GYTPOL

Comparison Analysis

Doc: GYT-MKT-003
Release: 3
Date: 3rd March 2022

Confidential: GYTPOL and approved recipients

Total pages:	9

Doc. Title:	GYTPOL Comparison Analysis

Doc. No.:	GYT-MKT-003	**Classification:**	Confidential
Revision:	3	**Restriction:**	GYTPOL and approved recipients
Date:	3rd March 2022	**Customer:**	

Owner:	Matthew Album	**Reviewers/ Approvers:**	Tal Kollender
Author:	Matthew Album		

Contents

GYTPOL Product Comparison

Introduction

The purpose of this document is to provide a comparison of the different categories of security tools to show the differences, similarities, and benefits of GYTPOL Validator.

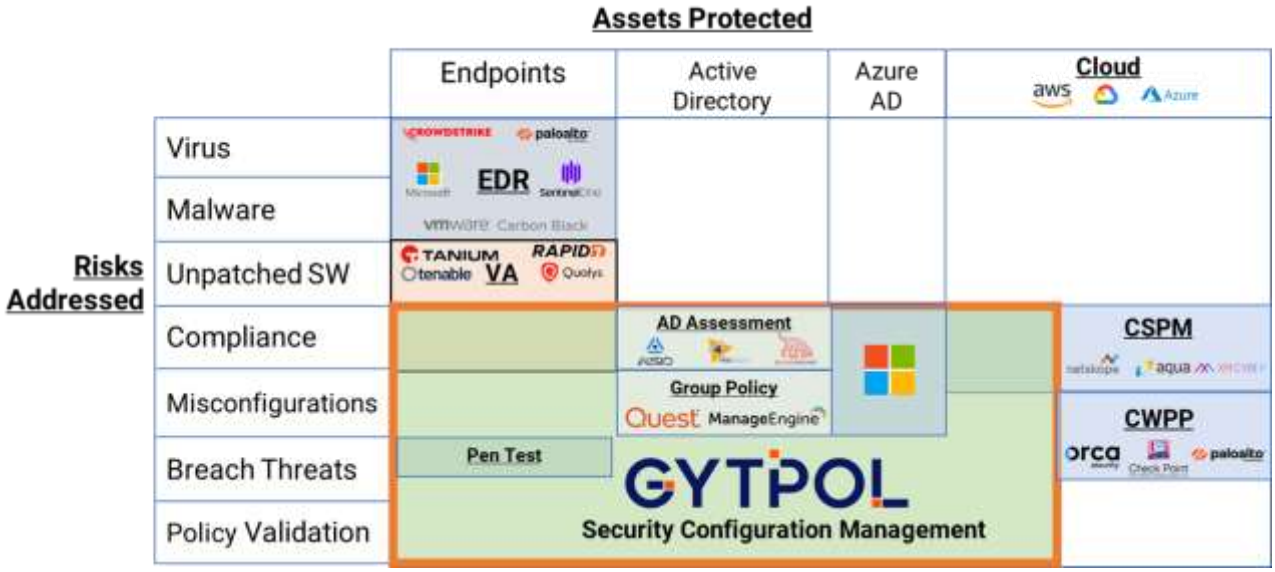
Disclaimer: This comparison does not compare specific products, rather the general concept of the product category. Therefore, it is acknowledged that certain specific products in a category might have more or less features than assumed for this document.

The categories under consideration are:

Category	Example of Product Vendors
Endpoint Detection & Response (EDR)	CrowdStrike, MS Defender, Sentinel 1, Cybereason
Endpoint Vulnerability Assessment (VA)	Tanium, Qualys, Tenable, Rapid 7
Cloud Secure Posture Management (CSPM)	XM Cyber, Aqua Security, Netskope
Cloud Workload Protection Platform (CWPP)	Palo Alto Networks, Checkpoint, Orca, Symmantec
Penetration Testing	Various Tools
Active Directory Assessment	Bloodhound, Ping Castle

Security Risk Identity and Protection Map

The diagram below shows how the different products categories map to different types of assets being protected.



Endpoint Detection & Response (EDR)

EDR products provide real-time detection of cyberattacks in endpoint devices (both PCs and Servers). They also offer mitigation capability. EDR products are viewed as the most important IT Security endpoint tool to deploy by organizations.

EDR products function by monitoring in real-time **files and processes in memory** to detect if they are infected by a hacker/cyberattack. EDR products will also provide offline scanning of all files on the endpoint. Some of the leading EDR products will utilize A.I. and global intelligence to further enhance their capabilities.

EDR will detect viruses, malware, ransomware, and phishing attacks.

EDR provides mitigation capability by stopping the infected file or process and preventing it from being used.

Vulnerability Assessment (VA)

VA are a category of tools used to discover vulnerabilities. A vulnerability is a bug in an application or operating system which can cause a security exploit. The bug needs to be fixed by the software vendor.

In general VA tools will scan for vulnerabilities based on a known catalogue of publicly published vulnerabilities called CVEs. Some VA products will also provide asset management and compliance checking.

A vulnerability is detected when the device (endpoint or server) has not been patched to the latest software version released by the software vendor where the vulnerability was fixed.

Some VA products offer remediation as a feature. In some cases, remediation is more of a workflow action as opposed to taking control and remediating the issue. For example, the VA will recommend to patch to version X and then send a ticket to ensure the action can be carried out by the IT Administration team. Some of the advanced VA vendors will also take care of the patching as part of their remediation capability.

Cloud Secure Posture Management (CSPM)

Cloud Security Posture Management (CSPM) automates the identification and remediation of risks across cloud infrastructures, including Infrastructure as a Service (IaaS), Software as a Service (Saas), and Platform as a Service (PaaS). CSPM is used for risk visualization and assessment, incident response, compliance monitoring, and DevOps integration, and can uniformly apply best practices for cloud security to hybrid, multi-cloud, and container environments.

Cloud Workload Protection Platform (CWPP)

Cloud Workload Protection Platform (CWPP) as defined by Gartner is a “workload-centric security solution that targets the unique protection requirements” of workloads in modern enterprise environments.

Penetration Testing (Pen Test or Ethical Hacking)

This is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify weaknesses including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

Pen Testing is typically performed 1 to 4 times a year in an organization. The testing itself focuses on a sample set of devices in the organization.

Pen Testers will use a collection of tools (both commercial and in the public domain) to perform the various tests in scope.

The output of a Pen Test is a report of recommendations. Remediation is not supported.

Active Directory Assessment

Active Directory Assessment provides you with an assessment of an Active Directory Environment with domain controllers running on-premises, on Azure VMs, or on Amazon Web Services (AWS) VMs. ... Active Directory Replication. Site Topology and Subnets. Name Resolution (DNS) Domain Controller Health.

AD Assessment is typically run 1-4 per year in an organization. The output is a report. Remediation is not supported.

Continuous monitoring of the AD Environment is available by a small number of leading vendors.

Security Configuration Management - GYTPOL Validator

Security Configuration Management addresses security gaps caused through misconfigurations in the operating systems of Endpoints and Servers as well as Infrastructure Services. Misconfigurations can be defined as settings which are caused by human/operator error or default settings from the OS vendor.

The impact of misconfigurations will allow hackers to breach a device and then use other misconfigurations or hacking techniques to gain addition privileges and laterally move within an organization.

Security Configuration Management is separate category of security tools as the other categories do not focus on misconfigurations.

Leading industry data, for example from Dark Reading and RSM Consulting report that 33-40% of all successful security attacks are caused due to misconfigurations. This percentage increases significantly when cloud misconfigurations in cloud infrastructure services are involved.

Security Configuration Management tools should support:

- Continuous monitoring for misconfigurations of all endpoints & servers covering all types and flavors of operating systems.
- Continuous monitoring for misconfiguration in Service Infrastructure components for both on premise (e.g. Active Directory) and Cloud (e.g. Azure, AWS, GCP).
- Accurate Detection and categorization of misconfigurations. Categorization should be according to a standard security framework.
- Severity in terms of potential risk and impact. This allows prioritization in the remediation stage.
- Detection of policy mismatches (i.e. validation that a defined policy is applied or not for the user or device.
- Security Baseline validation either a custom base-line of standards compliance based (e.g. CIS, ISO etc)
- Remediation

The leading Security Configuration tools support **remediation**. This is a major and important differentiator. Remediation should enable the resolution of the detected misconfigurations. Remediation should be :

- Fast. Ability to immediate close the security gaps for all impacted devices immediately.
- Automatic. Remove the need for operator action if a new device or existing devices are detected with the misconfiguration which has previously been authorized for remediation.
- Zero Impact: Remediation should not impact any business operation or cause a third-party application to fail. The tools should accurately show which devices will or not be impacted before the remediation action takes place.
- Revert: Undo any remediation action back to previous state.

Comparisons with GYTPOL

The table below takes each category of security tool and provides a comparison with GYTPOL including use cases where GYTPOL can augment this category.

Item	Explanation
EDR products	EDR products and GYTPOL do not overlap. EDR is focused in detecting and mitigating real-time attacks based on files and processes in memory. EDR does not monitor, detect, or remediate misconfigurations. This means that a hacker can continuously exploit the same misconfiguration to attack endpoints with different malicious malware. GYTPOL can also detect if the EDR itself has been disabled/uninstalled by a hacker (supported by some EDRs) GYTPOL can detect if more than one EDR is active or the corporate EDR has been replaced by another EDR (typically due to a user downloading freeware software). There are known cases where two EDRs running on the same machine can cause conflict and allow attacks to happen which will not be alerted by either EDR. GYTPOL can detect if the threat user has become a system account whilst EDR does not detect this as suspicious behaviour. EDR is unable to detect if an endpoint has weaknesses which can be exploited by a hacker to breach the endpoint. EDR is an endpoint only solution. It does not look at the end-to-end risk. EDR is an active agent in the endpoint. GYTPOL is a lightweight semi-agent (1.5MB) triggered by the task scheduler; runs once a day for up to 5 minutes.

Vulnerability Products	Most GYTPOL customers already have a VA product deployed but buy GYTPOL as they understand it is a different security category not covered by VA. VA products and GYTPOL do overlap for detection, up to a maximum of 10% for specific products. In most cases the detection method is different. For example both VA and GYTPOL would detect SMB v1 risk but GYTPOL goes further and also detects if SMB v1 is actually being used by the endpoint and can also remediate it. VA are detecting vulnerabilities based on the CVE catalog. Misconfigurations cannot be mitigated by software patching and will still exist even after an upgrade. This is because misconfigurations are not due to security software bugs in the product.
CSPM	There exists overlap between CSPM and GYTPOL. In general, GYTPOL views itself as complementary to CSPM rather than replacing. CSPM is dedicated to cloud services and detecting risks caused through misconfigurations. CSPM focuses on the cloud which means it does not consider the E2E environment of an organization. This includes the on-premises hybrid structure and the endpoints and servers themselves. GYTPOL complements CSPM in that it provides an E2E view of misconfigurations from both the cloud and on-premises to the endpoint. There exist numerous risk scenarios where conflicting configurations from both the cloud and on-premises policies. This can only be identified with a single tool which can provide the visibility and analysis of both mechanisms.
CWPP	CWPP does not overlap with GYTPOL. CWPP is focused on the risk to data and applications in cloud workloads. It functions as part of the CI/CD pipeline in a DevOps environment. Cloud Workloads (whether on-premises or in the cloud) sit on top of an Operating System. It is the OS itself where GYTPOL is detecting misconfigurations which can cause risks to the overall environment where the cloud workloads are functioning.

Penetration Testing	Pen Testing is carried out using a collection of different tools. Some customers / security services companies perform Pen Testing include GYTPOL in their toolset due to the unique set of results GYTPOL offers and the remediation capability. However, this is not the intended application of GYTPOL. Pen Testing is looking for a wide range of risks including misconfigurations, but the scope of misconfigurations identified by Pen Testing tools are significantly less compared to the GYTPOL product. Pen Testing is not continuous (i.e., 24x7). It does not analyze all endpoints and servers in an organization but a sample subset of devices. Pen Testing is costly to organizations, intrusive and impacts productivity during the period of the test. Pen Testing does not offer remediation. The output is a report of findings and recommendations. Organizations will then need to invest time and cost mitigating the risks and implementing the recommendations.
Active Directory Assessment	Active Directory Assessment tools are one-time scanning applications which are run 1-4 times a year. Some organizations might run them more frequently. The scope of items scanned compared to GYTPOL depends on the specific products although GYTPOL in general is broader in scope compared to most AD Tools we are familiar with. The tools are focused purely on the Active directory itself deployed on the domain controllers of the organization. AD Assessment is not continuous (i.e., 24x7). It does not analyze endpoints and servers in an organization, just the AD itself. AD Assessment does not offer remediation. The output is a report of findings and recommendations. Organizations will then need to invest time and cost mitigating the risks and implementing the recommendations.

GYTPOL's unique capabilities

The table below describes some of GYTPOL's unique capabilities.

Item	Explanation
24x7 Monitoring End-to-end	GYTPOL is covering end-to-end including endpoints, servers, on-premises infrastructure services (i.e., Active Directory, Domain Controllers) and cloud services (AAD, Intune, M365 etc). Supported Devices: • Windows PCs & Servers • Linux • Apple Mac • Chrome Book Future Planned Devices • IoT Devices • Android • IoS
Coverage of Misconfiguration Detections	The coverage of misconfiguration detected by GYTPOL is too large to include in this document. Please refer to the GYTPOL Core Indicators datasheet. GYTPOL is unique in that there is not another tool available which provides such an extensive coverage of misconfigurations from Endpoints, Servers, On-premises infrastructure services and cloud infrastructure services.
Remediation	GYTPOL's capability to remediate endpoint misconfigurations is a game-changer in helping organizations save significant time and risk. Some key features with GYTPOL remediation • Status monitoring of remediation actions. • Fast. Ability to close the security gaps for all impacted devices immediately. • Automatic. Remove the need for operator action if a new device or existing devices are detected with the misconfiguration which has previously been authorized for remediation. • Zero Impact: Remediation should not impact any business operation or cause a third-party application to fail. The tools should accurately show which devices will or not be impacted before the remediation action takes place. • Revert: Undo any remediation action back to previous state.

	It should be noted that other tools which support remediation only support raising a ticket and not actually resolving the issue itself.
Policy Validation and Enforcements	For organizations using either Group Policy Object (GPO) of Active Directory, Azure Intune Policies or both will be familiar with a well-known limitation that policies cannot be guaranteed to be correctly applied on the endpoint. With a lack of enterprise tools available, organizations have had to write their own in-house scripts to achieve a basic level of visibility. GYTPOL's Policy Validation module enables full visibility of wrongly applied policies, wrongly configured policies as well as numerous other capabilities of detecting orphaned policies and local policies created.
Compliance	GYTPOL has a two-stage approach to compliance validation. The first stage is validating policy compliance against the infrastructure (for example AD GPO). The second stage is ensuring the policies are applied correctly on all endpoints. There are numerous products available which can validate compliance standards such as CIS, ISO27001 etc for the first stage only. GYTPOL is the only product which offers both stages of the compliance validation.
Remote Employees	GYTPOL support continuously monitoring, alerting and remediation of misconfigurations for endpoint devices which are remote and not connected to a VPN. Here, GYTPOL's uniqueness is with providing visibility and remediation of items which rely on on-premises infrastructure services and normally require a VPN connection. For example, applying GPO policies are only possible with a VPN yet GYTPOL can be used to enforce the same policies without the need of a VPN.

GYTPOL's similar capabilities

The table below describes some similarities of GYTPOL capabilities with other product categories

Item	Explanation
SIEM Support	GYTPOL supports all SIEMS which can receive SYSLOG
Know-How Guides	GYTPOL supports Know-How guides on how to mitigate misconfigurations allowing organizations to choose to use their own mitigation and change process if they prefer to not use the GYTPOL remediation capability.
Auto Upgrade	GYTPOL's semi-agent requires distribution only once. Future updates of the semi-agent are done automatically via the GYTPOL Server application.
False / Positives	Some misconfiguration detections are considered valid by organizations and intended by design. In these instances, GYTPOL can mute the specific detection.
Lightweight Client	GYTPOL does not use an agent on devices but a semi-agent. This is a lightweight task scheduler of approximately 2MB in size and sending back approximately

Summary

Based on the comparison analysis provided in this document, it shows that other security tool categories provide functionality to address security risks. However, when addressing the misconfiguration attack vector these tools provide minimal coverage and that the security posture of organizations remain exposed and at risk.

This can be proven by the significant increase in reported successful attacks caused to organizations in both the enterprise and government sectors. In most cases, these organizations had deployed all categories of security tools as discussed in this document yet without the visibility and remediation capability of a tool like GYTPOL Validator they will continue to be left exposed.