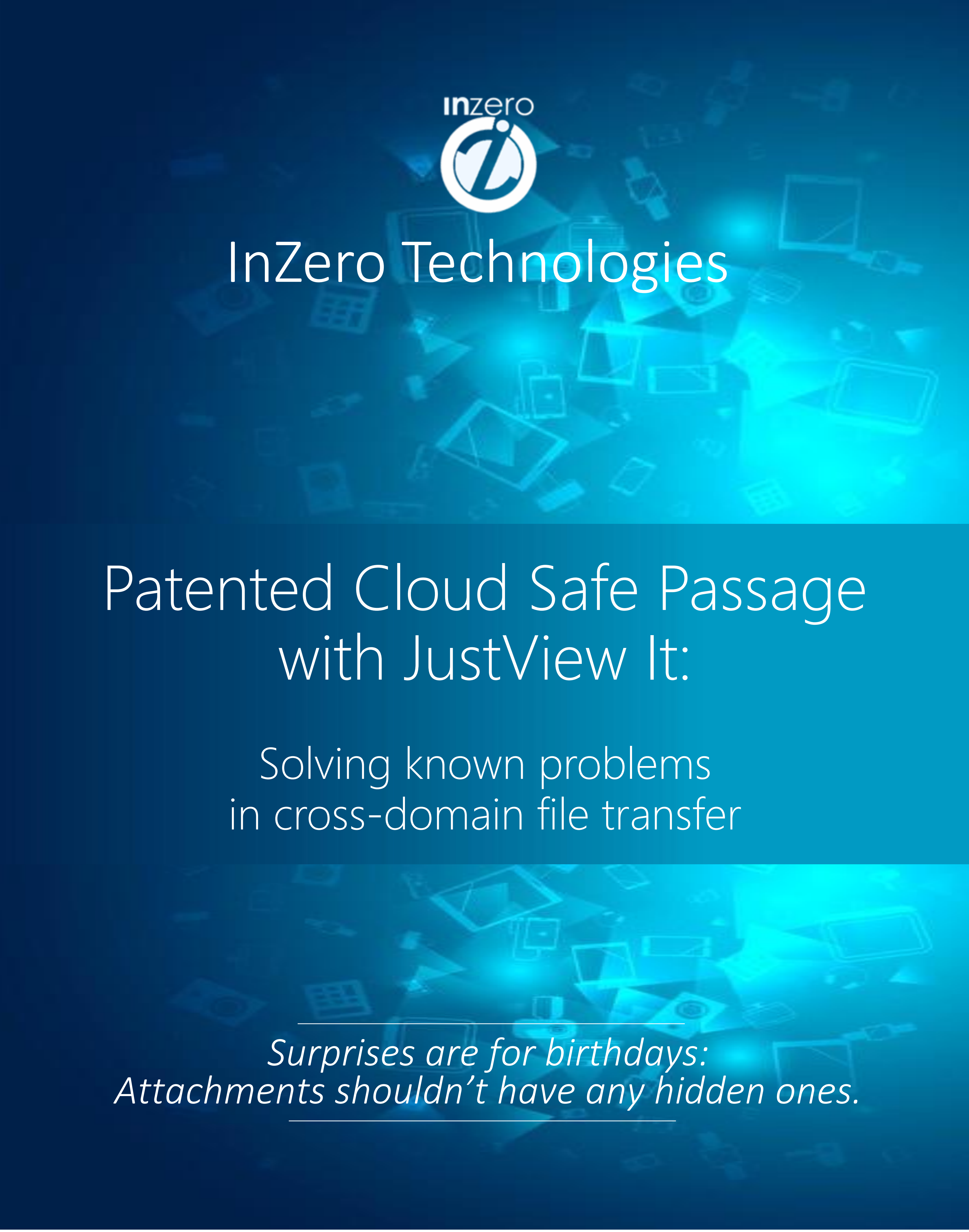


InZero Technologies

Patented Cloud Safe Passage with JustView It:

Solving known problems in cross-domain file transfer

Surprises are for birthdays:
Attachments shouldn’t have any hidden ones.

Introduction: Hidden malware is alive and well

Each year, major industry players like Verizon, McAfee and Symantec conduct surveys and analyses of data breach. And each year the results point to the usual suspects:

- ✓ The vast majority of breaches begin in the endpoint device[1]
- ✓ Often, the culprit is a legitimate looking email[2]
- ✓ But in reality, the email – or its attachment – is hiding malware, surreptitious code that can infect the user's endpoint device[3]
- ✓ And from there, malware proceeds to infect more devices or worse, causes widespread infection throughout the network[4]

Today, the risk of a malicious email or attachment is exacerbated by the increasing number of business groups – intranets – to which the user belongs. This especially includes government "trusted groups" (e.g., enclaves, interconnected IC ITE and other disparate networks, OCITE Primary and Secondary User Communities),[5] and high-security verticals (e.g., healthcare, finance, infrastructure, retail). These days, when it comes to receiving and forwarding emails, what may seem like "six degrees of separation" is really no separation.

And, when an email comes from a known business affiliate, it is rarely suspected of hiding malicious content, yet may contain malware not only from its original creation, but picked up along the way. The false comfort in assuming a colleague's email is safe and clean, is exactly why this form of attack – hidden malware in an email or its attachment – continues to be in vogue.[6]

> *"Just the simple act of opening the PDF file can exploit a vulnerability to automatically download malicious code from the internet and display a decoy PDF file to trick you into believing that nothing wrong has happened."*
>
> *nakedsecurity.sophos.com*

Current File Transfer Security: Vulnerable and Unreliable

Defenses typically used against such hidden malware generally fall into two security genres: (1) antivirus – software apps that, one way or another, attempt to uncover pernicious, or at least questionable, code passing through the user's device, and/or (2) content disarm and reconstruction ("CDR"), sometimes called "Sanitization" – using existing methods that convert data forms, like jpg images to bitmaps for example, to strip away other code which can carry hidden executable malware. To do this, CDR, first, with the help of common antivirus programs, attempts to determine "safe" file content, deleting or storing in quarantine "unsafe" code (the Disarm function) and second, transmits safe content, in new or original file format, to the recipient (the Reconstruction function).[7]

"Once hackers control the antivirus program they can manipulate it to execute all sorts of attacks"
wired.com

Antivirus solutions come in all shapes, colors and sizes, and at the end of the day are dependent on recognizing harmful strings of code, making this form of defense particularly vulnerable to newer and newer, zero-day attack methods. Industry researchers have long questioned whether antivirus solutions are "*worth the money*"[8] but perhaps more disturbing is that antivirus can be used as a conduit to transmit malware.[9]

This risk is very real and very serious. Earlier this year, researchers found that 14 vulnerable antivirus programs (Norton, McAfee, Kaspersky, TrendMicro, Bitdefender, Avast, others) can allow their programs to execute "*all sorts of attacks*":

> *"You're installing antivirus to protect you, but actually you're opening a new attack vector into your computer. . . As the attack unfolds, it allows malicious code to become persistent . . . even measures like a system reboot won't eliminate a DoubleAgent attack. And once hackers control the antivirus program they can manipulate it to execute all sorts of attacks, from passive surveillance to encrypting and ransoming off data, because of the inherent trust operating systems place in antivirus programs".*[10]

No wonder the U.S. Department of Defense calls cyber security "*Patch-and-Pray*".[11]

As for CDR, this approach has its roots in "data format conversion" methods that have existed for over two decades. Conceptually, CDR is effective to make sure that only the expected data format is transmitted, for example, that an MSWord (.doc) attachment is a genuine .doc file type, and not another file type.[12]

Implicit in standard CDR technology is the assurance that the CDR process cannot be usurped by malware, and that transmitted content is both valid file content and "good enough" to give the user what's needed.

Neither of these is correct.

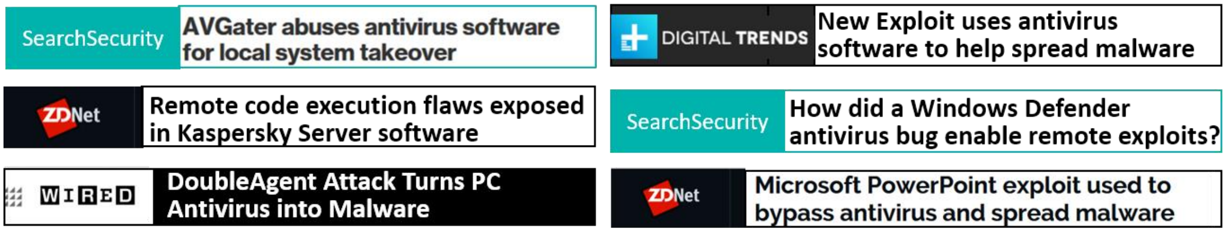
State-of-the-art of today's CDR technology: You can't be sure of what you're getting

Several commercial vendors offer CDR services, using known file format conversion programs. These are currently promoted as "new" and even "disruptive" – despite the fact that (as we elaborate below) InZero embodied such technology in its patented and NIST-certified InZero Gateway several years ago.

Regardless, when using known file format conversion programs, CDR inherently risks both malware infection itself, and incorrect replication of the intended safe content. For example, one vendor stresses that its CDR "*does its best to keep the data intact may it be the layout or the content*" . . . but using a conversion process, "*sometimes the layout is lost, sometime the content might be scrambled*." Moreover, the user is cautioned to "*stay aware that this might not work against well designed 0-days: If an exploit is found in the [Disarm process] . . . we won't remove anything.*" Likewise, researchers acknowledge *"that* *the use of CDR can decrease document usability by stripping out active code intended for legitimate purposes.*”[13]

The risk that incoming malware overcomes the initial Disarm function is very real, and may not be easily detected. When antivirus content analysis is used in the attempt to discover and delete (or quarantine) hidden malware, the antivirus technology itself may be vulnerable, as was made quite evident by this year’s Clever “*DoubleAgent attack*,” and Clever itself is a highly successful exploit method that avoided detection for over seven years of successful intrusion.[14]

Some Recent Headlines . . .



SearchSecurity — AVGater abuses antivirus software for local system takeover

DIGITAL TRENDS — New Exploit uses antivirus software to help spread malware

ZDNet — Remote code execution flaws exposed in Kaspersky Server software

SearchSecurity — How did a Windows Defender antivirus bug enable remote exploits?

WIRED — DoubleAgent Attack Turns PC Antivirus into Malware

ZDNet — Microsoft PowerPoint exploit used to bypass antivirus and spread malware

It is, therefore, not surprising that today’s CDR technology is accompanied by legal disclaimers and caveats – “As Is, “With All Faults”, including against “Cyber Attacks”, etc. – which all boils down to, when you subscribe to the vendor’s CDR service, you get what you get in both security and usability, or lack thereof.

Recognizing this unacceptable state-of-the-art, and drawing upon our successful development of a NIST-certified CDR, we have developed Cloud Safe Passage:

- ✓ To overcome the longstanding security vulnerabilities of standard CDR technology
- ✓ To employ proprietary CDR file format conversion programs to identically replicate the original expected content
- ✓ To make sure the user can even compare the original and replicated file without security risks
- ✓ As desired, to provide the CDR program itself for testing and verification as desired, so the organization is not dependent on some anonymous vendor service

Addressing the specific risks and problems of today’s CDR technology

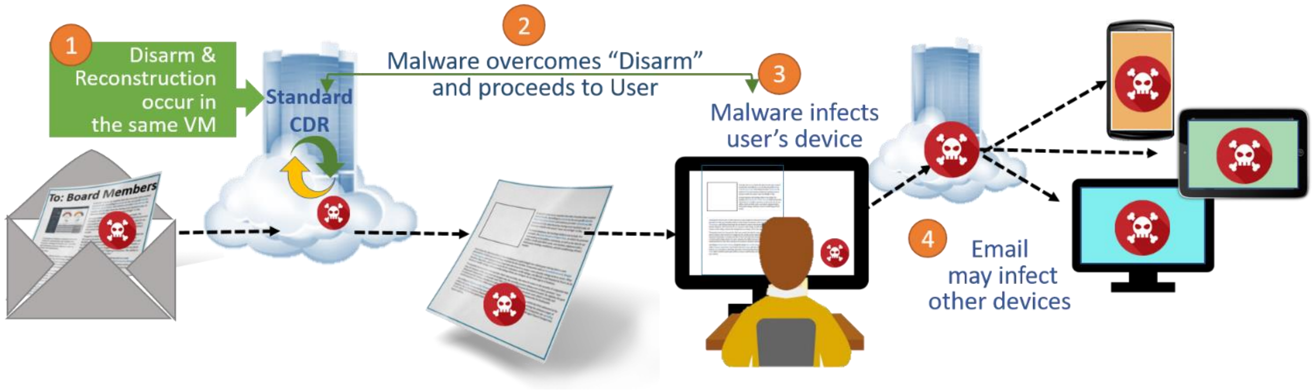
To provide a truly secure and reliable useful CDR technology means coming to grips with four main risks and problems:

1. **The malicious email making the rounds.** Current CDR technology is a single software program performing both Disarm and Reconstruction functions. Inherently, like other software security products – firewall, antivirus, IDS, etc. – it is vulnerable to malware, particularly when crafted to overcome it, just like Cleaver’s DoubleAgent could overcome many popular antivirus products. When this occurs, the Disarm function is ineffective and the hidden malware will continue on to the recipient,

who may forward the email to others. Even if security policy requires CDR processing for each transmittal, the malicious email will still overcome the Disarm function.

Problem No. 1 (Security)

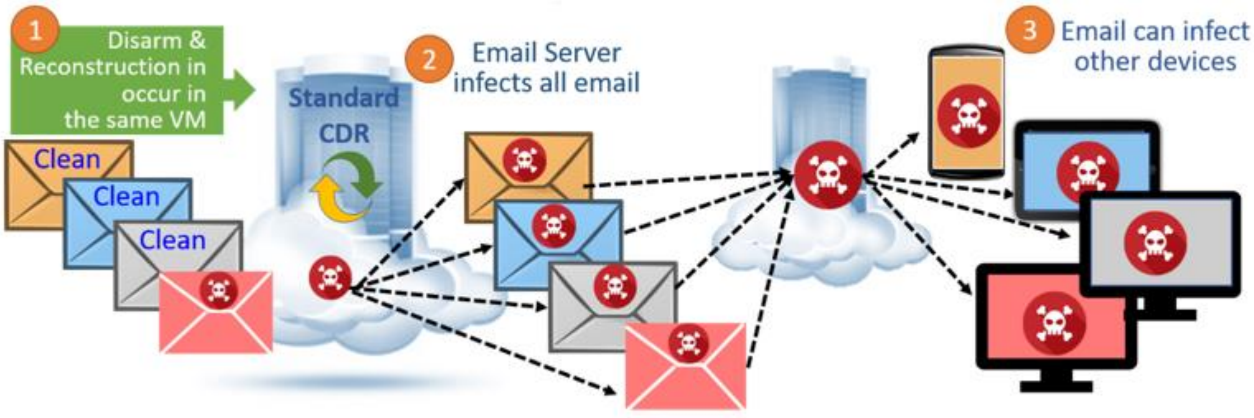
Malware is undetected in "Disarm" and proceeds through to "Reconstruction"


1
Disarm & Reconstruction occur in the same VM
To: Board Members
Standard CDR
2
Malware overcomes "Disarm" and proceeds to User
3
Malware infects user's device
4
Email may infect other devices

2. **Worse: Turning CDR into a conduit for network infection.** Malware that overcomes the Disarm function can also take over the CDR process and effectively attach itself, so to speak, to other emails and attachments, infecting clean files throughout the network. As we have seen, even antivirus quarantine has been used to launch network-level infection. In this way, using standard CDR technology, the Reconstructed email or attachment becomes the ultimate Trojan horse.[15]

Problem No. 2 (Security)

Malware undetected in "Disarm"
and infects CDR process to infect other emails going through

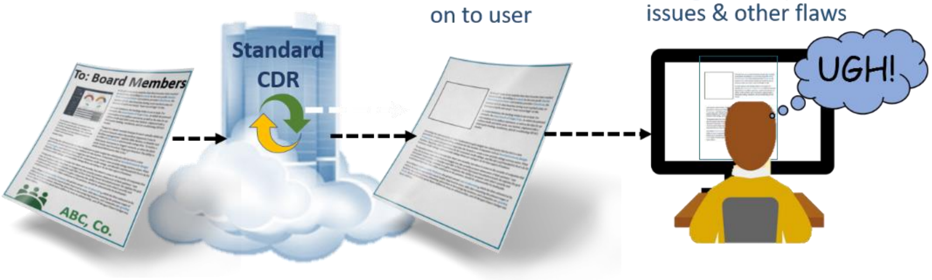

1
Disarm & Reconstruction in occur in the same VM
Clean
Clean
Clean
Standard CDR
2
Email Server infects all email
3
Email can infect other devices

Something's not quite right.

Common data conversion programs typically yield files that are not identical to the original appearing file, variously eliminating or transposing content, or changing format structure and the like. This obviously impacts not only the ability to work with content, but confidence and reliability in the Reconstructed file.

Problem No. 3 (Usability)

Reconstructed document is not identical to the original



Document is converted in CDR and sent on to user

Reconstructed document typically has obvious missing content, format issues & other flaws

Problem No. 4 (Usability)

And user can't compare documents to see differences, without risking infection

3. **Guessing what the original looks like.** It would be nice to at least compare versions. Standard CDR can preserve and store a version of the file, before processing it. However, for the user to be able to visually compare the original and Reconstructed versions, usually requires downloading the original and thereby subjecting it to the very infection sought to be prevented. This inability to compare further serves to lessen confidence and reliability in the Reconstructed file. Users shouldn't have to guess.

Standard CDR technology cannot provide the assurance that the CDR process remains unaffected by incoming malware, or that what the user finally receives is at least "good enough". Indeed, boilerplate disclaimers in commercial products caution as much.

Also, using commercial CDR puts the organization at the unknown risks that might be present in the vendor's process or network. In a perfect world, the organization would have full control of the CDR technology used on its emails and attachments.

The InZero solution overcomes the four main CDR problems and gives the organization the control it deserves.

InZero's Cloud Safe Passage: Using our experience to eliminate the risks and problems

InZero Systems is built upon a unique foundation: Directly attacking and slaying the known risks and problems that have permeated cyber security where, every year, the most damage originates – the endpoint device.

Our proprietary Technologies address the five major endpoint risks and problems:

- ✓ Escalated Privileges
- ✓ Hidden Malware
- ✓ Data Exfiltration
- ✓ OS Code Vulnerability
- ✓ Malicious Insider

Initially, this led to the development of the InZero Gateway for desktop security. To accomplish genuinely secure file transfer, the Gateway embodied CDR in its "Conversion Engine". The Gateway is patented, and is NIST-Certified, FIPS 140-2 (at https://csrc.nist.gov/Projects/ Cryptographic-Module-Validation-Program/Standards), and the validity of its security technology was independently validated by Verizon's ICSA Labs, among others.

While current CDR vendors present their technologies as "disruptive" and even this past March, Gartner called CDR "new", InZero pioneered CDR technology for its Gateway over five years ago, and our copyrighted "*Access the Internet Without the Internet Accessing You*" (2011-12) presented Gateway technology that

- ✓ *"Subjects the data to a process which converts (the "Conversion Engine") and reconstructs the data in the form of a trusted application embedded in the hardware"; and*
- ✓ *"Enables the user to work with the reconstructed data using standard applications on the PC supported by an embedded application".*

Subsequently, in turning to today's practical computing methods – notably, proliferation of mobile device use for both business and personal needs, and now, also for IoT – we have created the InZero Trilogy for "*incoming, outgoing, and sideways*" data transfer.

For incoming and outgoing security, we developed the first hardware-level multiple complete operating systems (OS's), called WorkPlay; the first practical mobile Type-1 bare-metal hypervisor, solving power and performance problems; and our hardware-level endpoint OS TrustWall, which prevents unauthorized outgoing traffic even if an endpoint OS is infected or the user is lured by a phishing attack to give up network login credentials.

And now, for truly secure and convenient *"sideways"* cross-domain file transfer, we have developed both Mobile Safe Passage (for in-device implementation) and Cloud Safe Passage (for cloud file transfer service.

Cloud Safe Passage: First and foremost, solving the main SECURITY risks and problems

Standard CDR suffers from the vulnerability that in the battle between hidden malware and the CDR process, malware can win. When malware overcomes the Disarm function, it remains resident in the process and can take over the Reconstruction function to not only cause circulation of an infected email or attachment, but to cause widespread network infection as well. By not recognizing malware, the CDR process may as well not occur at all – or worse, because it accesses the organization network email path, easily spreads infection.

To attack and slay this enemy, our proprietary and patented Technology:

- ✓ Separates Disarm and Reconstruction into two separate VMs
- ✓ Recognizing that the Disarm function can be compromised by effective malware, replaces the Disarm VM with a clean Disarm VM each and every time a file is processed to eliminate any possibility of continued infection of the process
- ✓ Include desired integrity checks

Cloud Safe Passage: Solving main USABILITY risks and problems, too

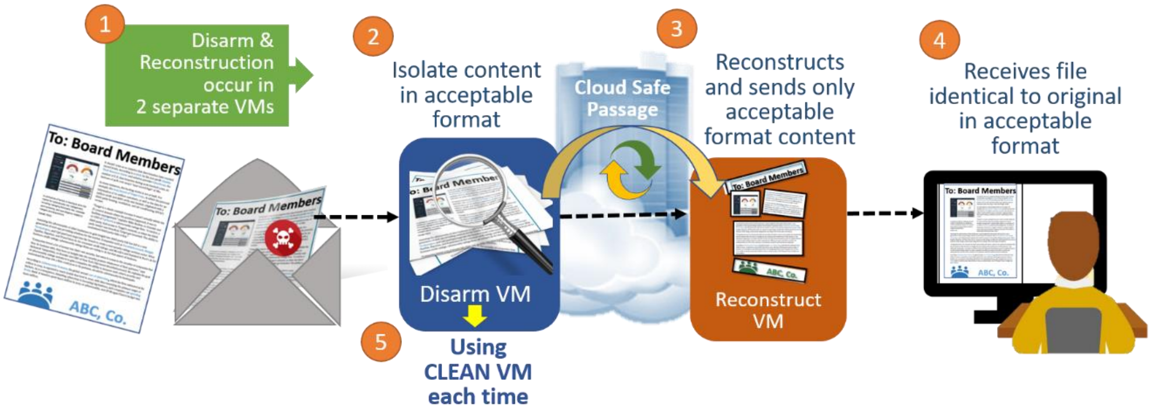
With current CDR technology, the user really has no way of knowing whether the resulting file looks and is identical to the expected, ostensibly clean email or attachment. What is known, is that the various data conversion programs offer varying degrees of accuracy in Reconstruction – quite often, omitting headers and footers, shifting graphics, changing font and so forth. This is both a matter of convenience – working with a file or forwarding a file purporting to be an original – and, critically, altering substance, because missing or changed information may lead to misinterpretation.

To attack and slay this enemy, InZero's Cloud Safe Passage:

- ✓ Employs proprietary code specifically developed to provide complete identical replication of the valid original file content, as it appears in the original

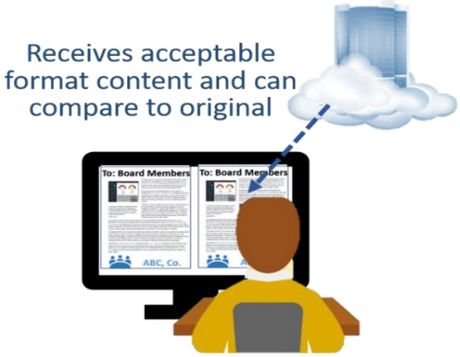
Solutions No. 1 & 2 (Security)

InZero Cloud Safe Passage


1
Disarm & Reconstruction occur in 2 separate VMs
To: Board Members
ABC, Co.
2
Isolate content in acceptable format
Disarm VM
5
Using CLEAN VM each time
3
Cloud Safe Passage
Reconstructs and sends only acceptable format content
Reconstruct VM
4
Receives file identical to original in acceptable format

Solutions No. 3 & 4 (Usability)

InZero Cloud Safe Passage


Receives acceptable format content and can compare to original
To: Board Members
To: Board Members
ABC, Co.

✓ For reliability, sends a link to the user which allows the user to compare the Reconstructed file with the original file that is visible in the cloud, thus eliminating the risk of downloading the original file, which of course renders the CDR function futile because it can contain the malware sought to be avoided.

Cloud Safe Passage for internet browsing

Cloud Safe Passage technology is applicable as well to internet browsing and file downloading. For this, we are developing the required end-user client, not needed for cross-domain email and attachment file transfer.

Meeting each customer’s specific needs

The vast majority of government and enterprise normal business email and file transfer communications employ Microsoft Outlook Exchange, and by and large, attachments are

created in certain well-known formats, notably, MSWord, PDF, Excel, PowerPoint and commonly used image formats, such as jpeg. These are the initial format types for Cloud Safe Passage use. Our proprietary code development method will yield identical replication of commonly employed file segments – e.g., logos and other images; headers and footers; graphics and tables; signatures; and so forth. Importantly, we can tailor proprietary code for identical replication of any special file template.

Our Cloud Safe Passage technology – the specially developed code to assure identical replication to meet customer needs – is available for license, and can be customized, verified and tested to assure it meets specific customer needs in security, usability and reliability. Our Cloud Safe Passage becomes your Cloud Safe Passage.

Product status: Ready to go

Patented Cloud Safe Passage is ready for customer evaluation:

- ✓ Custom, proprietary code has been created for commonly used file formats, each segment developed separately object-by-object (chunk-by-chunk) to assure exact replication of different file components, i.e., headers/footers, graphics, etc.
- ✓ Available as cloud service or customer hybrid cloud using AWS
- ✓ Implementation for pure cloud forthcoming

Cloud Safe Passage is made ready for delivery to our customer lock, stock and barrel. The customer is provided full possession and ownership of technology code/apps to enable the customer to perform the file transfer service for its own use or marketing to its customers. Additional file customization is available for proprietary or unusual formats, if desired.

Conclusion: It all boils down to . . .

We don't claim to have invented basic CDR technology, or that it's new or disruptive. We do claim we previously developed it in a patented and U.S. NIST-certified standalone device. Now, we have tackled CDR implementation for the cloud in the same way we tackled mobile security – attacking and overcoming security vulnerabilities and practical weaknesses. The result is a Cloud Safe Passage that:

- ✓ belongs to the customer,
- ✓ provides identical file replication (excluding hidden active code),
- ✓ keeps the new file Reconstruction away from incoming malware, and
- ✓ just in case, gives you peace of mind comparing the original with the result.

What you get is what you expect. And no surprises.

[1] https://www.darkreading.com/endpoint/new-study-shows-mobile-devices-the-cause-of-some-data-breaches

[2] https://www.csoonline.com/article/3172711/phishing/5-ways-to-spot-a-phishing-email.html

[3] https://www.us-cert.gov/ncas/tips/ST04-010

[4] https://www.us-cert.gov/publications/virus-basics

[5] https://govtribe.com/project/osd-compartment-it-enterprise-business-requirements

[6] https://www.theregister.co.uk/2017/11/16/terdot_banking_trojan/

[7] https://en.wikipedia.org/wiki/Content_Disarm_%26_Reconstruction

[8] http://www.zdnet.com/article/is-paying-for-antivirus-a-waste-of-money/

[9] https://www.wired.com/2017/03/clever-doubleagent-attack-turns-antivirus-malware/

[10] https://www.wired.com/2017/03/clever-doubleagent-attack-turns-antivirus-malware/

[11] https://www.networkworld.com/article/3188632/security/darpa-to-eliminate-patch-and-pray-by-baking-chips-with-cybersecurity-fortification.html

[12] https://en.wikipedia.org/wiki/Content_Disarm_%26_Reconstruction

[13] https://github.com/docbleach/DocBleach/wiki

[14] https://www.wired.com/2017/03/clever-doubleagent-attack-turns-antivirus-malware/

[15] https://fossbytes.com/avgator-exploit-abuse-quarantine-restore/

InZero Technologies, LLC