TeamViewer
Remote Management

Help (Even Your Resistant) Clients **Protect Against Ransomware**

Your clients may not understand IT security and their role in maintaining security – so it's up to you to protect them in the background

INTRODUCTION

Dealing with various client systems every day, the average managed service provider (MSP) quickly understands the benefits of standardization

A homogenous operating environment is much easier (and therefore cost-effective) to manage, for instance.

It's certainly in your own interest to strengthen security safeguards for your clients – particularly those on fixed monthly contracts. Maintaining a long-term relationship with these clients will depend on the service you provide; a ransomware breach will always reflect badly on your MSP business. But insisting on a common baseline among them is not purely self-serving. Standardization makes it much easier to protect your clients' systems and data against cybersecurity threats.

TeamViewer Endpoint Protection further simplifies matters by triggering alerts whenever there is a network event. These alerts not only advise when there is an issue requiring attention, but also offer documented evidence of what your engineers are doing, and how you are providing value to the customer.

Though you have a real obligation to help clients better secure their systems, many are simply not interested until something goes wrong. All too often security is circumvented because it is felt too 'intrusive' or 'restrictive.' Only when something goes horribly wrong do people begin to take the cybersecurity threats seriously.

As an MSP, you perform many roles. You educate clients about the risks they face. You proactively implement security provisions in agreement with your clients. And you help to pick up the pieces when your best-practice advice is ignored and something goes wrong.

To further complicate matters, modern cybersecurity risks typically come from multiple sources.

Successful defense against ransomware depends on a combination of education, technology, and vigilance.

THE MALWARE **THREAT**

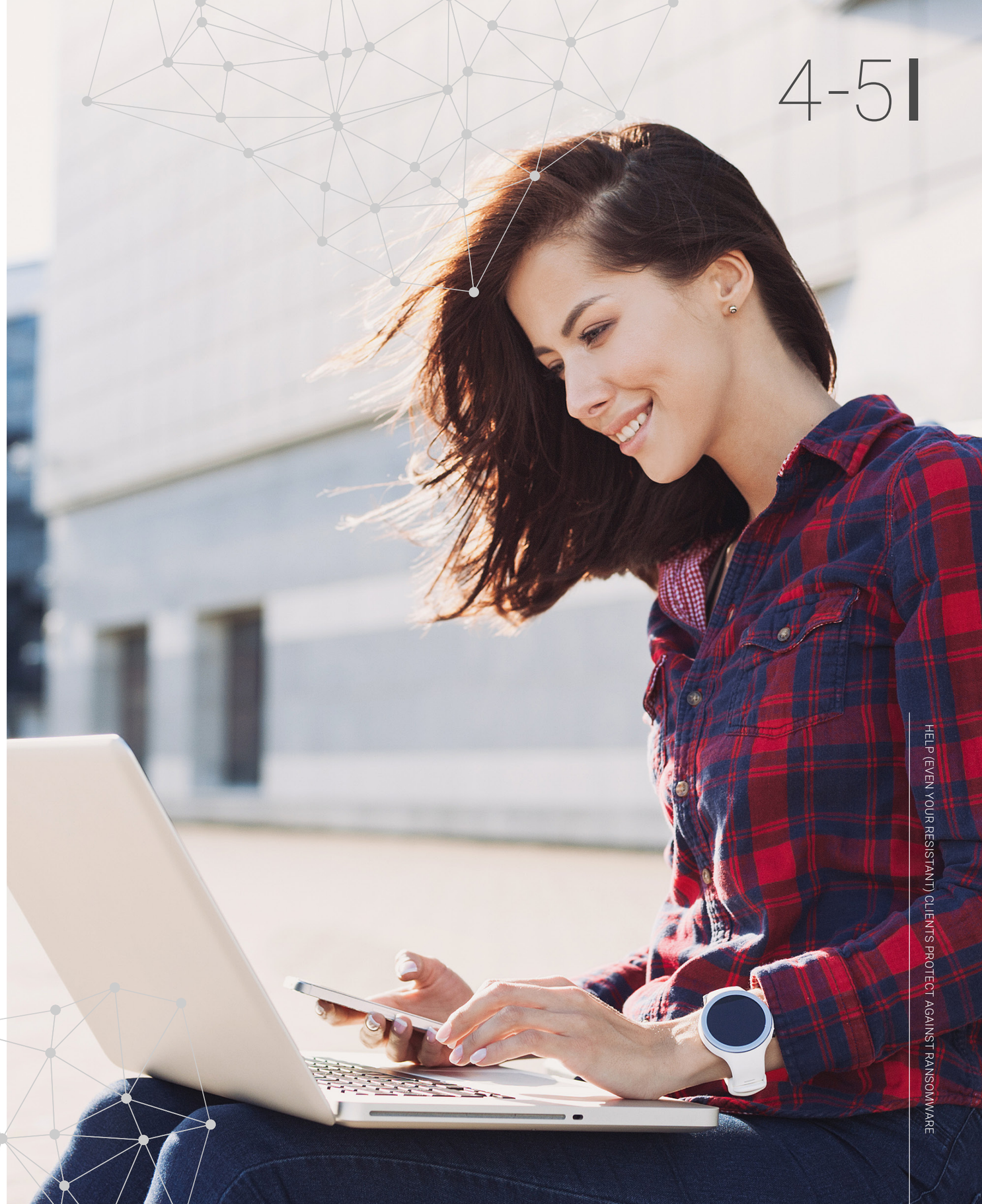
Warnings about malware and ransomware are repeated so often precisely because the threats are so severe.

Headlines about the Petya and WannaCry ransomware outbreaks were inescapable during 2017. But clients have a gift for believing they will never fall victim to a similar event. This willful ignorance can have enormous ramifications.

The latest SecureList report into malware shows a constantly changing threat landscape. More importantly, it reveals that the number of attacks continues to increase month-on-month, reaching nearly 80,000 victims in September 2017.[1]

Even if the MSP is fully informed, their clients may not be. That's why it pays to understand the potential for disaster in advance.

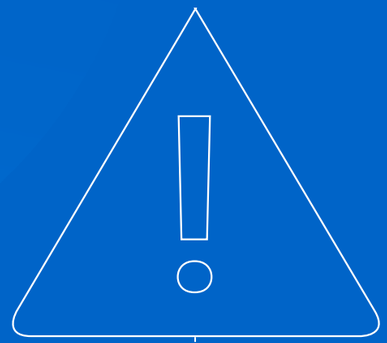
[1] IT threat evolution Q3 2017. Statistics, SecureList https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/

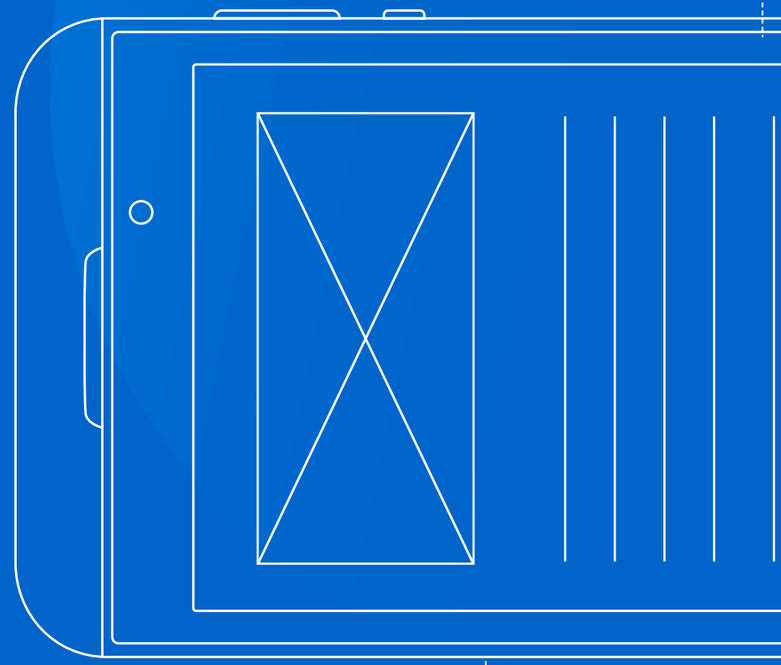


TeamViewer
Remote Management

COMMON SOURCES OF **MALWARE INGRESS**

The modern IT network has so many moving parts that criminals have a huge number of potential attack surfaces with which to work.





As the managed service provider, your duty is to ensure that client systems are as secure as possible.

There are three main routes of ingress into the clients' systems – and modern attacks typically use a combination of at least two.

As mentioned, security is a combination of technical safeguards and awareness training – so you will need to cover them all.

HARDWARE

The devices contained within your client's network will be relatively secure. Defenses at the network perimeter generally perform very well at identifying and blocking malicious traffic and hacking attempts.

Keeping firmware and settings updated will dramatically reduce the risk of network infiltration.

Unfortunately there are still other ways that malware can enter the corporate network. Removable storage devices – like USB thumb drives – can circumvent perimeter defenses and infect local machines directly. Even BYOD presents a potential risk where uncontrolled end user devices are joined to the network.

Many businesses are still heavily reliant on removable drives for transporting data, while others are keen to join the BYOD revolution. Where adoption has been accelerated, corners are often cut. The sad truth is long-term security is often sacrificed for the convenience of instant deployment.

The use of personal equipment in the workplace can be a political nightmare. Obviously clients want to maximize productivity wherever possible. But do they have the right to demand end users provide administrative access to personal devices for security purposes? Even if they do have that right, most will not fully exercise it.

For the MSP, ransomware infections on an end user's personal device are of little interest. But that indifference changes once the personal device connects to the corporate network.

SOFTWARE

Software presents a similar challenge for the managed service provider. Clients use an almost infinite array of applications, each with its own configurations and vulnerabilities.

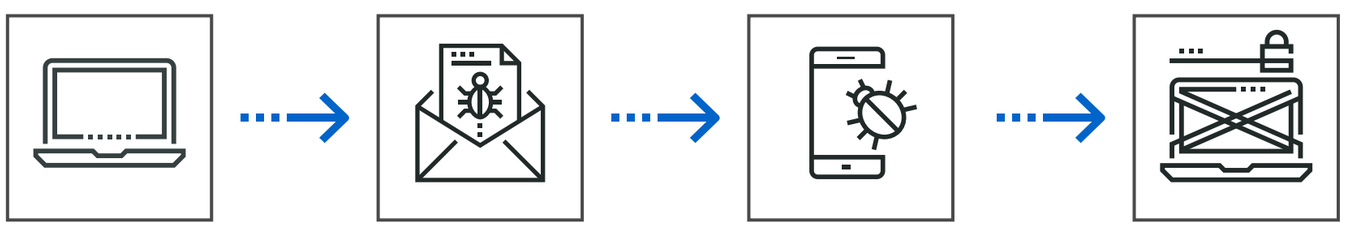
In most cases, software vulnerabilities or operating system bugs provide the launchpad for ransomware attacks. Once a computer within the network is compromised, malware is able to spread itself, inflicting maximum damage and inconvenience for your customers.

The success of the Petya and WannaCry ransomware outbreaks used a Windows OS vulnerability to encrypt files and spread from machine to machine. Microsoft had released a patch to address the issue.

But many organizations chose not to install it.

Obviously, the whole situation could have been avoided by applying patches in a more timely fashion, but the interference with day-to-day operations is clearly unpopular with clients.

This places the managed service provider in an uncomfortable situation, unable to properly fulfill their responsibility to protect client systems – precisely because the client asks them not to.



THE HUMAN FACTOR

The weakest link in any security system is the human factor. Knowing this, hackers are increasingly reliant on social engineering techniques to introduce their malicious payloads.

Infected email attachments are still the primary route into your clients' networks, and the messages more convincing.

Alongside the technical safeguards – spam filters, desktop antivirus, software install permissions – the MSP also needs to help raise the profile of data security concerns with end users. Helping customers recognize and delete suspicious messages will save time, money and resources in the long run.

Unfortunately, end users can be extremely stubborn – some will simply ignore advice and training, while others miss warning signs because they are distracted, stressed, or otherwise engaged.

The MSP will need another weapon to assist in their war on ransomware.

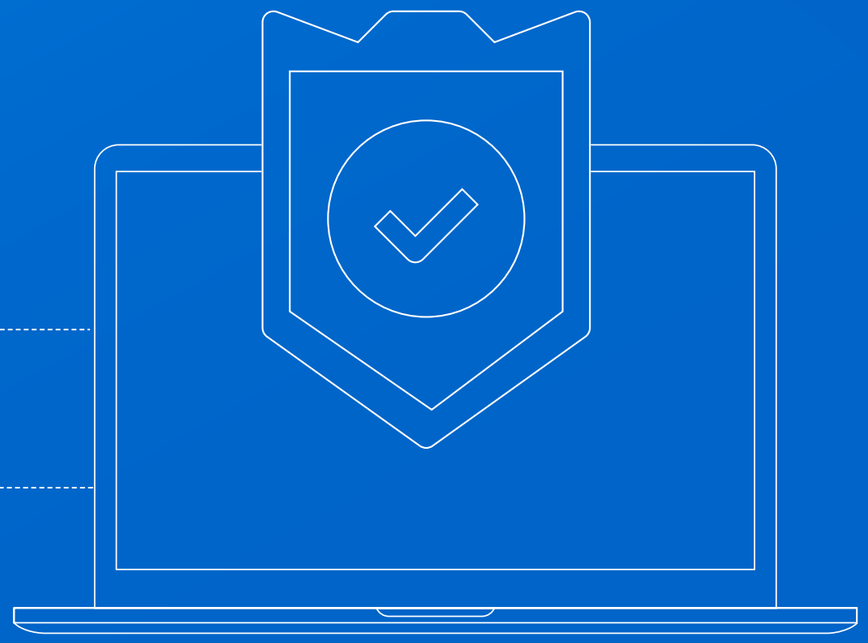
BEHIND THE SCENES **PROTECTION**

Ransomware protection is non-negotiable. But many traditional anti-malware applications struggle to correctly identify and block infections before damage is done.

TeamViewer Endpoint Protection with active ransomware protection takes a slightly different approach. Critical business data is ring-fenced in protected folders – called “safe areas” – that are completely secure from interference. Straight out of the box, securely signed applications from trusted vendors like Microsoft and Adobe will be permitted access to the protected folders.

Nothing inside these protected folders can be modified by unsigned applications. For most customers, these default settings will be all they need. In the event that you do have clients who rely on unsigned applications, you can add them to the active ransomware protection whitelist, thereby granting modify access to the protected files.

Anything else, including ransomware, will remain blocked – permanently. Which means that data cannot be encrypted, deleted or corrupted. Importantly, TeamViewer Endpoint Protection with active ransomware protection overcomes two major complaints about traditional IT security products.



SECURITY “GETS IN THE WAY”

Active ransomware protection (TeamViewer Endpoint Protection) is completely transparent to the end user – and low resource usage means they won’t see any performance degradation on their PC.

The data they need is always available in the apps they use. In most cases they will never realize that information is unavailable outside those applications.

Because they can’t see it, they think the “problem” doesn’t actually exist.

SECURITY **“TAKES TOO MUCH EFFORT”**

Some security solutions are incredibly restrictive – or give the appearance of being so – simply because the end user can “see” them.

Anything that changes the status quo (“I’ve always done it that way”) will prove contentious. You may even find that end users divert significant time and energy to trying to defeat the safeguards intended to protect them. Because TeamViewer Endpoint Protection active ransomware protection tool (part of the Anti-Malware offering) permits access via the apps they already use, it’s unlikely to provoke more complaints from end users. Importantly, the toolkit is built into TeamViewer so you, the MSP, have complete control over the settings.

The active ransomware protection whitelist can be updated within seconds, allowing you to resolve customer issues quickly without creating “temporary” workarounds that could be exploited.

In reality, active ransomware protection works straight out of the box. So end users have one less thing to complain about as you work to keep them safe.

THERE IS A **BETTER WAY**

Ransomware and malware continue to present a significant threat to your customers – even if they refuse to accept the truth. But armed with the right tools – TeamViewer and TeamViewer Endpoint Protection – you can begin to implement safeguards to protect their systems.

And thanks to the transparent nature of the "safe areas," ransomware can be blocked long before any important corporate data is affected. The simple policy-driven management console provides complete control of application access permissions, locking out even the most sophisticated malware.

For those clients who avoid software updates, patches and upgrades, TeamViewer Endpoint Protection is a no-brainer. Ransomware may affect their client devices and cause havoc at the desktop level – but their data is still protected; an object lesson for those clients who refuse to take security seriously.

To learn more about TeamViewer Endpoint Protection, or to arrange a free trial, please get in touch.

TeamViewer
Remote Management

20-21 I

TAKEAWAYS

Malware is a genuine threat to operations – even when your clients disagree

With so many moving parts in IT infrastructure, MSPs need reliable tools to protect their clients

TeamViewer Endpoint Protection active ransomware protection offers transparent security to protect clients behind the scenes

TeamViewer Endpoint Protection works like your end-users, offering protection without hindering productivity

TeamViewer Endpoint Protection (with active ransomware protection) integrates directly with TeamViewer to offer complete control of the client's network

PROTECT YOUR SYSTEMS AGAINST RANSOMWARE ATTACKS **WITH TEAMVIEWER ENDPOINT PROTECTION**

Keep your computers clean and safe. TeamViewer Endpoint Protection protects your computers against threats such as viruses, Trojans, rootkits, spyware, and ransomware. 24/7 - no matter if on- or off ine.

The active ransomware protection in TeamViewer Endpoint Protection simplifies the process of properly securing information against malware. Determine time, scope and thoroughness of each scan-policy and apply them to different computers or groups.

INSTALLS QUICKLY
Effortless deployment – Security in no time.

STAY UP-TO-DATE
Install and forget! No maintenance required on your part.

APPLY REAL-TIME PROTECTION
Protection round the clock – from the second you activate ITbrain Anti-Malware on them.

TACKLE SHADOW IT
USB Auto Scan offers protection from private devices such as smartphones and USB sticks.

STAY IN THE LOOP
Prompt alerts and notifications inform you of important actions - even when you're on the go.

TeamViewer

Remote Management

FOLLOW US ON