Newly Released GYTPOL 2.0 Solves Familiar Cybersecurity Problem

Platform detects and remediates endpoint misconfigurations – making security more efficient, effective, and durable

NEW YORK, NEW YORK, UNITED STATES, May 7, 2024 /EINPresswire.com/ -- GYTPOL Inc. has announced the general availability of its upgraded GYTPOL 2.0 platform. GYTPOL 2.0 is the next generation of the company's configuration security assurance and policy validation platform. Delivering unmatched visibility and context-awareness, GYTPOL identifies and prioritizes ill-advised device settings that can expose network data, systems, and services.

> With misconfigurations on lockdown, we're able to move on to other vital tasks and strive for new levels of efficiency and security."
>
> *Ruben Chacon*

When misconfigurations are registered, they are itemized and packaged as alerts – sortable according to severity, security group, device type, and attack vector. These alerts can then be bulk-actioned and remediated with the push of a button. The system even allows users to leverage dynamic grouping to auto-remediate future misconfigurations (on new devices).

Value is added not only in the newfound scalability of detection and correction efforts, but in the platform's zero-disruption guarantee. While operators might normally be reluctant to make changes due to unknown dependencies and the risk of "breaking things," GYTPOL empowers users to act decisively – hardening their security without fear of unintended consequence.

Using GYTPOL, users can easily identify and limit remediations to devices and setups without any functional dependencies. And if they want to take a more aggressive approach, they can operate with complete confidence knowing they have rollback-at-a-click capabilities.

The problem of endpoints configured in vulnerable ways is nothing new. It's been around virtually as long as devices have been networked and internet-connected. And while recent years have seen all manner of cybersecurity innovation and up-tooling, when it comes to misconfigurations, operators still remain mostly on their own.

Other cyber fronts are shorn up by bridging technological gaps and enforcing universal best practices. The objective nature of the work lends itself well to third-party innovations. When it

comes to misconfigurations however, the problem does not reside in the technology, but in its use. There are no universal standards and no outright design flaws. The flaws are more nuanced – rooted in the deployment rather than the tech – and the "right" configuration depends entirely on the context. There's no silver bullet and no one-size-fits-all solution. It's not something that can be patched and there's no easy fit for third-parties.

So vendors largely ignore the problem, leaving operators to their own devices (literally) – relying on careful attention-to-detail and manual best efforts. But that's rarely enough and today misconfigurations run rampant.

It's estimated that 73% of organizations have at least one critical security misconfiguration putting their business at risk. In fact, 35% of all security incidents and 80% of ransomware attacks are caused by misconfigurations. Going forward, these numbers are only expected to grow.

The problem is exacerbated by operational fragmentation. Different device types, different operating systems, different needs, and different software results in fragmented visibility, fragmented tooling, fragmented controls.

GYTPOL was created to solve this problem and, with the release of GYTPOL 2.0, the company says that goal has been principally achieved.

"When it comes to cybersecurity, if you're vulnerable anywhere, you're vulnerable everywhere," says GYTPOL co-founder and CEO Tal Kollender. "That's why we're so determined to provide an alternative to improvised policies, hope for the best enforcement, and manual reviews. Because right now the whole market is vulnerable."

Kollender adds, "The traditional approach just doesn't work. Everyone knows it, but very few are doing anything about it. It's a classic head-in-the-sand situation, with organizations just waiting to see if they get attacked."

According to GYTPOL, that's all about to change. The 2.0 release improves the platform's UI and UX, while adding more integrations (ServiceNow, Palo Alto Networks, CrowdStrike, etc.) and significant new functionality. Among other capabilities, the new release introduces:

•Browser and web server hardening
•Intune intelligence
•Database settings security
•Framework (CIS, NIST, etc.) compliance
•ROI tracking
•AI assisted prioritization

This functionality, much like GYTPOL's legacy functionality, is designed to deliver maximum

coverage and push-button resolution. The company's commitment to scalable and secure operations has resulted in a loyal and growing customer base. Today GYTPOL serves over 300 companies worldwide, securing more than 3 million devices.

One of those customers is EATON. "The GYTPOL platform has been present in the marketplace for a few years now. For us, it's always been a breath of fresh air, but with the release of GYTPOL 2.0 it's a complete game-changer," says Ruben Chacon, Chief Information Security Officer of EATON.

"GYTPOL's totally unparalleled - both in terms of capabilities and convenience," adds Chacon. "It allows us to handle configuration security in a much more air-tight manner, in way less time, and with zero hassle. With misconfigurations on lockdown, we're able to move on to other vital tasks and strive for new levels of efficiency and security."

Kollender sums it up nicely, explaining that "In many ways, it feels like configurations are both the final frontier and the wild west of cybersecurity. There's no reason businesses should continue to operate at such serious levels of risk. There's a better way and I'm proud to say that GYTPOL is paving it."

To learn more about how GYTPOL secures endpoint configurations, you can visit their website at www.gytpol.com. Demonstrations can be scheduled via gytpol.com/demo. Free security assessments are available upon request at www.gytpol.com/free-trial.

􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀

About GYTPOL
Founded in 2017, GYTPOL is a first-of-its-kind platform to help manage and harden endpoint configurations. GYTPOL detects and corrects misconfigurations that put connected devices at risk. The platform enables push-button remediation and reversion to secure any individual device or device group according to the relevant standards or controls.

Ilan Mintz
GYTPOL Inc.
ilan@gytpol.com
Visit us on social media:
Twitter
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/709232613

Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.