CYBER

Highlights.

Innovations
Next Gen Dynamic Detection
Next Gen Static Detection
Agile Cloud Deployment

Threat Coverage
APTs
Zero Days/N-Days
Phishing
Malware
Impersonation
BEC

Solution
Advance Collaboration Security (Email, Shared drives, Messaging, CRM*, Any File/URL Exchange) on Windows & MacOS*

Patents
Two patents pending

Architectures
Intel x86 / x64
ARM**

Future**
Web Browsers
Mobile
IoT
Endpoints
Data Centers

*2019 Roadmap
**Potential Applications, Requires R&D

Contact Us

www.vtcyber.pl
info@vtcyber.pl

We're in
Warsaw | Poland

Next Gen Threat Detection Technology.

Any threat. Any channel. Any platform. Agile cloud deployment.
Cutting edge detection built for a digital-first world.

The Urgent Need for Next Gen Threat Detection.

Nearly 90% of enterprises* are pursuing a digital-first strategy as their procceses and interactions become primarily digitized and data-driven. To enable this, IT infrastructures are shifting from a chaos of solutions to perimeter-free, cloud-based architectures. In this environment, potentially malicious communications and data are crossing a multitude of new unsecured entry points.
Cybersecurity built to enable this transformation is critical to success.

* IDG State of Digital Transformation

The Problem.

Legacy security solutions are neither aligned to the modern enterprise nor are they sufficiently effective against today's threat landscape, as they are:

- Reliant on outdated Sandbox and CDR detection technologies that are easily evaded
- Unable to scan 100% of traffic due to speed and scale limitations
- Not providing truly holistic coverage of threats, channels or platforms
- Expensive and complicated to deploy, manage and maintain

This is ultimately a significant barrier to securing digital transformation.

Our Cybersecurity as a Service.

Our proprietary platform provides unprecedented detection and prevention of APTs, phishing, malware, impersonation, BEC attacks and more, delivered with the speed, scale and flexibility of the cloud. Very easily deployed in just a few minutes. POC without any change to the existing environment or processes.

Our core innovations at a glance:

1

Next-Gen Dynamic Detection.

"The Sandbox Killer"
Unique CPU-level visibility see incoming code before it can be masked to stop advanced attacks at the exploit stage, pre-malware.

2

Next-Gen Static Detection.

Anti Evasion Engine
Deep scanning to unpack embedded files & URLs, preventing the utilized evasion technique of malicious content hidden within clean content.

3

Digital-First by Design.

Agile & Unified
Holistic threat coverage.
One-click deployment.
Maximum speed & scale.
Single view across channels & platforms.

* See next pages for further details on each pillar

C Y B E R

Advanced Email Security

Cutting edge threat prevention for the modern enterprise

The Urgent Need For Next Gen Email Security.

The need to communicate and collaborate on a global level has created a proliferation of cloud-based tools for businesses. **Email. Cloud Storage apps. Messaging platforms. Social Networks. CRM.** As many as 20 apps in a single enterprise.

But with new channels come new gaps for hackers, and many new security blind spots. **You need full threat visibility across channels with a solution that works at the speed your company does.**

OUR SOLUTION:

Faster Interception + Holistic Protection.

Our Advanced Email Security combines cutting edge threat prevention with the speed, scale and flexibility of the cloud. We've built in multiple scanning engines and threat intelligence for enhanced protection against attacks like phishing, spam, commodity malware and BEC.
For advanced threats, **we've invented cutting edge technology that combines hardware visibility with software agility** to see what leading solutions miss. Propriety software algorithms x-ray code at the CPU-level to intercept attacks at the earliest stage possible - the exploit - before malware is even delivered.

Our cyber security as a service deploys in a single click, analyzes in seconds and has limitless scale to always scan 100% of your traffic.

Zero Day, N-day, & Everyday Threat Coverage.

Our platform protects your business from the full range of attacks

Everyday Threats	N-day Threats	Zero-day Threats
Signature-based + Payload less attacks	Masked attacks & unpatched software	Unknown vulnerabilities
Spam, Phishing, Commodity Malware, BEC	Exploits leveraging known vulnerabilities. Altered signatures prevents detection.	Exploits leveraging unknown vulnerabilities in Office, Adobe and browsers.

Customer Quote

> *"Integrating Perception Point's platform into our Office365 was quick and seamless with absolutely no impact to our email service levels.* ***In less than a month they've already blocked a potentially damaging attack*** *that could have easily tricked our users and caused a serious disruption. It's rare that I see immediate returns that quickly."*
>
> CISO, Healthcare

Highlights.

Real-time prevention
Block malicious content before it ever reaches the end user.

X-ray visibility
"X-ray" any code executed by the system for 100% visibility into malicious intent.

Deep scanning
Unpack files and follow URLs to detect evasive malicious intent.

Zero delay
In-line engines work in a matter of seconds.

One-click deployment
Easy and fast deployment on the cloud. No change to existing processes.

Unlimited scale
Scan 100% of email traffic, regardless of volume.

Email services
Office 365, Gmail, any cloud email service, Exchange.

Privacy & compliance
SOC2 compliant. No data stored on servers.

24/7 Threat response
Expert intelligence team continuously monitoring incidents.

Contact Us

www.vtcyber.pl
info@vtcyber.pl

We're in
Warsaw | Poland

Advanced Collaboration Security

Holistic threat detection for the digital-first enterprise.

Cloud Collaboration Apps:
A growing security blindspot across the enterprise.

The need to communicate and collaborate on a global level has created a proliferation of cloud-based tools for businesses. **Email. Cloud Storage apps. Messaging platforms. Social Networks. CRM.**
As many as 20 apps in a single enterprise.
But with new channels come new gaps for hackers, and many new security blind spots.
You need full threat visibility across channels with a solution that works at the speed your company does.

OUR SOLUTION:

Agile & Unified Threat Detection For Any Channel.

We stop malicious content (files, URLs & payload-less attacks) from infiltrating your organization via any collaboration channel. Unique CPU-level visibility plus deep scanning capabilities detect the advanced attacks and evasion techniques that easily bypass legacy security technologies. In addition, multi-layered platform combines multiple threat intelligence, image recognition, static and BEC engines to prevent phishing, malware, impersonation and social engineering attacks.

Our service deploys in one-click, has virtually zero scanning delay, and limitless scale – so your employees can collaborate both securely and seamlessly, wherever they are.

Email

G Suite
Exchange
Office 365

Any web-based email service

Cloud Storage

OneDrive
Dropbox
Google Drive
box
SharePoint

Cloud Collaboration

New
Salesforce
zoom
slack
Teams

API

Integration with any other application where files or URLs are exchanged.

Custom development per client needs.

Highlights.

Threat Coverage
APTs
Zero Days/N-Days
Phishing
Malware
Impersonation
BEC

Real-time prevention
Block malicious content before it ever reaches the end user.

X-ray visibility
CPU-level visibility sees code before it can be masked.

Deep scanning
Unpacks and follows URLs to detect evasive malicious intent.

One-click deployment
Easy and fast deployment on the cloud. No change to existing processes.

Unlimited scale
Scan 100% of content, regardless of volume.

Zero Delay
In-line engines work in seconds.

Contact Us

www.vtcyber.pl
info@vtcyber.pl

We're in
Warsaw | Poland

Free 30-day trial

Set-up a trial in less than an hour, with no interference or disturbance to the end user or organization.
No content will be stored and all data is encrypted.

Advanced Cloud Storage Security

Cutting-edge threat prevention for the collaboration-driven enterprise.

Cloud Storage:
A Growing Security Blindspot.

Cloud-based file sharing apps are an essential productivity tool for the modern enterprise. They allow for simple and easy collaboration, no matter where people are working from. However, they also pose a new cybersecurity risk. Given their growing usage, they pose an attractive target for hackers, yet aren't nearly as protected as more traditional vectors like email, endpoints and networks.

Cloud Storage apps can be highly effective malware distribution platforms, whether the malicious content is coming from another channel open to the outside (like email), an insider threat, or an unmanaged endpoint from a third party. Once malicious content is on the file sharing service, it can easily travel to any unsuspecting user with access.

It is not enough to just secure the data in collaboration channels, you have to ensure that the content inside these channels is clean and safe.

OUR SOLUTION:

Any threat. Any file. Any URL. Any cloud storage.

VT Cyber Advanced Cloud Storage Security, delivers the same robust prevention typically only available for email. Cutting-edge cloud solution **prevents malicious content (files & URLs) from being uploaded, downloaded or utilized to infect previously clean files.** Unique CPU-level visibility plus deep scanning capabilities detect the unknown attacks like zero days and n-days, pre-malware release. Multi-layered technology combines multiple threat intelligence, image recognition and static engines to prevent phishing and commodity malware.

Our service deploys in one-click, has virtually zero scanning delay, and limitless scale – so your employees can collaborate both securely and seamlessly, wherever they are.

Key Features

- Real-time prevention for OneDrive, SharePoint, Dropbox, Google Drive and Box.
- Run-time scan and detection of all files uploaded to the file sharing service.
- Pre-scan ("hunting") and detection of all historical files.
- Ability to define scan policy and extend existing Security policy
- Ability to define quarantine policy.
- Forensics of all file scans using the same tools used for email.

Highlights.

Real-time prevention
Block malicious content before it ever reaches the end user.

X-ray visibility
"X-ray" any code executed by the system for 100% visibility into malicious intent.

Deep scanning
Unpacksfiles to detect evasive malicious intent.

One-click deployment
Easy and fast deployment on the cloud. No change to existing processes.

Unlimited scale
Scan 100% of content, regardless of volume.

Supported services
OneDrive, SharePoint, Dropbox, Google Drive, and Box.

Privacy & Compliance
SOC-2 compliant. No data stored on servers.

24/7 Threat Response
Expert intelligence team continuously monitoring incidents.

Contact Us

www.vtcyber.pl
info@vtcyber.pl

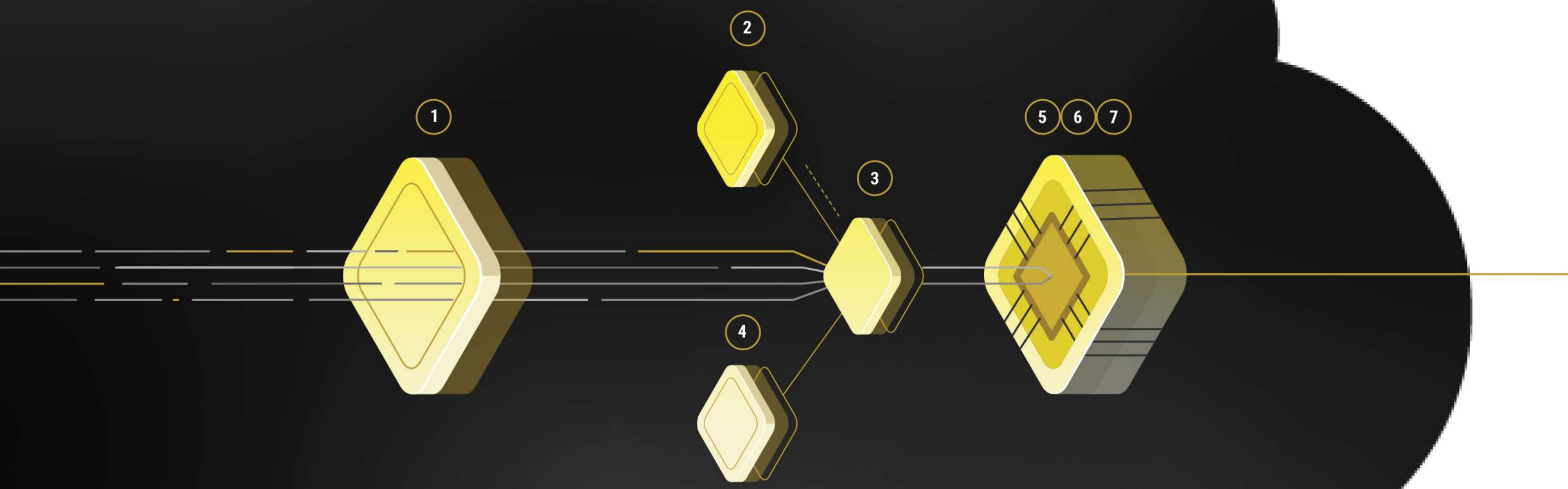
We're in
Warsaw | Poland

Free 30-day trial

Set-up a trial in less than an hour, with no interference or disturbance to the end user or organization.
No content will be stored and all data is encrypted.

Inherent Layered Solution

Enhanced standard layers + cutting-edge APT protection for the most high-performance defense on the market.



Everyday Threats | Phishing, Malware, Impersonation, BEC, etc.

1

Recursive Unpacker.

Unpacks the file into smaller units to identify hidden malicious attacks. All of the extracted components go separately through the next layers.

2

Threat Intelligence.

Combines multiple threat intelligence sources with our internally devloped engine that scans URLs and files in the wild to warn about potential or current attacks.

3

Phishing Engines.

Combines best-in-class URL reputation engines and an in-house image analysis engine to identify impersonation techniques and phishing attacks.

4

Static Signatures.

Combines best-in-class signature based anti-virus engines to identify malicious attacks. In addition, we've developed a tool that acts to identify highly complicated signatures.

N-DAY/ ZERO-DAY THREATS

First Hardware-Assisted Platform (HAP™)

Unique CPU-level technology acts earlier in the kill chain than any other solution. Blocking attacks at the exploit phase - pre-malware release - for true APT prevention.

5

HAP™ (Dropper).

Employs advanced heuristics-based engine for detecting logical bugs and handling macros and scripts.

6

HAP™ (CFG).

Records the CPU while it processes the input (files and URLs) and identifies exploits by examining the entire execution flow - detecting any deviation from the normal flow of a program in order to deterministically identify malicious activity.

7

HAP™ (FFG).

Detects advanced techniques such as exploits that are written to bypass common CFI algorithms. Proprietary semantic aware control flow graphs developed for each application identify deviations of the execution flow during runtime.

Protect multiple channels with our full Advanced Collaboration Security platform.
Email, Messaging, Cloud storage, CRM + API for any content-exchange channel

CYBER