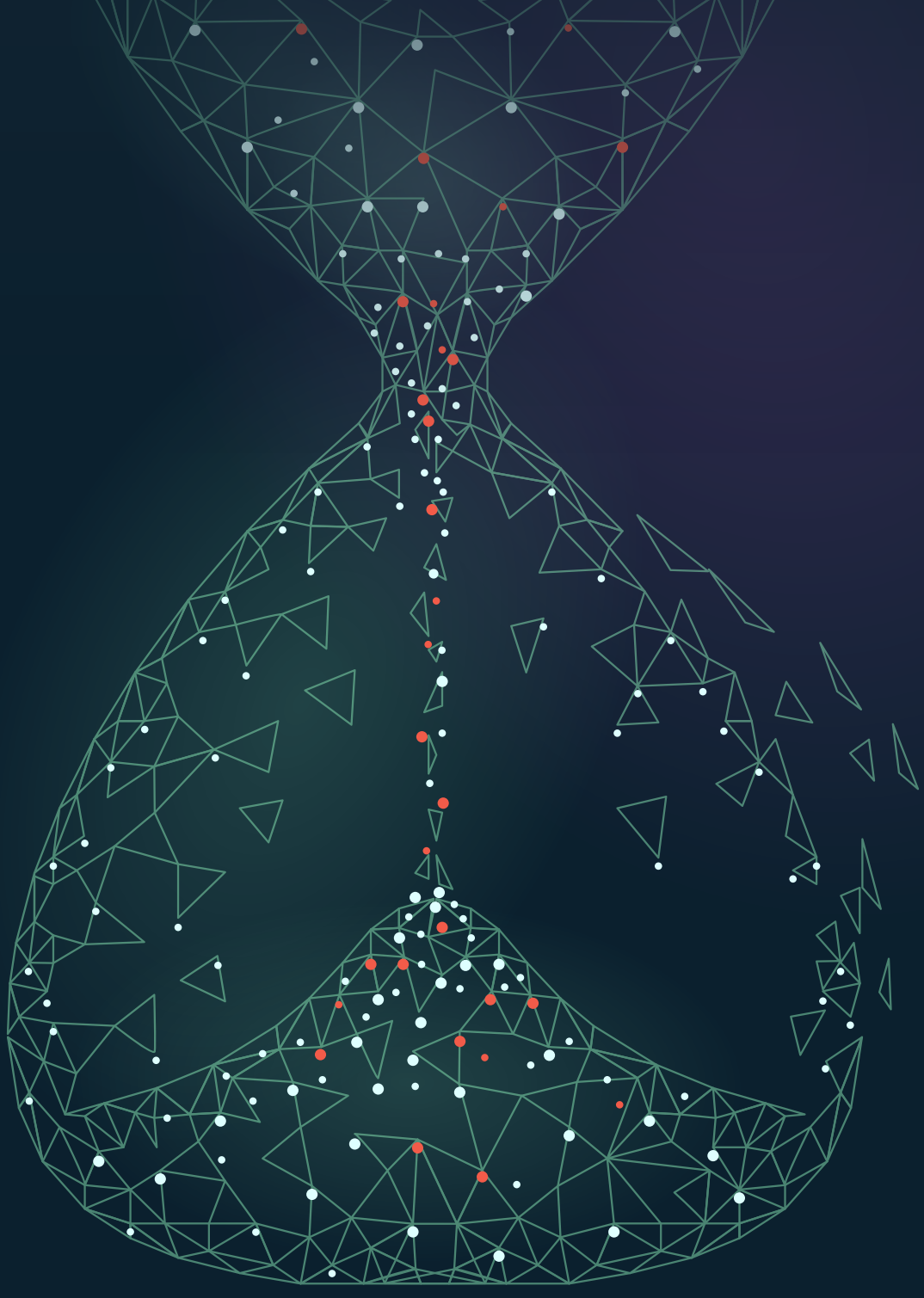
Cyberint

YOUR CYBERSECURITY DEBT AND THE COST OF DOING NOTHING



> **Left unchecked, technical debt will ensure that the only work that gets done is unplanned work!**
>
> - Gene Kim

One of the primary causes of cybersecurity debt, which is in fact, tech debt for a company is the neglect or delay in modernization:

When organizations fail to upgrade their aging technologies, devices, software, and defenses. Those companies accumulate debt because legacy software and tools may not be capable of meeting modern speed and performance expectations, complying with regulatory requirements, and may be vulnerable to various exploits. Given that outdated technology is inevitable, businesses need to include Cybersecurity debt considerations in their budgets.

Status quo is the silent killer of innovation, especially in cybersecurity. Especially in times of digital transformation.

In the wise words of the late Colin Powell: "If it ain't broke, don't fix it" is the slogan of the complacent, the arrogant or the scared. It's an excuse for inaction, a call to non-arms. It's a mindset that assumes (or hopes) that today's realities will continue tomorrow in a tidy, linear and predictable fashion."

The reality is that when it comes to cybersecurity,

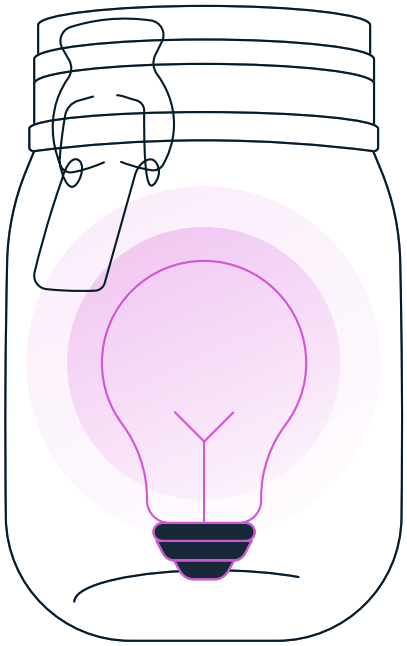
You can't afford the cost of doing nothing

Here's why:

Change is not just something you put in a jar

In today's business environments, change is the only constant. Currently, digital transformation is a driving force behind this change. As new external threats are emerging, new technologies are introduced. New logos compete on new Gartner quadrants. A seasoned team should know when to take the right action and embrace a new technology.

We'll show you how converging threat intelligence, external attack surface management, digital risk protection, supply chain intelligence and vulnerability intelligence technologies will impact the future of your budget, people, and your cybersecurity debt. Then, we'll demonstrate the ROI of turning into an impactful intelligence driven enterprise.



Here's what you probably know:

New pressure/more pressure will be placed on your organization, eroding your budget and your team in the constant battle to stay ahead of the threat curve.

Challenges your peers are facing:

Digital footprint only expands - and so does your cybersecurity debt

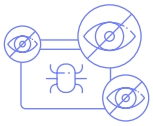
More users, more servers, more cloud instances. Misconfigurations that lead to vulnerabilities are not a matter of "if" anymore, but a matter of "when". Threats are growing in number and sophistication. Gen Z, the largest generation on the planet, is entering into cybercrime. Cybercrime-as-a-Service (CaaS) makes it easy to launch attacks with minimum knowledge and bring corporations to their knees.

Good help is hard to find

In 2022, the global cyber workforce gap increased by 26.2% compared to 2021. There are more than 3.4 million open positions that need to be filled. More and more cybersecurity teams are finding themselves understaffed and overworked - which increases the chances of human error, the source for 13% of all breaches in cloud environments.

Going on a "vendor-bender" takes its toll

Enterprises use on average 45 different cybersecurity products. Combined with dozens and even hundreds of other systems such as ticketing and communications, the number of potential integration breaking points is staggering. Some sources cite the average time technicians spend on integration issues is up to 50% - it's a huge productivity killer for cybersecurity and IT teams that drains tens of thousands of dollars from your cybersecurity budget.



Too many false-positives

False positives can happen due to various reasons, such as incorrect configuration of the security system or outdated threat intelligence. False positives can have significant implications for cybersecurity work, including wasted resources, alert fatigue, reduced credibility, compliance issues, and disruptions to business operations. It is important to manage false positives effectively to avoid these negative impacts and ensure security systems are functioning optimally.

Too many Blind spots

Lacking visibility into your external attack surface can have a significant impact on your organization's security posture. It increases the risk of security breaches and makes it difficult to identify security gaps, and to track and investigate incidents. It makes complying with regulations challenging, and consequently, increases operational costs. Proper visibility into systems and networks is crucial to effectively detect and respond to security threats.

Which correlates with the two cyber challenges every CISO faces:

Time & Cyber Security Posture

Time

As a cybersecurity leader you have to make sure your team/s are using their time in the most efficient way. Removing "time-suckers" such as false-positives and time wasted on integration related issues can have a dramatic effect on your bottom line.

Time, within the context of performance, is primarily measured in "Full Time Equivalents'' (FTEs). Other "time" metrics are:

- Mean time to detect
- Mean time to remediation

Cyber posture

Defined by NIST as "The security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes."

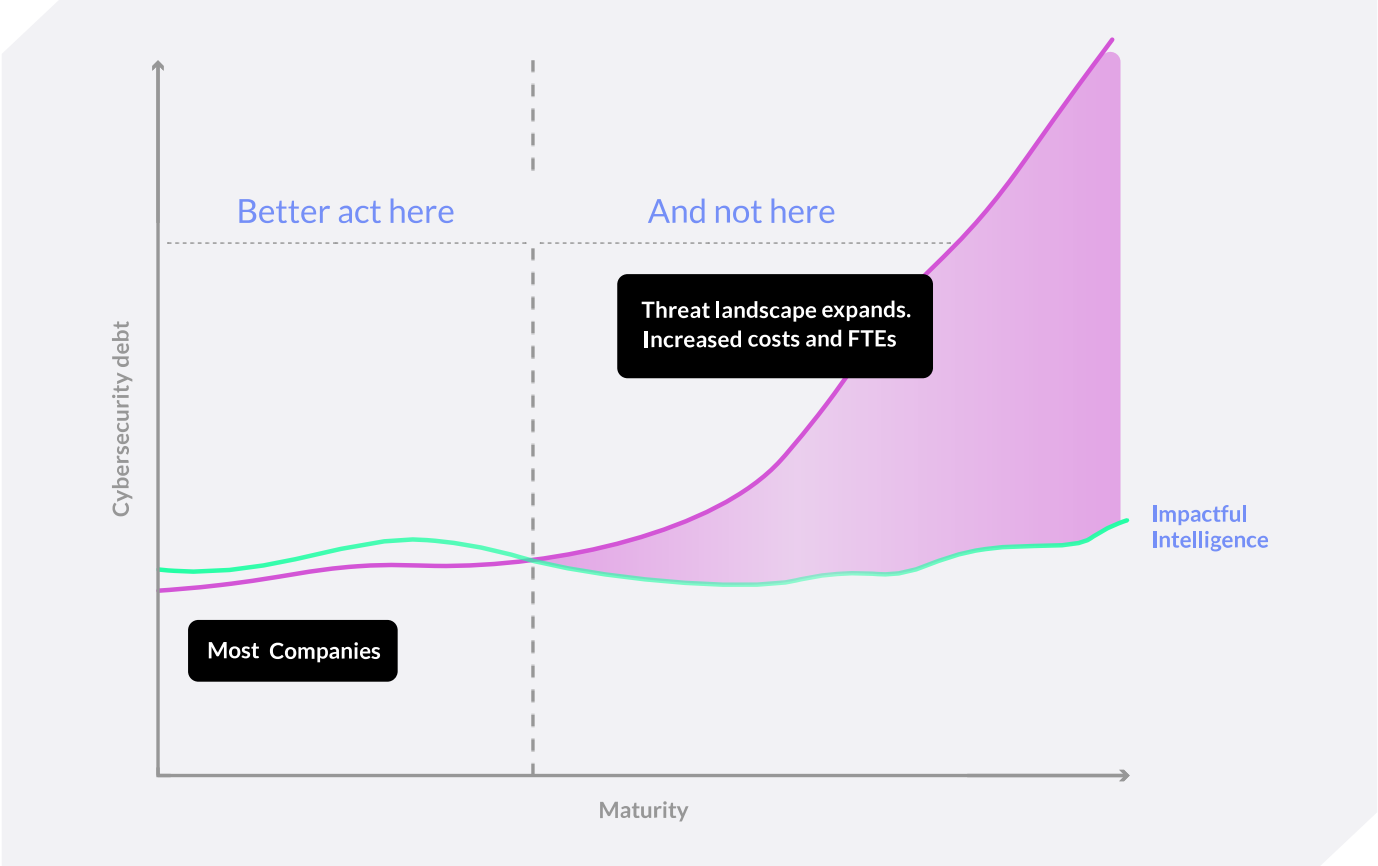
Cybersecurity posture primarily manifests in risk reduction, business outage savings, and minimized impact exposure KPIs such as:

- # cyber-related loss events
- Incident response costs
- Fines & penalties
- FTE hrs recovered due to less/shorter events
- Productivity gains from other affected business units.

› Learn more about Cyber KPIs and ROI on page 10

As a company's cybersecurity program matures, risk goes up. Companies going on a vendor bender will exponentially increase their debt.

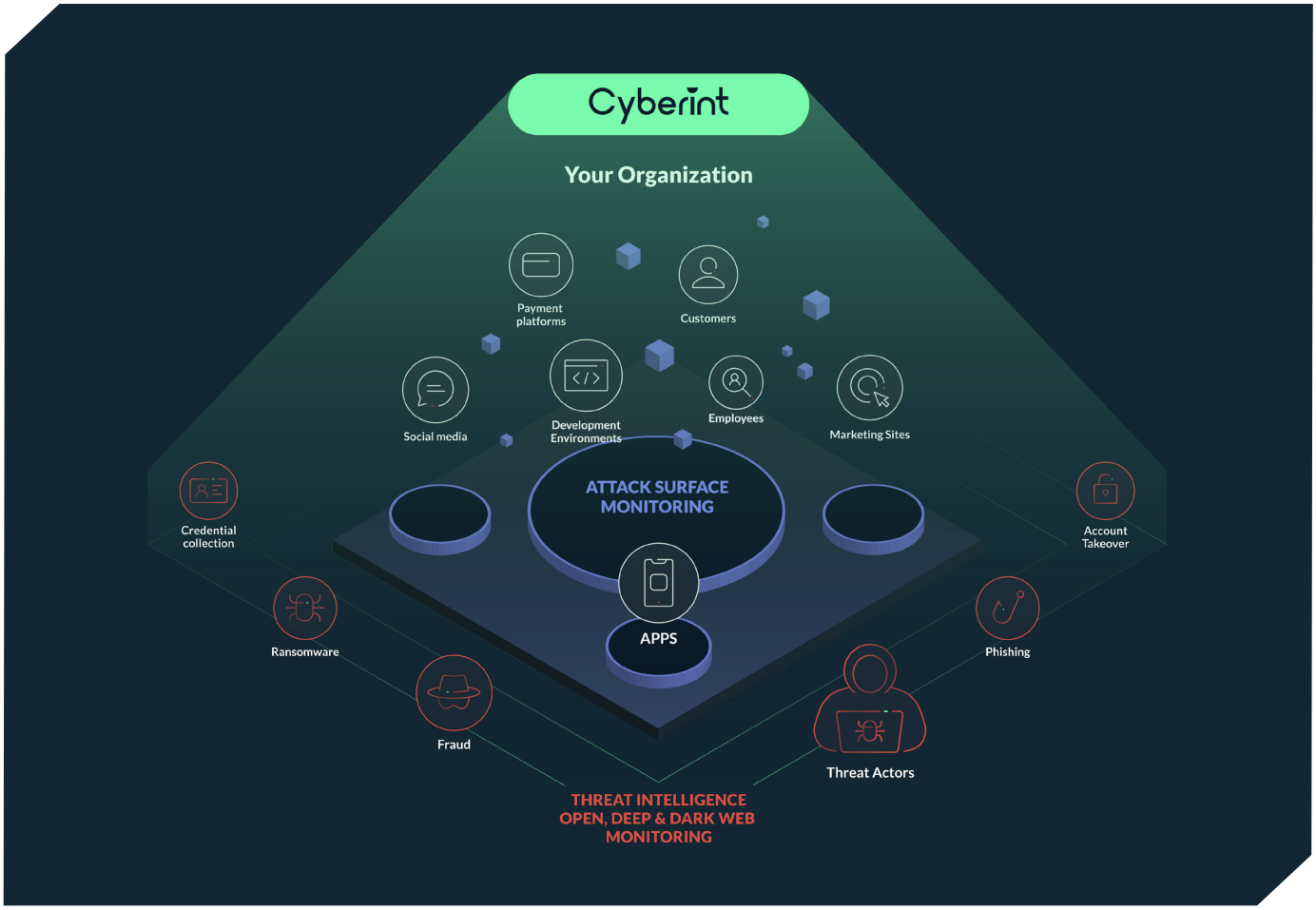
Increased visibility + more threats + expanding attack surface = more tools needed and more labor hours needed for integration related issues (a.k.a cybersecurity debt)



Most companies are on the left half of the graph, having either a one point solution (TI or EASM), or both. Maybe some are open-source solutions and/ or open source feeds, as well as a vulnerability management solution of some sort. At this stage, labor and product costs might consume a big chunk of your budget but you might feel it's manageable.

However as your organization grows so does its digital footprint and, as a result, your attack surface. More resources means bigger chances for misconfigurations and vulnerabilities. The vendor bender continues which means it consumes more resources. Growing cybersecurity debt (the purple area in the graph) means you'll need more staffing, time, and budget to accommodate evaluation, integration, and operation of additional solutions.

By converging threat intelligence, attack surface management, and digital risk protection, coupled with expert service you are eliminating future cybersecurity debt and maximizing the impact of your programs.



Cyberint's Argos is a platform that converges digital risk protection, threat intelligence, and attack surface management functionalities into a unified service, providing organizations with extensive visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, it allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier on the cyber killchain.

Gartner

Cyberint is listed in the Gartner Hype Cycle for Security Operations, 2022 in three different categories. Cyberint is also listed in Gartner's Emerging Tech Impact Radar: Security, and Emerging Tech: Adoption Growth Insights in Digital Risk Protection Services Reports.

> Learn more

What does the outcome look like on each aspect of the business?

	Primary Benefit	Operational KPIs	Business KPIs
SecOps efficiency gains	Improved speed, scope, & productivity of SecOps & analysts	Events investigated Relevant events reviewed Mean-time-to-detect (MTTD)	Current FTE hrs recovered New/future FTE hrs averted
Risk reduction	Lower probability of successful cyber events	Triggered security incidents Audit Findings and reviews Account resets or escalations	Cyber-related loss events Fines & penalties (number & size) Incident response costs
Minimized impact exposure	Reduction in the consequences & costs of successful cyber events	MTTR Internal (proxies, gateways, firewalls, etc.) MTTR External (takedowns, data recovery) Account resets (Size & scope)	Losses due to cyber events Fines & penalties (number &size) Incident response costs
Optimized security stack	Improved security technology & data from TI integrations	IOCs proactively blocked by NGFW, mail gateway, or EDR Enriched SIEM data & analytics	FTE hrs recovered Costs saved from other technology investments
Business outage savings	Improved user productivity from fewer cyber-related outages	Cyber-related events causing business disruption Scope duration of business disruptions from remaining events	FTE hrs recovered due to fewer and shorter events Productivity gains from other affected business units
Domain-specific benefits	Additional ROI from specific use-cases	Time to detect insider threats Relevant & TI prioritized CVEs	Protected asset value-at-risk (VARs) Vulnerability management efficiency gains
All-in-one ETI solution advantages	Advantages of a unified external threat intelligence product suite	Threat data quality from data processing and enrichment Seamless investigations, threat hunting and pivoting	FTE productivity gains, improved dashboard fatigue Bundle savings, two TI tools in one solution suite Shortened payback period

The economic impact of eliminating vendor-bender with Cyberint

364%
ROI OVER 3 YEARS

3 months
Investment repayment period

12.5%
Total risk-adjusted security budget savings

15%
Expected annual reduction in managed incidents

30%
Reduction in security operational time due to fewer wasteful and low-impact false positive reviews

$1,750,000
Cost-effectiveness of approximately

Want to learn more?

› Download eBook

Further Cyberint Publications

4 key considerations
before renewing your DRP Service

> Download

Raising the Stakes for Attack Surface Management

> Download

Info Stealers Overview

> Download

About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats

> Get started

Recognized by the industry's most respected analysts

Gartner