WHITE PAPER

THIRD-PARTY CYBER DEFENSE

How Prevailion is Charting a New Course for Businesses

PREVAILION

THE WEAKNESS IN MODERN CYBER DEFENSES

Most of today's businesses are beholden to a fundamental weakness—lack of visibility. As businesses grow larger, their vast third-party vulnerabilities unfurl themselves, exposing the business to huge risks they aren't even aware of.

This weakness grew out of what started as a strength. Successful businesses have expanded their reach by co-opting the specialties of external organizations. This expansion has made the network perimeter of the average business almost ephemeral.

> 80% of organizations rank cyber risk as a Top 5 concern, yet only 11% had confidence in their ability to assess cyber threats, prevent attacks, and respond effectively.
>
> Source: 2019 Marsh Microsoft Global Cyber Risk Perception Survey

---

Consider all the connections a modern business shares — from manufacturers, vendors, and customers to partners and outsourced specialists. Offloading those aspects of business is efficient, but the strategy comes with an often ignored cost: *Their* perimeter becomes *your* perimeter. This makes attacking you much, much easier, and defending your territory much, *much* harder. Your weakest link becomes the vector of infection, allowing threat actors to get inside your network and begin exfiltrating your data without you even knowing.

A survey of existing network security solutions shows a few common techniques in the market, all of which have their faults when pitted against sophisticated threats:

CASTLE AND MOAT DEFENSES — The concept of protecting your territory with a figurative thick wall and a deep moat around it has effectively failed modern organizations. It has left them open to attacks across the bow of their vast third-party connections.

INDICATORS OF COMPROMISE — Businesses today are inundated with tools that feed their analysts *thousands* of false positives each day, leaving them paralyzed over how they should defend themselves. Even in the information age, too much can be a bad thing.

CYBER RISK SCORING — A number of other solutions, such as risk scores and cybersecurity assessments, have emerged to offer an aggregated sense of security to organizations. But cyber risk scores are critically flawed.
Consider:

1. They provide only a data snapshot, locked in the time of its capture
2. They indicate potential, not actual compromise
3. They provide no context of the associated threat actor campaign
4. They can be slow and intrusive
5. They are not standardized

WHAT MAKES PREVAILION DIFFERENT?

Cybersecurity defenses have not evolved at pace with the resourcefulness of threat actors. They provide poor visibility into an organization's true network surface area, and they inundate organizations with thousands of false positives each day. This is a lethal cocktail.

"Armed with intelligence like this, customers can take action in a much more effective way"

For modern organizations to thrive today, they need visibility on all the possible nodes of access through their third-party networks, and they need a way to prioritize evidence over indicators of compromise—continuously.

Prevailion proposes a new paradigm for security. Instead of living cloistered within a defensive apparatus, surrounded by expensive endpoint solutions, we propose an *offensive* tactic.

Let's start looking at the adversaries' efforts, and understand where they are, and how they're building infrastructure to collect the payloads harvested by these victims. In doing so, we're able to then attribute further, and ultimately instill some concern and fear in the adversary, to the extent that they may begin limiting their range of attacks.

Right now, threat actors are quite cavalier. They have no reason to stop what they're doing, because they're anonymized, their attacks are scalable, and it's cost-effective. We believe that if we can put a dent in their sphere of influence with a new approach to compromise visibility, we can put the power back into the hands of their victims, changing the dynamic overnight.

By definition, that is exactly what **Compromise Intelligence** is. It is information captured from the adversary's own achievements, and details where they are, how they're doing it, along with the cadence and the velocity of that compromise. Armed with intelligence like this, customers can take action in a much more effective way than with traditional security solutions.

Compromise Intelligence gives businesses a method not only to continuously monitor their third-party connections, but view the history of compromises in an organization, and wield pre-emptive knowledge of compromise campaigns as they tear through global industries.

EVOLVING FROM THREAT INTELLIGENCE TO COMPROMISE INTELLIGENCE

Most everyone at this point has become familiar with threat intelligence in some regard. Threat intel has become a broad category that probably everyone consumes in one fashion or another.

The problem is that threat intelligence creates a massive amount of noise for analysts who are simply looking for solid optics on compromises in and around their networks. Successfully executing threat intelligence is also a daunting, invasive procedure for any organization.

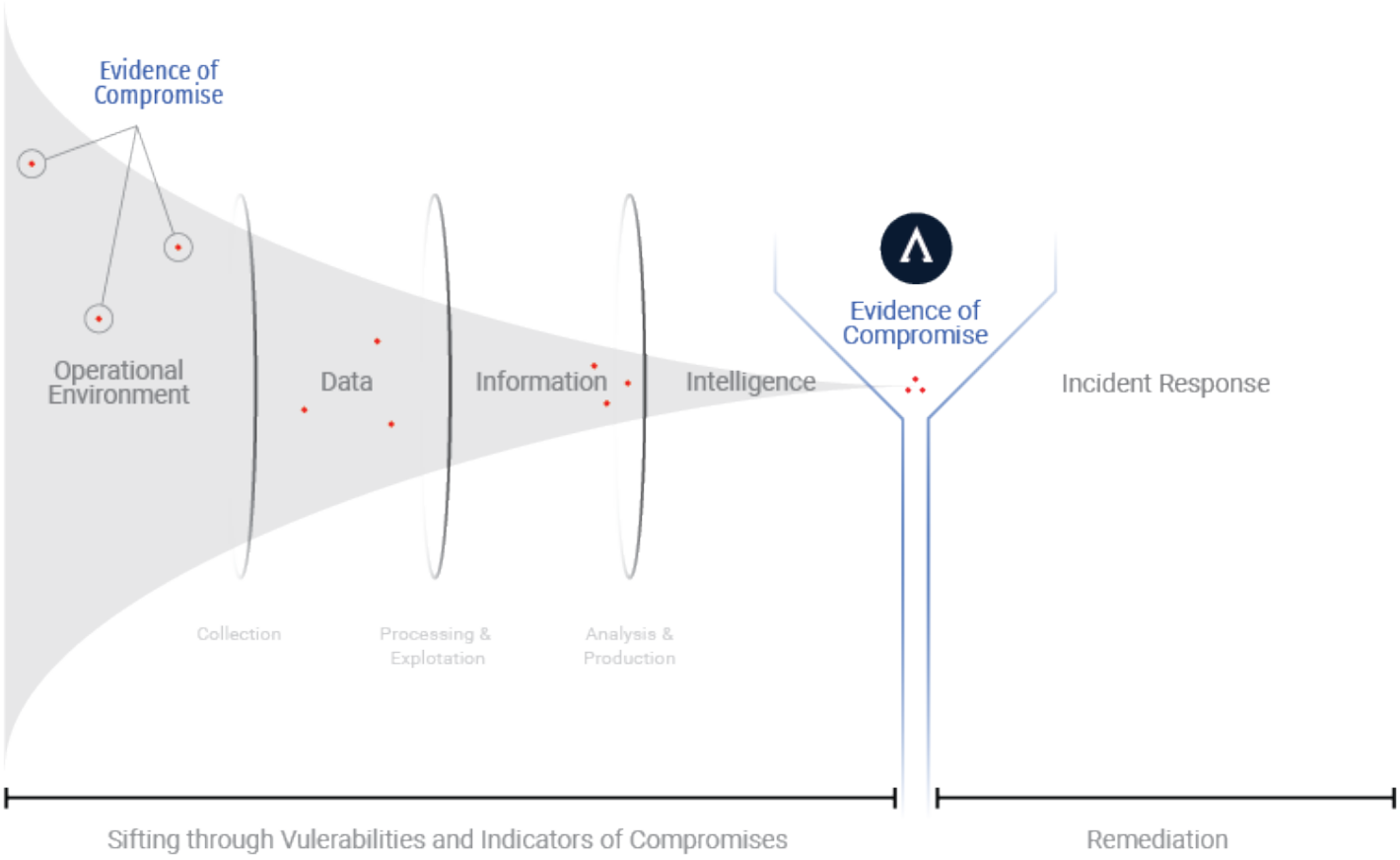
"You are empowered to continuously monitor the compromise status of your network and beyond"

A basic prerequisite is ingesting all network traffic so that anomalies can be analyzed in real-time and compared with known threats. It picks through everything it encounters and places its findings into different piles for further analysis. Eventually, those piles accumulate into a mountain where there is no way you can build a team large enough to actually parse it. That is a real problem that many organizations face on a daily basis.

Compromise Intelligence gives organizations a way to highlight only the known signal of compromise from all of that traffic, without having to ingest everything. Prevailion takes a further step in what it concludes to be evidence of compromise by scrubbing away false positives. Was this a security researcher detonating malware for educational purposes? Was this a sandbox? Those are confirmed to be false and so they are removed as active compromises.

Our Apex Platform enables customers to see the true scope of global victims through the target lenses of the adversaries themselves. We capture all of the victimology associated with those efforts, clean it, and report it on our platform.

When a tool or malware is deployed by an adversary, it beacons back home—its command and control center. That's where we're sitting to effectively collect all of the victimology associated with that attack. This method of approach to victimology is the exact opposite of how other solutions gather their intel.

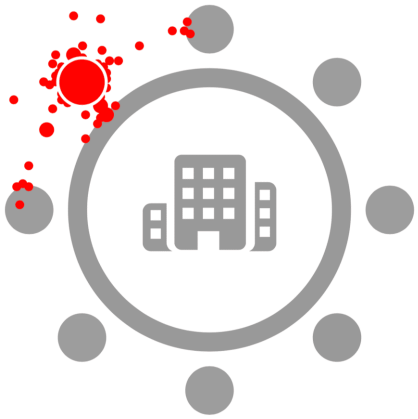


By approaching the compromise at its endpoint through the command-and-control context, it is a step beyond an indicator of compromise—it is evidence. You can actually run with confidence with this and actually pursue it, armed with context that helps your organization prioritize where to defend, what to defend, when it occurred, and how severe the situation is. You can diagnose the threat to your organization and strike first with actionable intelligence.

You are empowered to continuously monitor the compromise status of your network and beyond — your current and prospective partners, competitors, and the world at large.

USE CASE:
Risk Management < Compromise Management

Compromise intelligence empowers organizations to move from a risk management approach to compromise management, putting them one step ahead of the adversaries. Suddenly, you can see the industry you operate in being targeted, with compromises dotting the map throughout organizations surrounding your own. This visibility gives your organization an opportunity to manage the compromise before it manifests as a breach in your network.



Envision your organization and the networks you regularly touch. Around you are your third-, fourth-, fifth- party connections. You're seeing the partners of your partners, along with your partners. Perched at this scale of visibility, you can see an impending compromise as it moves laterally through your distant partner ecosystem. And unlike some of your partners who are currently in the crosshairs—you're aware of the trajectory of the enemy's next attack.

USE CASE:
Vetting Vendors and Future Partners

The power of this visibility can also augment standard investigative methods. Before you ingest a new partner into your organization's ecosystem, you can discover how their compromise level looks—not just at this exact moment, but dating back six months. Do their security standards meet your own? Or has a compromise lingered unchecked for months?

Performing this health check will either give you confirmation about whether you are dealing with a best-in-class organization, or a plague ship headed for your port.

One of Prevailion's customers is a utility — **SouthEastern Illinois Electric Cooperative, Inc.** — that leverages our platform for vendor vetting. If a vendor is found to be laden with compromise, the utility has the opportunity to pivot away and guard itself from impending danger, or lock down connections with existing vendors.

SEIEC's IT Director **Matt Ohmes** said Prevailion is a valuable tool for his organization to help verify whether a vendor is serious about security before it awards costly projects. If a vendor is found to be compromised, Ohmes can take that information to his CEO and the board to evaluate that relationship.

"Prevailion has given me some assurance. My vendors were green and stable — that gave me a sigh of relief, because you never know what you're going to find."

—Matt Ohmes, IT Director, SEIEC

Prevailion empowers Ohmes and his organization to:

- Vet a vendor ahead of awarding them expensive projects
- Monitor existing third-party vendors and identify active contagion
- Act on that evidence by limiting a vendor's access to a network
- Share compromise information with leadership to make informed partner choices

ADDITIONAL USE CASES:

Third-Party Management

Learn the history behind a partner's past and acrive compromises before they become your own.

Investment Decision Support

Get an edge during due diligence, and use pre-cognitive knowledge of an active compromise to make key decisions—fast.

Mergers & Acquisitions

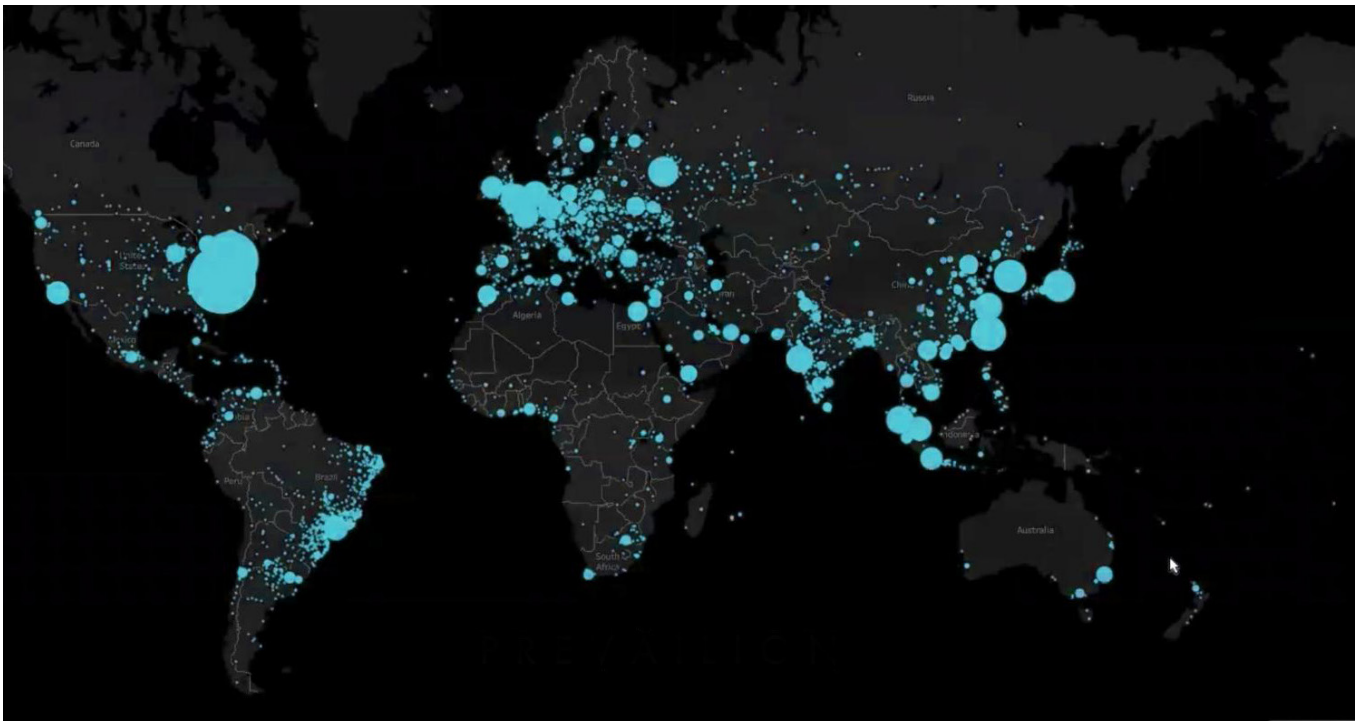
Make informed, profitable decisions with actual Evidence of Compromise associated with potential acquisitons.

Assess Your Own Risk

Identify active and historical compromises, giving you a lead time on potential breaches before they become damaging.

READY TO TRY PREVAILION TODAY?

Access to our revolutionary **Apex Platform™** is available for free. Prevailion is 100% zero-touch — it is simple to use, and there is nothing to install or deploy. Simply register for a free account, and discover your cyber contagion today.



PREVAILION.COM

ABOUT THE AUTHOR

Karim Hijazi is the Founder and CEO of Prevailion, a first-of-its-kind cybersecurity SaaS platform that provides businesses with unprecedented visibility into their own network as well as existing third-party partners and potential new partners, acquisitions or investments, empowering them to mitigate their compromise before it becomes their own.