

3 *The New York Times*, "Los Angeles Hospital Pays Hackers $17,000 After Attack," by Stacy Cowley, February 18, 2016



Wyse 5040 all-in-one thin client

However, as veterans of disaster recovery efforts will readily explain, enterprise IT departments are in a constant arms race with malicious actors, one that requires new moats and drawbridges to thwart whatever innovation allows bad actors to breach safeguards. Case in point, on December 1 of last year, it was reported that as many as one million Google accounts may have been affected by malware that infects Android devices to access authentication tokens.[4] Then on December 14, Yahoo announced that more than one *billion* of its accounts may have been compromised by "forged cookies" that could access user accounts without password credentials.[5]

A New Approach to Endpoint Security enabling fine-tuned control with high productivity

Fortunately, advances in security occasionally put enterprise IT one or two steps ahead of those who would try to degrade worker productivity. The development of thin and zero clients was one such advance: their limited attack surface makes it difficult for viruses and malware to find a footing. Additionally, the ability to manage USB ports and lock the OS from a centralized console, means users have fewer ways to accidentally infect their own endpoints or your broader network.

Wyse's industry unique ThinOS and our zero clients don't have an attack surface that can be easily exploited but thin clients based on Windows Embedded operating systems can be subjected to attacks. If your IT organization doesn't keep the Windows OS regularly patched and protected it can make them vulnerable. Wyse ThinOS thin and zero clients however can be treated in a "set-and-forget" manner, but most other thin clients should not.

But what if you selected a Windows-based thin client for its flexibility, familiar management, and easy peripheral compatibility? How do you remove the risk of successful attack to those devices?

4 *CNet News*, "Google Accounts Hit With Malware," by Joan E. Solsman, December 1, 2016

5 *The New York Times*, "Yahoo Says One Billion User Accounts Were Hacked," by Vindu Goel, December 14, 2016

Enter Dell Data Protection | Threat Defense, a tiny software add-on for Windows-based thin clients, which stops malware from executing, and makes Windows thin clients both flexible **and secure**, even against zero-day attacks. Threat Defense, which could be thought of as the icing on our Cloud Client-Computing security offerings, makes Wyse endpoints the most secure Windows thin clients available. Our innovative malware prevention technology provides an important additional canopy to protect your network and clients, preventing downtime from having to execute an all-hands, full stage recovery effort.

So is it worth it? One minute after an incursion is found to have caused a disruption, security solutions that may have seemed extravagant or redundant suddenly seem reasonable. Cost often becomes a secondary consideration to the daydream of how much might have been saved if only it had been implemented yesterday or a week ago. Preventing the loss of critical data and avoiding the stressful exercise of having to figure out what records and workloads can still be recovered is absolutely sensible.

And yet, IT professionals who have recently invested in desktop virtualization solutions and are certain they have the security situation all figured out, may not be taking advantage of all of the useful options that are now available. The fact is that any endpoint (be it a traditional PC or a hardened thin client) with a browser and email capability, can still propagate malware if a user clicks an infected link or uses a compromised USB drive.

As a result, IT managers leveraging traditional tools such as firewalls, intrusion detection and prevention software, and signature-based malware detection may still be at a disadvantage in this modern era. Luckily, our innovations on the malware prevention side have given IT managers a distinct advantage to prevent risky executable files from launching and corrupting your corporate data.

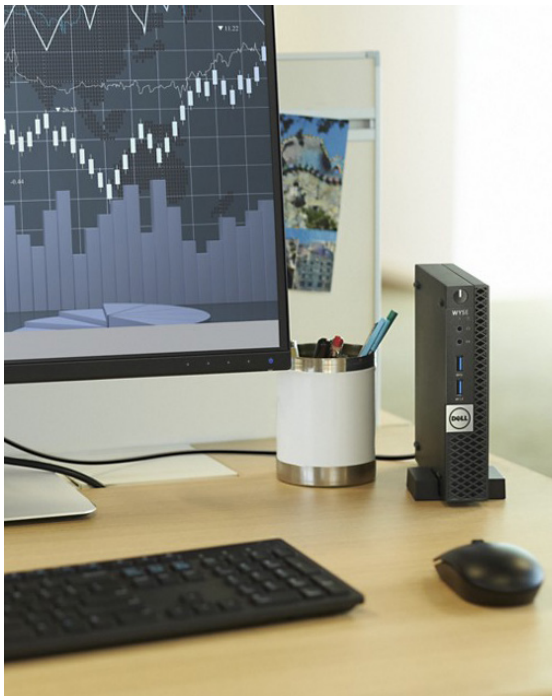
Specifically, rather than relying on constant virus definition updates, or performance killing memory and storage scanning, our solution leverages dynamic mathematical models and artificial intelligence to stop malware before it executes, replicates, or wreaks havoc on your afternoon. Our solution works by looking for executables in the thin client (and is also available separately to protect Citrix, Microsoft VDI, or VMware servers) that diverge from a prescribed, existing software profile. As a result, our solution is able to stop even unknown malware without requiring constant updates to a virus definitions file.

And while it can be frustrating to have to consider a new solution to keep pace with an escalating but often abstract threat, IT managers need to visualize network protection against advanced and persistent threats as a layered, overlapping canopy of multiple safeguards. While thin and zero clients are highly effective, our revolutionary Threat Defense software provides an important new sentry to make your vigilance much more effective.

So while the malicious actors may have been able to count on adding a slight wrinkle to their code to evade detection in the short term, there is now a solution for PCs, Windows thin clients, and even VDI servers that takes a more holistic approach, and does not rely on a cadence of definitions to protect your users and endpoints. Threat Defense can also protect physical PCs, MacOS endpoints, and VDI servers running Windows Server. Regardless of the security solution you may have just deployed, Dell Threat Defense and Wyse endpoints are worth considering in today's consistently unpredictable landscape.

Jeff McNaught is Marketing VP, Cloud Client-Computing at Dell, Inc.

Wyse 3030 thin client



Dell Data Protection | Endpoint Security Suite Enterprise: is a full suite containing three features: Advanced Threat Prevention (ATP), Data Encryption, and Advanced Authentication. Organizations can use the Enterprise Suite to protect virtual desktops and physical PCs.

Threat Defense: contains solely the ATP feature. Organizations can use Threat Defense to protect thin clients running WES7/7p or Win10 IoT Enterprise, physical PCs and Mac OSX.

Learn More

Dell.com/DataSecurity

Dell.com/Wyse/Shield

Dell Cloud Client-Computing
One Dell Way
Round Rock, TX 78664
www.dell.com