ComputerVault Prevents Ransomware and Malware Infections

ComputerVault, Inc. White Paper
November 2019

Stops Ransomware /Stops Malware / Zero Trust Security Model / Virtual Desktops

ComputerVault Prevents Ransomware and Malware Infections

Introduction

Endpoint devices cannot be reliably protected with traditional methods and technologies, because the end-users make mistakes, and every device has vulnerabilities:

- The end-user is the vector for infection
- Ransomware is an industry that costs more than $1 billion annually

The only way to stop ransomware and malware is to adopt ComputerVault Virtual Desktops, (www.ComputerVault.com) because they are specifically architected to prevent ransomware and malware infections from corrupting corporate data and/or shutting down operations, even when endpoint devices are compromised.

Other commercially available virtual desktop products are not viable alternatives because they perform slowly, frustrating the end-user and inhibiting productivity. They also lack ComputerVault's cybersecurity features and are too expensive for widespread adoption.

ComputerVault

- **Faster than a local PC**
- **Costs less than PC's**
- **Stop Ransomware & Malware**

ComputerVault Virtual Desktops are the only virtual desktops that:

1. Run *faster* than a local PC
2. Cost *less* than buying and supporting PC's
3. Have a Cybersecurity Architecture to *prevent* ransomware and malware infection from corrupting corporate data

Because they perform so well, ComputerVault Virtual Desktops also let organizations eliminate PC's and laptops and replace them with a variety of thin clients.

Problem: How to Protect Corporate Data, IP and Operations

The customary prevention strategies for defeating ransomware and malware usually include:

1. Secure Every Device, e.g., antivirus, firewalls, updates
2. Staff Education so as not to divulge personal information
3. VPN Access Updates to make IT aware of traveling staff members
4. Disable Unnecessary Windows Processes
5. Frequent Backups

While endpoint security software identifies malicious file attachments, there will always be unknown threats. Nor can endpoint security software detect links to malicious websites. Inevitably, end-users will unwittingly download malicious files, malware and ransomware and no amount of staff training and

education will prevent an end-user from occasionally being inattentive or unlucky.

Additionally, the endpoint devices themselves have a constantly changing code base that will always contain vulnerabilities. Vigilant patching cannot fix all issues. Lastly, while backups are critical, they frequently fail and they themselves can be infected with malware, rendering them useless.

Solution: ComputerVault Virtual Desktops

Because of their performance and cost characteristics, ComputerVault Virtual Desktops are the first virtual desktops suitable for widespread adoption. Physical PC's aren't needed as the primary staff computing device. Nor are they needed as endpoint devices in a virtual desktop environment as is often the case with competing products. Using a variety of thin clients, an organization no longer need to make the capital investment in PC's and endure the high cost of supporting them.

How ComputerVault Stops Ransomware and Malware

With ComputerVault, every endpoint device only connects to the Internet and a specific virtual desktop. Endpoint devices are not connected to other corporate resources or any other endpoint devices. Furthermore, ComputerVault does not allow any file upload from the endpoint device to the virtual desktop. Malware cannot move from an infected endpoint device to a ComputerVault Virtual Desktops. This makes the ComputerVault Virtual Desktop the conduit to all corporate resources and acts as a buffer between corporate data and the endpoint device.

ComputerVault

- **Eliminate Endpoint Vulnerability**
- **Compromised Endpoints have no effect on data, files or operations**

Any malware that infects an endpoint device travels no further than that device. Since the endpoint contains no data or files, there is no need to recover the endpoint device. The infected endpoint device is removed and replaced with a new endpoint and the user reconnects to their virtual desktop. The infected device is wiped clean and its software reinstalled.

In this way, every endpoint may be treated as always compromised, and completely removes the endpoint device as a vulnerability.

By default, the ComputerVault Virtual Desktops have no access to the Internet. The virtual desktop accesses corporate resources, e.g., applications, files, data, file shares, etc., isolated from both the Internet and the endpoint.

If Internet access is required for the virtual desktop, ComputerVault makes use of a Whitelist. For example, the virtual desktops may need to connect to

the Microsoft Azure Cloud for Office 365. Internet access is then open to Office 365 only. All other domains and websites are excluded.

In this way, Internet access to the virtual desktop is limited to a few known, safe domains that the user requires for work. General Internet browsing is performed by the client, thereby keeping the virtual desktop out of reach of malware.

Prevent Phishing

This capability even stops email phishing attacks. If an email with a malicious link reaches the ComputerVault Virtual Desktop's email client and the user clicks on the link, the request is never sent outside the ComputerVault. Since the malicious website in the link is not part of the ComputerVault Whitelist, that connection is never made and no malware is downloaded.

It is for this reason that ComputerVault uses Whitelists rather than Blacklists. Blacklists contain known malicious domains and websites. But new malicious websites are continually created, and if a domain is not part of the Blacklist then any request to connect a site not excluded by the Blacklist is made.

However, with a ComputerVault Whitelist, it is not necessary to know the existence of every malicious website. ComputerVault has a true Zero Trust Security Model and the architecture and Cybersecurity Suite to prevent malware and ransomware from reaching and infecting corporate data.

Zero Trust Security Model

There are two parts to a Zero Trust Security Model:

1. All endpoint devices are assumed to be compromised
2. There are no trusted domains, users or devices

Because there are no trusted domains, users or devices, every user must provide Authentication as to their identity. Once authenticated, end-users are then Authorized to access only those resources granted to them. Doing so eliminates automatic access to the network and unencumbered access to resources. This limits the damage if valid usernames and passwords are known to a malicious actor.

While an organization must do their best to secure endpoint devices, they should understand and accept that it is impossible to secure endpoints with 100% confidence. Therefore, it is better to adopt the posture that every endpoint device is assumed to be compromised, i.e., infected with malware. ComputerVault Virtual Desktops allows end-users to function productively in this environment without endangering corporate data, files and resources.

Adopting a Zero Trust Security Model, however, involves a significant and difficult transition for an existing IT infrastructure. Even if trusted domains, users and devices can be successfully eliminated, implementing an architecture that incorporates compromised endpoint devices without allowing security breaches is extremely difficult. With ComputerVault, all this is built-in and deployed seamlessly.

Conclusion

ComputerVault Virtual Desktops are installed onsite from a DVD. Their deployment and use require no Rip ‘n Replace or any changes to existing infrastructure.

ComputerVault Virtual Desktops:

- Perform *faster* than local PC’s
- Cost *less* than buying and supporting physical PC’s
- *Prevent* Ransomware and Malware infections

ComputerVault can do this because the technology stack is 100% proprietary. It does not share any of the architecture, components or code base of competing products. Unlike all the other competing products, ComputerVault does not license any software or components from third parties. Customers license it with a monthly, quarterly or annual subscription.

Included in the subscription is the cybersecurity suite and 24x7 monitoring and support of the ComputerVault technology stack from the ComputerVault Network Operation Center.

Every ComputerVault Virtual Desktop uses exactly the same operating system as a physical PC. ComputerVault Virtual Desktops does not use engineered operating systems that are stripped down PC versions. ComputerVault brings no change to the end-user experience.

Active Directory integration is included as well. Customers manage their virtual desktops in exactly the same manner that they manage their existing physical PC’s and network accounts.

The performance, cost and manageability of ComputerVault Virtual Desktops means that any organization can protect their corporate resources, data and files and prevent ransomware and malware from disrupting their operations.

ComputerVault Prevents Ransomware and Malware Infections
November 2019
Published by ComputerVault, Inc.

Authors: Paul Angelo and Peo Nathan, ComputerVault, Inc.

ComputerVault, Inc.
65 Boston Post Road W
Marlborough, MA 01752
U.S.A.
http://www.computervault.com/

Inquiries:
Phone: +1.508.624.9900
Fax: +1.508.624.9905