WHITE PAPER

From Reactive to Preventative: Stopping Today's Attacks, Preventing Tomorrow's

In an ideal world, security organizations operate from a preventative security and risk management posture, stopping attackers before they come to the door. Unfortunately, that's not the reality.

Most companies operate — and are stuck — in reactive mode, just trying to stay on top of the continous influx of alerts. While organizations have a variety of tools to help manage security and risk, these tools are often siloed and underutilized due to staffing limitations. It's no wonder that only the largest enterprises have the resources to staff and equip a security operations center capable of achieving and maintaining a preventative security and risk management posture.

That is, until now. Impelix is delivering technology that empowers organizations to mature their security and risk management programs from reactive to proactive to preventative. For the first time, organizations have access to technology that demonstrates measurable improvements in security and risk management postures while addressing the challenges that have traditionally kept security teams from maturing beyond reactive mode.

The Challenge: React — With Your Hands Tied

For years, the security industry has told organizations that attacks are inevitable. The key is to reduce response times — to catch attackers before they escalate privileges, disrupt services, or exfiltrate data. But it has become increasingly difficult to detect these attacks, never mind reduce detection and response times. Decentralization, work-from-home, and rapid cloud adoption have forced organizations to protect and defend an ever-growing and ever-changing attack surface.

As new threats arise and risks are understood, security vendors respond with point solutions that are added to a growing security technology stack. Each of these tools offers a narrow view of the behavior that it's monitoring without context of the organization as a whole. Analysts are forced to determine, based on the content of a single alert, if the behavior detected is indeed malicious. And if it is, they must manually correlate that alert to dozens of other logs, in an attempt to understand the breadth of the incident across the entire enterprise. This is inefficient, at best, and commonly misses key parts of the attack, as it moves throughout the network. To efficiently detect anomalous activity, security analysts need a complete view of the environment across LAN, WAN, (hybrid) multi-cloud, identity, endpoint, and more. Consolidating the views provided by these siloed tools helps build a more *complete* picture of the attack surface, but this introduces another challenge: cost.

Regardless of the size of the budget, sooner or later, log ingestion becomes cost prohibitive. To stay within budget, organizations must pick and choose the logs they want to ingest into their security information and event management (SIEM) platform. Even though every tool contributes details that enrich their understanding of the environment, organizations are forced to make a judgment call on the

logs that will provide the most value. Sometimes the choice is easy. If a tool's log data is not supported by the SIEM, it's not included. Other times, the decision is not so easy. Often, the telemetry from non-security tools can provide valuable context when trying to understand the relationships between multiple, disparate log sources. Regardless, the result is always the same: security analysts can't "see" the entire IT environment. And this lack of full visibility hampers their ability to detect and respond to threat activity — if they can see it at all.

To mature their security operations, and move from reactive to proactive, organizations must conduct post-mortem investigations of security incidents, and then apply the lessons learned. However, many organizations do not have the time or staff to move outside of the "alert-react loop," just trying to stay on top of the security data they need to contend with on a daily basis. The vast majority of this time is spent analyzing alerts to simply weed out the false positives and duplicates across various tools. This leads to alert fatigue and eventually analyst burn out.

All of these pains are amplified by the fact that organizations are short staffed. The shortage of qualified security personnel is affecting every industry. The number of unfilled cybersecurity jobs worldwide has reached 3.5 million in 2023, with more than 750,000 of those positions in the U.S., according to Cybersecurity Ventures. And this problem won't be solved overnight. The firm predicts that the disparity between demand and supply will remain at least through 2025. In the meantime, security analysts are working harder than ever just to react to the threats they are aware of and hopefully stop attackers before a serious breach occurs.

Breaking Through the Noise

Organizations need a tool that helps them not only deal with ongoing threats, but also focus on improving their security and risk management posture. The only way to do that is to start by providing the security team with the key information they need, without the hours of manual work spent looking for "the needle in the stack of needles." This gives them back valuable hours in their day to focus on understanding their overall security posture and to start making systemic improvements.

Problem: Exorbitant cost of log ingestion

Solution: Unlimited ingest

Advances in technology have significantly lowered storage costs, so there's simply no reason to continue paying exorbitant fees to ingest log data. To understand the complex relationships between thousands of entities across the LAN, WAN, datacenter and cloud, organizations need not only all of their security data, but also all of the non-security logs for the critical telemetry data they provide. This combination of data sources is critical for understanding the complex relationships between assets and the blast radius of an attack as it spreads across the enterprise.

Problem: SIEMs only get you so far

Solution: Security response, simplified

Traditional SIEMs require security analysts to do a lot of the heavy lifting. Associating internal events to external threats, building parsers to ingest data and normalize objects for corroboration, and investigating and remediating breaches are manual tasks that require time and skill, both of which are in high demand. Organizations need a way to automate these processes and simplify the efforts of their analysts. They need to get as close as they can to an "easy button" for security detection and response – so it's all done quickly, within a single platform, and without significant security expertise.

Problem: Lack of resources to maintain yet another tool

Solution: No additional overhead

Just as there's no reason to pay the exorbitant fees legacy SIEM providers charge for log ingestion or compute, there's also no need to procure and maintain compute resources, whether they be onsite or in the cloud. The simplification delivered by a modern SIEM extends to the solution itself. A SaaS-based solution eliminates the overhead traditionally associated with running and maintaining a platform.

Problem: Difficulty proving value

Solution: Deliver clear ROI

The notorious difficulty of demonstrating the return on a security investment creates organizational obstacles to maturing their security and risk management postures.

Organizations need a platform that measures security and risk management maturity as proof of continuous improvement over time. This is a key (and often overlooked) part of the process for getting budget and implementing a successful security operations strategy.

Beyond that, organizations need visibility into the efficacy of their security controls. This means not only analyzing the effectiveness of the individual point solutions, but also determining which tools are doing more harm than good with limited effectiveness and/or high volumes of noisy alert data. Since the platform is collecting logs from every tool in the environment, it can also provide insights into the tools that no longer fit the organization's requirements or can be fine tuned to be more effective.

Problem: Still too many tools

Solution: Integrated compliance and risk monitoring

Security and risk management initiatives go hand-in-hand and are requirements for doing business today. But if not properly managed, they can generate significant costs to the business. Organizations need security and risk management processes optimized to make them as efficient as possible. Combining security and risk management into a single platform provides these efficiencies. While the security team tracks the current threat landscape and responds to ongoing breach attempts, the risk team can continually monitor compliance status and deliver incremental, continuous improvements to the security posture of the organization.

From Reactive to Preventative with the Impelix IMPACT platform

At Impelix, we understand the challenges security organizations face on a daily basis. Since 2010, we've been helping enterprises build, manage, and mature their security operations to become preventative in the fight against cyberattacks. Recognizing the market need for a tool, like the one we use to assist our customers, we decided to release the Impelix IMPACT platform.

As the first of its kind, the Impelix IMPACT platform is an integrated security, risk, and compliance management solution designed to address the security and risk management challenges organizations face today and help them move from being reactive to proactive and finally to a preventative security model.

REACTIVE

With user-based pricing, the Impelix IMPACT platform eliminates the budget constraints typically associated with data ingestion and SIEMs. The platform leverages machine learning to validate and corroborate security events for security analysts, and only alerts on high-risk/high-confidence incidents. These capabilities significantly reduce the volume and increase the fidelity of alerts that are presented to the security team. Automated and real-time event correlation presents the complete enterprise-wide impact of a security incident, with no manual effort required, reducing the time to detect and react to a threat.

PROACTIVE

With one year of data retention in hot storage, security organizations have plenty of data at their fingertips to hunt down threats beyond alerts. Natural language queries reduce the skills barrier, enabling members of the security and compliance teams to search for known indicators of compromise/attack, investigate anomalous behavior, and uncover threats that may have bypassed detection technologies. This helps security teams move from being reactive to proactive; taking actions to find and root out potential threats, before a breach occurs.

PREVENTATIVE

The Impelix IMPACT platform provides visibility into the security technology stack itself, including tool efficacy and redundancy. This enables teams to continuously tune and improve the tools in their security stack, as well as find the gaps in their security controls. By understanding their current exposure, security teams can then move to a preventive security model by prioritizing and implementing changes that shore up the underperforming areas of their security controls, decreasing the risk of a future breach. In tandem, real-time risk monitoring and compliance framework assessment help teams manage their level of risk and compliance within major security and regulatory frameworks.

How Impelix makes an IMPACT

- ✔ Predictable user-based pricing model with unlimited ingestion and one year of retention
- ✔ Enable swift (automated or one-click) incident response within a single platform
- ✔ Understand business and reputational risk, financial risk, supply chain risk, and potential data leaks
- ✔ Tool efficacy provides a cost analysis for tools and staff resources
- ✔ Simple to use SaaS platform with < 30-day time to value

For the majority of organizations, security operates in a perpetually reactive mode. The lack of contextual visibility, automation, and skilled staff make it difficult to move beyond this mode. To deliver a return on investment, any additional tools added to the security technology stack must not only demonstrate a measurable reduction in risk but also enable the organization to operate more effectively and mature their security and risk management programs to a preventative security model.

The Impelix IMPACT platform is exactly what these organizations need — a turnkey SaaS platform that enables teams to understand their security posture and implement a continuous improvement program using real-time data on cyber readiness and risk, compliance readiness, and tool, staff, and resource efficacy (including ROI, operational efficiency, and third-party risk).

Get A Demo