

A man in a white shirt and lanyard is looking at a tablet in a server room. The background shows server racks with blue lights.

VOTIRO✓

How to

Plug the Gaps Found in Antivirus, Next-Gen Antivirus and Sandboxes File Security

Table of Contents

3 How to Plug the Gaps Found in Antivirus, Next-Gen Antivirus and Sandboxes File Security

4 Stages of Vulnerability Life Cycle

5 The Need for Better File-Based Security

6 figure 1. Perceptions About Endpoint Security Risk

7-9 Security Technologies and Their Gaps

10 Common Sandbox Evasion Techniques

11 Positive Selection Technology Stopping Threats Other Solutions Can't

12 How Positive Selection Technology Works

13 Key Benefits

14 Summary

15 About Votiro

How to **Plug the Gaps Found in Antivirus, Next-Gen Antivirus and Sandbox Content Security**

Many organizations believe that using antivirus (AV), next-gen antivirus (NGAV), and sandbox security technologies is the best practice for content, data, and file security.

While these technologies are certainly important for threat prevention, each has its own vulnerabilities that can be exploited by malicious hackers seeking a way to disrupt business activity and make quick money.

This eBook explores these security techniques, identifies the gaps in each, and explains how a particular technology – Content Disarm and Reconstruction – can fill those gaps and ensure your files, content, and data are safe of hidden threats.



Stages of Vulnerability Life Cycle

Software vulnerabilities open the door to cybercriminals. A hacker who discovers a vulnerability can use it to gain entry to a system and then obtain unauthorized access to data. A vulnerability consists of three stages: undisclosed, zero-day, and patched.

Stage 1 Undisclosed

At this stage, a vulnerability in an application, system, or hardware is unknown to the vendor or the security community but has been discovered by someone, possibly a researcher in a cyber warfare organization or the hacker community. This type of vulnerability presents a high security threat to everyone and can go undetected for years.

Because the application's vendor does not know of the vulnerability, countermeasures cannot be developed to prevent or block its exploitation. Undisclosed vulnerabilities are frequently used by groups that gather cyber intelligence or trade information to receive large cash payouts.

Stage 2 Zero Day

At this point, the vulnerability has been disclosed to the vendor and the security community. A zero-day vulnerability is a software flaw that has just been discovered for the first time, and no patch for it has yet been developed. This type of vulnerability presents a high risk of exploitation; intrusion detection systems or traditional protection systems using signature-based detection might identify exploitation activity after gathering and extracting several samples, but an exploit that a hacker has manipulated will be able to avoid signature detection.

Zero-day vulnerabilities can go unaddressed for some time, because vendors may take 90 days or even more to respond to reported threats.

Stage 3 Patched

At this stage, although the vendor has already issued a patch for the vulnerability, it can be opportunistically exploited in non-patched environments of out-of-date applications. Large enterprises may be particularly susceptible to opportunistic attacks, because patch management is more cumbersome than in smaller organizations. The threat level at this stage is low, because the vendor has provided a patch.



The Need for **Better File-Based Security**

According to the [2020 Annual Study](#) on the State of Endpoint Security Risk by the Ponemon Institute, the frequency of attacks against endpoints is increasing. 68% of respondents reported that their company experienced one or more endpoint attacks that successfully compromised data assets and/or IT infrastructure over the past 12 months, an increase from 54% of respondents in 2017. 51% stated that their endpoint security solutions are ineffective at detecting advanced attacks.

An average of 10 million new malware threats are recorded per month.
- AV Test



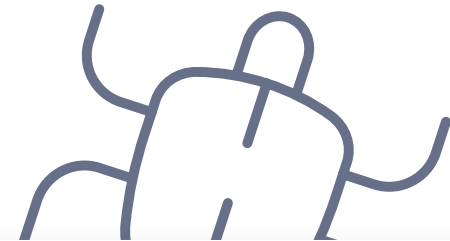
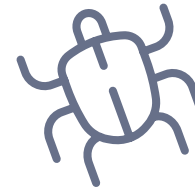
These difficulties may stem from the fact that an average of **80% of successful breaches are new or unknown zero-day attacks that are not recognized by traditional signature-based detection solutions**. In addition to being more effective, zero-day attacks have also become more prevalent and are increasing in frequency, with new or unknown zero-day attacks expected to more than double in the coming year.



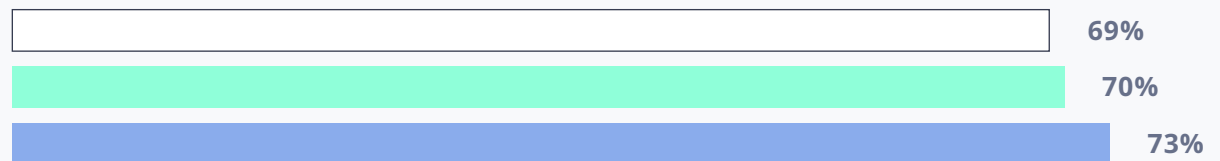
Figure 1

Perceptions About Endpoint Security Risk

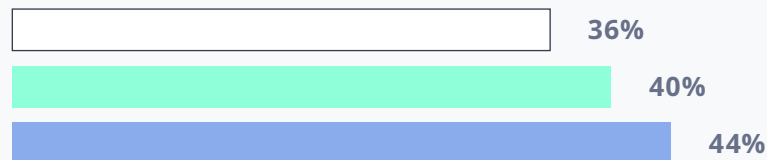
Strongly Agree and Agree Responses Combined



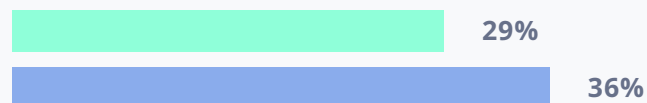
New and unknown threats against our organization have significantly increased



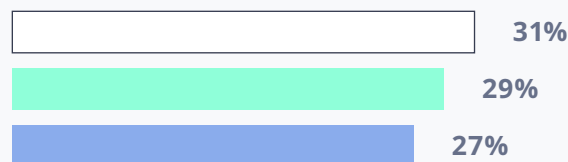
We have ample resources to minimize IT endpoint risk due to infection or compromise



Endpoints are more at risk today due to infection or compromise than a year ago*



Traditional, signature-based antivirus solution(s) provides the protection needed to stop all serious attacks against systems including new and unknown threats



□ FY2017 ■ FY2018 ■ FY2019

* Not a response in FY2017

[See Source](#)

Security Technologies and Their Gaps

Antivirus: What Is It?

Antivirus is a program located at an endpoint on the customer's machine that continuously checks a library of known malware signatures with the goal of identifying suspicious or malicious files, in order to quarantine or destroy them before they can cause damage. As long as the antivirus version is updated by the user and the software vendor keeps their library of malware signatures current, the user's files are reasonably secured.

Antivirus: The Gaps

Cannot keep up with dynamic threats:

Thousands of new file-based malware are created daily and target organizations via email, cloud services such as Dropbox or Slack, third-party APIs, and file transfer or collaboration platforms. While antivirus solutions are the first line of defense in securing known threats, they cannot keep up with the everchanging risk surface that includes undisclosed threats and zero-day exploits.

Not future-proof:

As antivirus solutions safeguard specific machines, they are not particularly suitable for dynamic and fast-moving business environments where access requirements change regularly and cloud-based services are the norm. The frequently required updates and maintenance for all the antivirus installations across the workforce is time consuming and costly.

In fact, global spending on cybersecurity products and services is expected to [exceed \\$1 trillion cumulatively](#) from 2017 to 2021.

Operations may be impacted:

Background processes such as database updates and virus scans can increase latency, causing machine slowdown and affecting user productivity. In addition, according to the Ponemon Institute's [2020 Annual Study](#), current AV solutions return high levels of false positives and alerts. Aside from safe files being blocked unnecessarily, files flagged as malicious may still be opened accidentally by users.

The same report by Ponemon states that **antivirus products missed an average of 60% of attacks**. This has resulted in 56% of respondents indicating that their organizations replaced their antivirus solution in the past two years. Of these respondents, 51% said they kept their traditional antivirus solution but added an extra layer of protection to ensure a higher level of security.



Next-Gen Antivirus: What Is It?

In an attempt to keep up with the dynamic malware environment, antivirus companies have upgraded their solutions with innovative technologies, resulting in “next-gen” AV (NGAV). NGAV takes a more proactive approach to protection by using the power of advanced data science, artificial intelligence (AI), and machine learning, as well as cloud scanning technology, which checks irregularities against a massive cloud database of programs to look for patterns of behavior used by attackers. NGAV utilizes forensic data to analyze the malware infection, enabling the software to learn from these events as time goes on.

Interestingly, according to [Gartner](#), the differences between traditional AV and NGAV solutions are shrinking every year, with traditional AV vendors incorporating many of the NGAV technologies into their solutions.

Next-Gen Antivirus: The Gaps

Too many false positives:

As NGAV software attempts to identify unknown and never-before-seen malware, it commonly returns a high volume of false positives, which can disrupt business productivity and waste users’ time. When NGAV solutions take a blacklisting/whitelisting approach, it can be especially disruptive to IT admins who regularly use scripting languages.

Focus still on detection:

Even with advanced technologies, NGAV solutions still work through mining databases of existing threats, looking for known attack signatures or searching for anomalies in traffic patterns and behavior. With the rise of unknown or zero-day exploits, even NGAV is not sufficient for protecting an organization’s assets.

The bottom line, according to [Minerva Labs](#), is that **86% of exploit kits and 85% of payloads utilize evasive techniques that aren’t being detected by either AV or NGAV security solutions.**



Sandboxing: What Is It?

A sandbox is an isolated testing environment that stands apart from the production environment, where a file or program from untrusted sources can be executed in isolation. The sandbox is designed to ensure that if a program or file is malicious, it will be discovered and blocked without compromising organizational security.

Sandboxing is advantageous to organizations as this technology can be effective against some regular malware, as well as against some zero-day attacks. When security teams catch a zero-day attack on the sandbox, it gives them the opportunity to take action before the hidden vulnerabilities can be executed. Sandboxing may also be useful in stopping advanced persistent threats (APTs) intended to wait patiently on a network with the goal of stealing corporate data over time. With sandboxing, security experts can observe suspicious code before negative consequences occur.

Sandboxing: The Gaps

Bypassing is possible:

Hackers have figured out how to get around the sandbox's protection. Simple Google searches will provide attackers with the information they need to ensure their malware can evade detection within the sandbox – only executing once inside the production environment—or bypass the sandbox altogether.



Common Sandbox Evasion Techniques



Detecting virtualization via Hypervisor, virtualization DLLs, side channels or unusual hardware



Identifying an artificial environment via cookies or browser history, recent file count, screen resolution or by detecting old vulnerabilities



Defeating the monitor by removing or working around hooks or by delaying malware execution



Being context-aware by checking for user interaction, date or time zone, or encrypted payloads



Exploiting Visual Basic for Applications (VBA) macros

Business interruption:

Large file uploads can cause bottlenecks in the sandbox, causing files and messages get stuck in lengthy processing times. This may slow down operational workflow and reduce an organization's efficiency and productivity. Users who expect to receive files quickly must wait for them to exit the sandbox.

Resource intensive:

Maintaining a sandbox requires extensive IT resources, time and money, as well as the need to continuously update complex security policies.

Bottom line:

As detection technologies improve, so do malware techniques.

Gartner suggests:

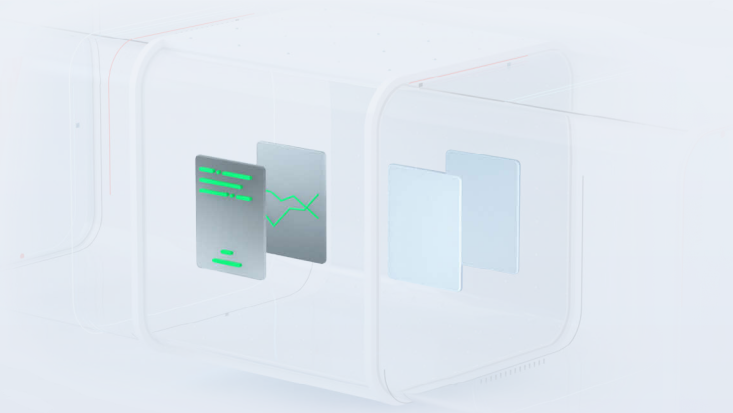
"As malware sandbox evasion techniques improve, the use of content disarm and reconstruction (CDR) at the email gateway as a supplement or alternative to sandboxing will increase."

Content Disarm & Reconstruction

Stopping Threats Other Solutions Can't

Votiro's category-leading Content Disarm & Reconstruction solution, Votiro Cloud, fills in the gaps left by AV, NGAV and sandboxing technologies because it neutralizes external malicious content threats – including undisclosed and zero-day exploits – without impacting file fidelity, file throughput, or creating a lot of false positives. Votiro Cloud technology reconstructs clean, safe versions of incoming files using only the files' vendor-approved objects. This means that all file sections, metadata, and pieces of active content (such as benign macros, scripts, OLE objects, and other elements) are neutralized of any threats. All this is done in micro-seconds, with no interruption to the user, and the reconstructed and sanitized file preserves the integrity and functionality of the original file, combining the highest levels of security and productivity.

Votiro's leading Positive Selection technology protects organizations from cyber-attacks brought on by exploits at all three stages of the vulnerability life cycle.



As opposed to antivirus,

Votiro Cloud is agentless. Each incoming file will be disarmed before entering the organization's network, allowing security experts to manage and maintain one product on the organizational level rather than supporting all of their endpoints individually.

Unlike antivirus,

Positive Selection technology does not rely on a known database of signature threats, and it does not need to whitelist or blacklist files. Every single file is disarmed, neutralizing both known and unknown – including zero-day – threats. As a result, Votiro's Positive Selection technology solutions have never suffered a single breach in seven years, across more than 5 Billion files elements processed and counting

As opposed to sandboxing,

Positive Selection neutralizes your files automatically. The whole Positive Selection process takes less than one second. The process is not visible to your users, doesn't impede your operations, and actually reduces bottlenecks as all files can be opened right away, with no risk.

Unlike sandboxing and many antivirus solutions,

Positive Selection requires no maintenance, meaning your resources can concentrate on more strategic business activities.

How Votiro Cloud's Content Disarm & Reconstruction Technology Works

Step 1

Identify the File Format

Every file must adhere to strict, vendor-based specifications that are unique to that particular file format. Votiro's Positive Selection technology - the most advanced form of Content Disarm & Reconstruction - uses an intelligent fingerprinting technique that identifies a file's content type and format based on file structure and characteristics.

The entire process is invisible to users, does not disrupt business activity — and normally takes less than a second!

Step 2

Generate a New Version of the File

Votiro Cloud then generates a new, clean template of the file and imports over the content from the original file while leaving behind exploits and malicious objects. This regenerated, safe version of the file, based on known good templates from the file vendors, ensures that all the content (including active content and embedded objects) is kept in its original format while preserving file functionality.


Macros, scripts, OLE objects, and all other elements are sanitized and regenerated into the new file as usable elements, neutralizing any exploitation attempts. This process ensures that both user experience and file security remain intact. All files--suspicious or not--are not trusted to be malware-free and therefore go through this process, which takes less than a second and is invisible from the user's point of view.

Step 3

Use the New File

All malicious code and exploit threats are sanitized, and the new file preserves the integrity and functionality of the original file. The file is now safe to save, edit, use, and share.

Key Benefits



**Effective against both known
and unknown threats**




**File cleansing in under
one second**




100% success rate to date



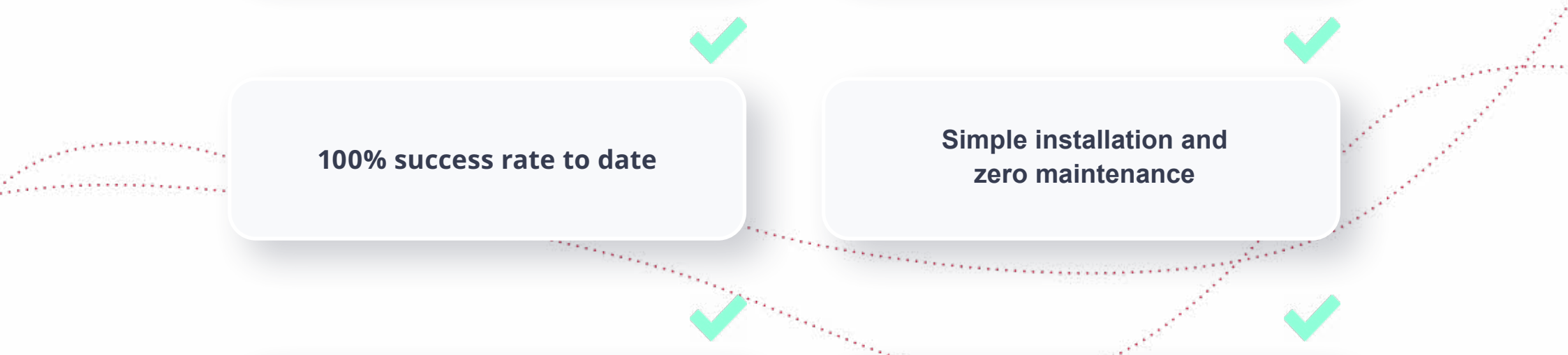
**Simple installation and
zero maintenance**



**Unlimited number of files
neutralized with no bottlenecks**



**All files go through the
sanitization process**



Summary

Traditional security strategies like antivirus solutions and sandboxing are often the first line of cybersecurity defense. However, in order to deal with unknown and zero-day threats lurking in today's dynamic work environment, organizations must become more proactive in plugging the holes left by these traditional solutions. **Votiro Cloud enables organizations to stay ahead of the curve, quickly and effectively cleansing every file, neutralizing threats at the network level, and ensuring that vital and business-critical assets are safe.**

Your Next Step

Sign Up for a Live Demo

See for yourself how easy it is to safeguard your organization with Positive Selection.
[Sign up for a live demo](#) or [contact us today](#).

About **Votiro**

Votiro is an award-winning zero trust content security company serving hundreds of commercial and government organizations, worldwide. Votiro Cloud offers an open, API-centric Content Disarm and Reconstruction (CDR) solution to deliver safe content to your modern digital business processes, content-rich applications, data lakes and eliminate file-borne threats targeting remote workers, supply chain collaborations and B2C digital interactions. Headquartered in the United States, with offices in Australia, Israel, and Singapore, Votiro is trusted by millions of users worldwide to receive content with complete peace of mind. Votiro Cloud is SOC 2 Type II compliant solution and certified by the international standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). To learn more, visit www.votiro.com or contact us at info@votiro.com.

