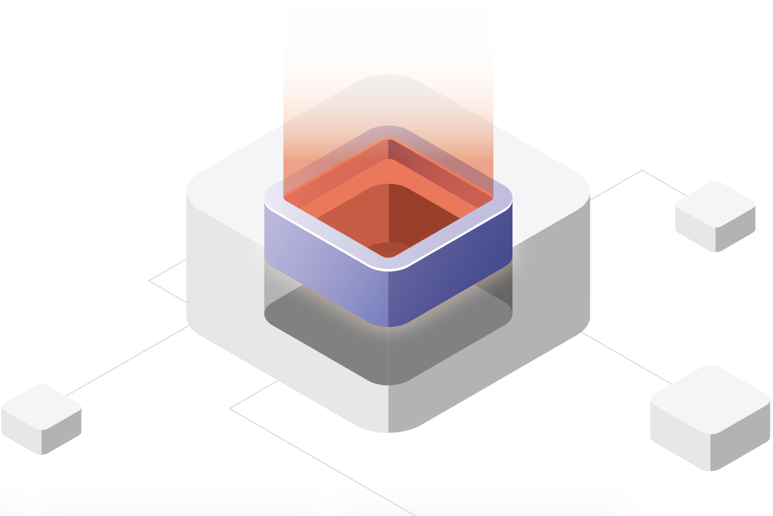
PERCEPTION
POINT

Perception Point Fusion™

Transform your existing security stack with the combined power of next gen dynamic, static and anti-evasion detection.
Leverage to prevent the most advanced attacks of today and tomorrow.

Patented SANDBOX KILLER Technology
Lightening Fast Scans. Unlimited Scale. Deep Forensics.



PLUG & PLAY DEPLOYMENT:

Upgrade your Existing Platform in No Time.

Unique architecture allows quick and simple deployment to any security stack. Partners can easily decide where and how to deploy Perception Point Fusion™ in their security stack without affecting existing layers.

Sample Applications:

Network

Unlimited scale to scan 100% of files passing through the network.

Firewall

Stop malicious traffic at the firewall based on scans instead of rules.

CASB

Fortify a CASB with advanced threat detection and forensics for any cloud app.

Web Gateway

Ultra fast scanning times eliminate URL scanning latency.

Deteriorating Detection: A Rapidly Growing Challenge

It's common knowledge that not only are cyberattacks becoming more sophisticated, they are increasingly successful at evading mainstream security stacks. Despite the layering of multiple AVs, threat intelligence and sandboxes, declining detection rates are widespread and rising false positives are increasing business disruption.

The weakest links in any legacy security stack are the fact that not all content is dynamically scanned (due to cost and speed issues), the inability to detect deeply embedded attacks, and the diminishing efficacy of statistics-based technology. Moreover, non-cloud native deployments prevent systems from responding to evolving threats. However, with hundreds of millions of dollars already invested in current technologies, the prospect of replacing them with entirely new, internally developed systems presents crippling process and profit challenges.

OUR SOLUTION:

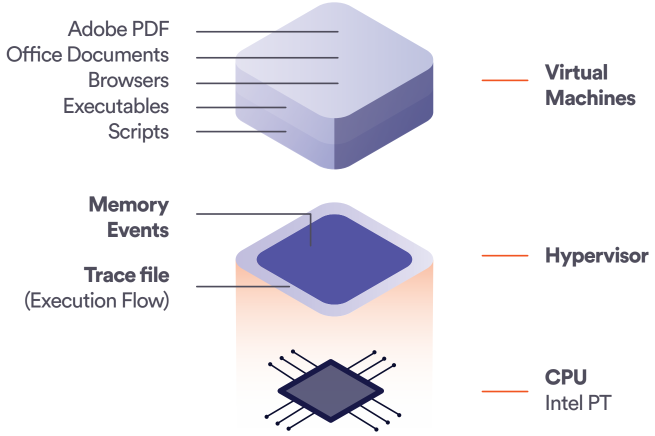
Next Gen Dynamic + Static + Anti-Evasion Detection

Perception Point Fusion™ dramatically boosts the detection rate, user experience, speed and scale of your existing security stack, without requiring extensive R&D processes or investments. It consists of three core capabilities:

1

Dynamic Detection (aka the Sandbox Killer)

Cloud-native anti-exploitation technology dynamically scans 100% of content to deliver unprecedented detection of unknown attacks (Zero-days, N-days, APTs). Leveraging Intel PT (Processor Trace), Perception Point Fusion™ enables visibility to data in the hardware level within a SaaS solution - monitoring, observing, and recording every single executed command performed by CPU to detect the highly-evasive attacks that sandboxes and other solutions simply cannot see. Agile cloud deployment ensures 100% of content is dynamically scanned without cost or scale limitations.

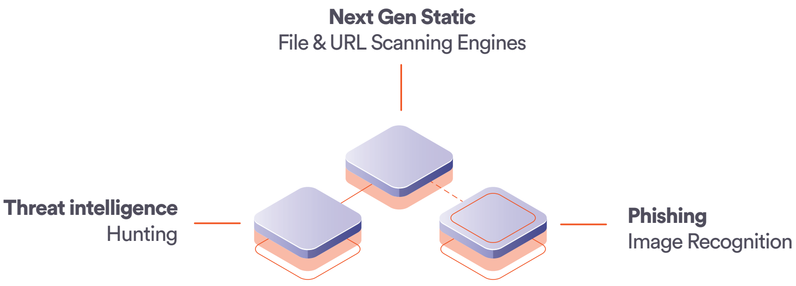


2

Static Detection

In-house built algorithms enhance best-in-class engines of leading security vendors to provide 360-degree coverage against URL, file and text-based attacks. Selected enhancements include:

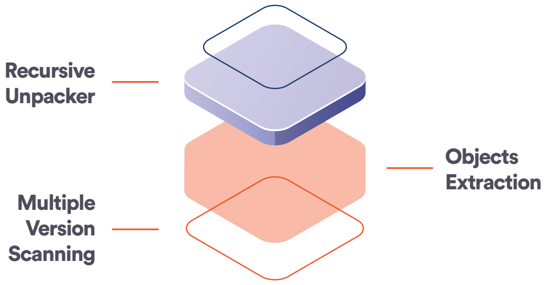
- **Ongoing threat intelligence source:** automatic cross referencing of incidents between customers in addition to an internally developed "hunting" tool scans potential threats in the wild.
- **Anti-phishing:** image–recognition engine actively scans URLs to prevent zero-day phishing attacks and highly concealed known phishing attempts.
- **Bulk Detection:** Grouping of emails based on machine learning and AI identifies malicious campaigns.



3

Anti-evasion

Proprietary technology prevents commonly used evasion techniques by conducting deep content inspection to uncover embedded attacks up to several layers, in less than a second. Once the attack is unpacked, each individual file, URL text or even smaller objects within the content, can be scanned separately. In addition, unique algorithms run the same files and URLs in multiple versions and patterns to make sure the attack is not leveraging unseen evasion techniques.



Advanced techniques Perception Point Fusion™ is uniquely able to prevent include:

All known exploitation techniques, including Return Oriented Programming (ROP), Call Oriented Programming (COP), Jump Oriented Programming (JOP), and Counterfeit Object-Oriented Programming (COOP)

Attacks concealed by embedding the malicious payload in other pieces of content (e.g. phishing link within a file or a link to cloud storage platform)

Spear-phishing + whaling: highly targeted impersonation attacks that leverage a known brand to cause unsuspecting users to execute their malicious payload

Advanced evasion techniques, such as environment detection (specific artificial objects) and user behavior (real user vs. artificial environment)

"Sleepers": an internal stalling mechanism that delays the actual run of the malware for several minutes

Fileless malware (tools that abuse tools built-in to the operating system) and code injection attacks

Key Advantages

Rapid Deployment

Designed to complement existing security infrastructure by delivering advanced detection capabilities and threat intelligence to existing security products, processes, and workflows.

Continuous Augmentation

Native cloud deployment enables the system to be augmented on a daily basis to evolve with the threat landscape and deliver new capabilities to customers.

Lightning Fast

Deep analysis is concluded in a matter of seconds – up to a maximum of 30 seconds – to ensure no delay in verdict delivery.

Unlimited Scale

Native cloud architecture combined with rapid scans ensure the ability to scan 100% of content, 100% of the time.

Deep Forensics

In-depth analysis of all incidents, including file & URL classifications, attack types, attack paths, and full mapping of most targets attacks.

Near-zero FP rate

Deterministic approach dramatically reduces the false positive rate.

Market Validation

#1 in Independent Detection Testing

Gartner

Gartner Recognized Security Vendor

Strategic OEM Partnerships

Boost your security offering with Perception Point Fusion™.
Superior detection. Seamless integration.

PERCEPTION POINT