



Configuration Security for Endpoints & Servers

Validator



Endpoint Security Insights

68%

Organizations were hit by a **cyber attack** in the last year

70%

Successful Breaches originate on the Endpoint & Server

84%

Organizations feel exposed due to **lack of visibility of remote endpoints**

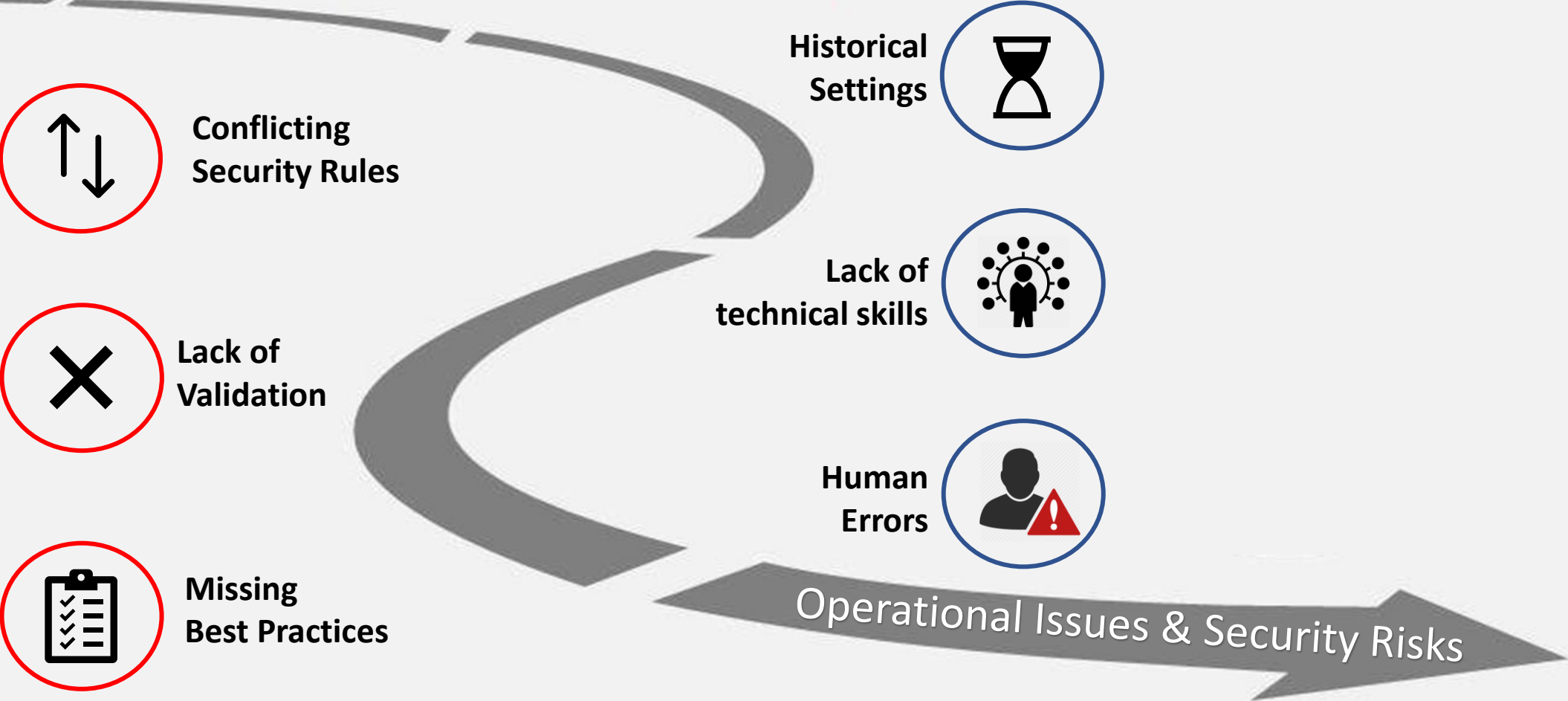
**CONFIGURATION SECURITY
WILL HELP REDUCE THESE METRICS**

Endpoint Security Quotes

“There are two types of companies: those that have been hacked, and those who don't know they have been hacked.”, John Chambers, previous Cisco Chairman & CEO

“Active Directory is #1 attack vector”, Daniel Wiley, VP Incident Response, Checkpoint

Misconfiguration Roots



MISCONFIGURATIONS ARE EVERYWHERE



INFRASTRUCTURE ON PREMISES & CLOUD



Microsoft
Active
Directory



Microsoft
Azure AD



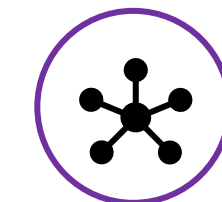
Microsoft
365



Microsoft
Intune



Amazon



Software
Defined
Networking

ENDPOINTS & SERVERS



Microsoft
Windows



Apple
Mac



Linux

MOBILE






























Apple



Android

IoT



Services	Consumer	Public Sector	Financial	High Tech
<p>Mishcon de Reya</p>  <p>ELVALAL</p>	<p>sodastream®</p> <p>DIPLOMAT</p>	  <p>Population and Immigration Authority</p>  <p>MINISTRY OF DEFENCE</p>  <p>Municipality</p>  <p>THE OPEN UNIVERSITY OF ISRAEL</p>	 <p>UNION BANK</p>  <p>Bank Yahav</p>  <p>CLAL INSURANCE</p>  <p>HAREL Insurance & Finance</p>  <p>MERCANTILE 100 YEARS OF GROWTH</p>  <p>SHOMERA INSURANCE COMPANY LTD.</p>  <p>MIGDAL CAPITAL MARKETS</p>  <p>AYALON INSURANCE COMPANY LTD.</p>	 <p>Mellanox TECHNOLOGIES NVIDIA company</p>  <p>Click salesforce company Actual Intelligence. At Work.</p>  <p>Playtika</p>  <p>matrix</p>
Manufacturing	Healthcare			Cyber Security
 <p>IAI ISRAEL AEROSPACE INDUSTRIES</p>  <p>ADAMA</p>  <p>ASHTROM Group EXCELLENCE IN CONSTRUCTION</p>  <p>CHEMOVIL כימוביל</p>	 <p>Bnai Zion Medical Center</p>  <p>HOSPITAL ASSUTA RAISING HEALTH STANDARDS</p>  <p>HERZLIYA MEDICAL CENTER</p>			 <p>Check Point SOFTWARE TECHNOLOGIES LTD</p>  <p>CYBERARK</p>

Trusted on over 1 million Endpoints

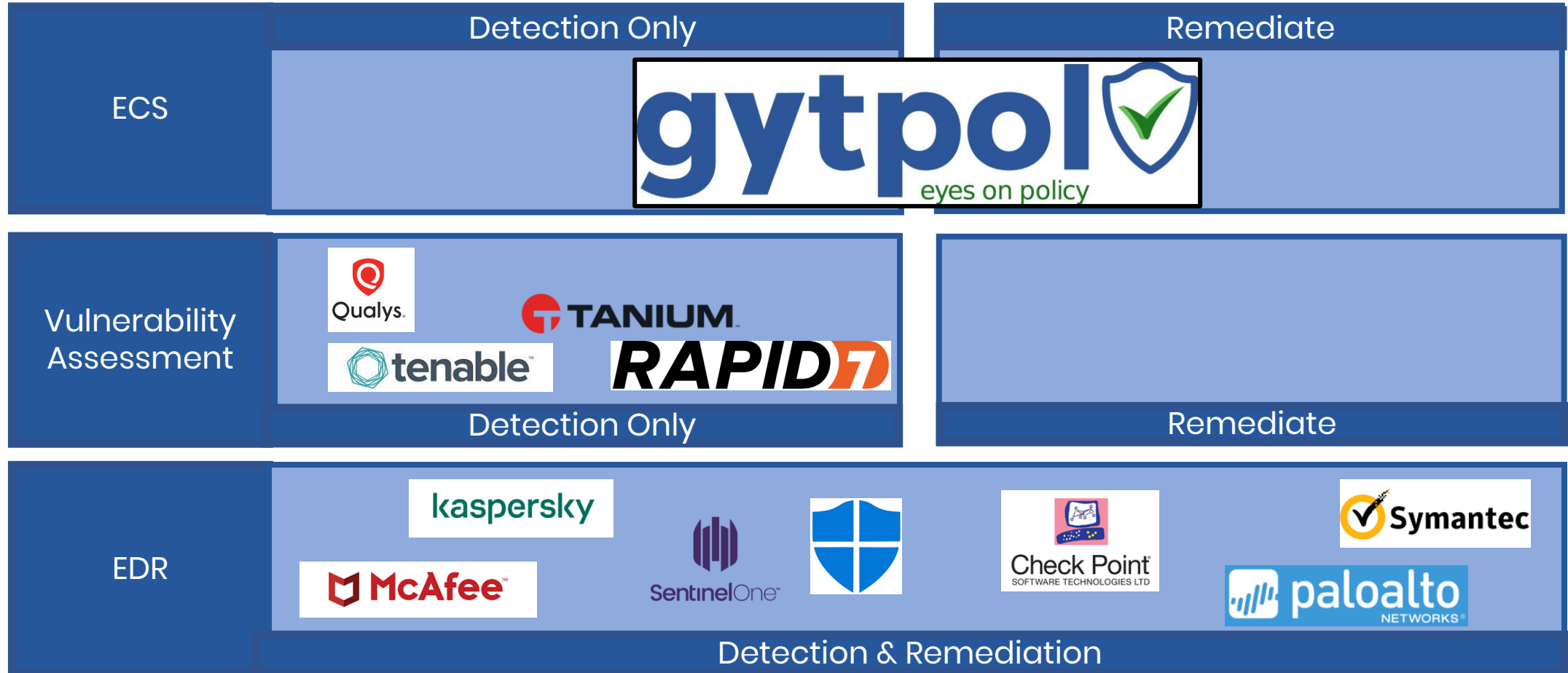
gytpol Validator

- **First and Leading** Configuration Security Solution for Endpoints & Servers.
- **Unique Product.** Detects & remediates security risks caused through misconfigurations & wrongly applied policies. These gaps go undetected by other threat & vulnerability security tools, which are exploited by hackers.
- **Enables Visibility.** Allows organizations to extend their overall security protection coverage and reduce operational issues.

Configuration Security for Endpoints & Servers

- Finds **security risks** in endpoints overlooked by other tools such as EDR, Vulnerability Assessment (VA) and Penetration Testing
- Customers use **Gytpol Validator** in addition to other security tools.
- Provides a more **comprehensive security**

Endpoint & Server Security Components



gytpol Validator

- **First and Leading** Solution in Configuration Security.
- **Includes 6 Key Modules**
 1. Configuration Risks
 2. Policy Validation
 3. Remote Workforce Analysis
 4. Compliance & Audit
 5. Performance Optimization
 6. Remediation



gytpol Validator Key Features



**Configuration
Risks**



Policy Validation



**Remote Workforce
Analysis**



**Compliance and
Audit**



**Performance
Optimization**



Remediation

gytpol Validator Key Features



Endpoint & Server Configuration Risks

Discovers critical configuration risks in endpoints. Identifies unprotected credentials & clear text passwords. Alerts local admins, unauthorized open ports, inactive anti-virus in endpoints and much more



gytpol Validator Key Features

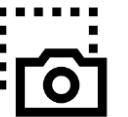


Policy Validation

Prove Security Policies are applied and work correctly on the Endpoints & Users.

Identifies Active Directory threats. Intune & Group Policy discrepancies & vulnerabilities.

Verifies OS Security Updates

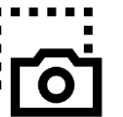


gytpol Validator Key Features



Remote Workforce Analysis

Maintain visibility on employees working from home even if they are not connected to the network by VPN.



gytpol Validator Key Features



Compliance and Audit

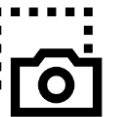
Near real-time validation of compliance, supporting GDPR, ISO 27001, NIST, CIS, SOX, PCI DSS, HIPAA. Create and customize your own internal audit rules for validation

gytpol Validator Key Features



Performance Optimization

Improves Start-up and Login times.
Correlates delays with hardware types



gytpol Validator Key Features



Remediation

Remediation actions allowing issues to be fixed quickly and accurately without risk. Trusted knowledge you can rely on.

Validator Remote Workforce Module

**84% OF ORGANIZATIONS FEEL EXPOSED
DUE TO LACK OF VISIBILITY OF REMOTE ENDPOINTS**

How hackers exploit remote endpoints

- WiFi with weak encryption or fully open
- OS and Policies are not updated or un-patched
- VPN reliability. Encryption fails 40% of the time
- Anti-malware is either deactivated or missing 28% of the time
- Use of home devices to access corporate resources
- Use of unauthorized apps installed on corporate endpoints



Validator Remote Workforce Module

- Provides **visibility** of Remote Workforce endpoints to IT & SecOps allowing issues & vulnerability to be quickly identified and remediated
- E2E Encryption for Endpoints that are **not connected to the network** through our public cloud SaaS

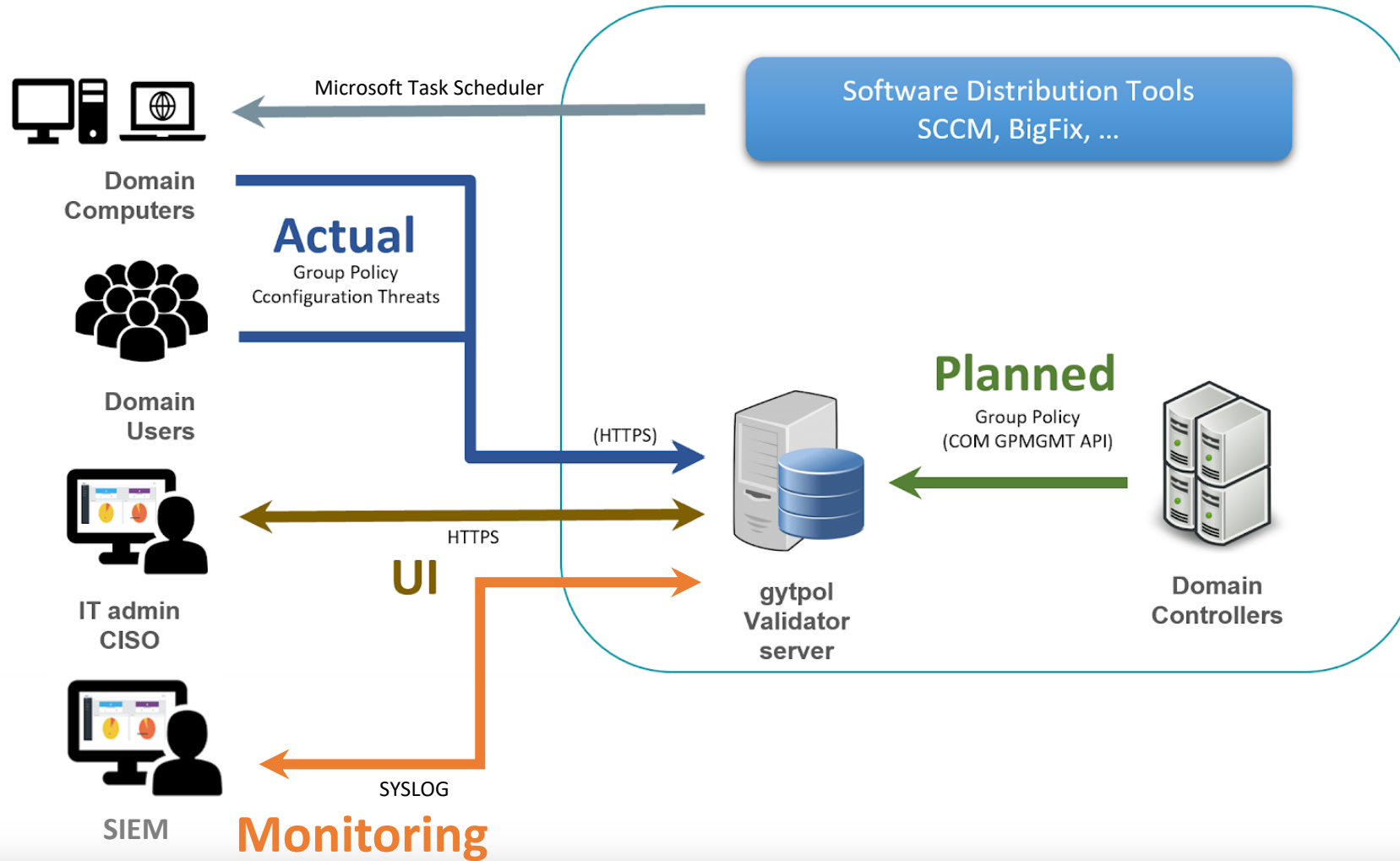


Validator Remote Workforce Module

Analysis Includes:

- **WiFi connection.** Alerts if a weak encryption type or weak password is being used
- **Remote Desktop.** Reports if the RDS is active. Unless required RDS should be left inactive due to Microsoft vulnerability
- Last time the **OS and Policy** were updated on the endpoint
- **Services.** Check essential services are active on the endpoint for continued security
- **Geolocation** of Endpoint based on real IP Address
- **Bitlocker.** Alerts if the hard disk volumes are not encrypted. An encrypted hard disk helps prevent malware attacks and if the endpoint is stolen.
- **Proxy Redirects.** Checks any proxy redirects to another gateway belong to the organization.
- **Firewall.** Checks that endpoint firewall rules are active even when not connected to the organization network

gytpol Validator - How Does It Work?

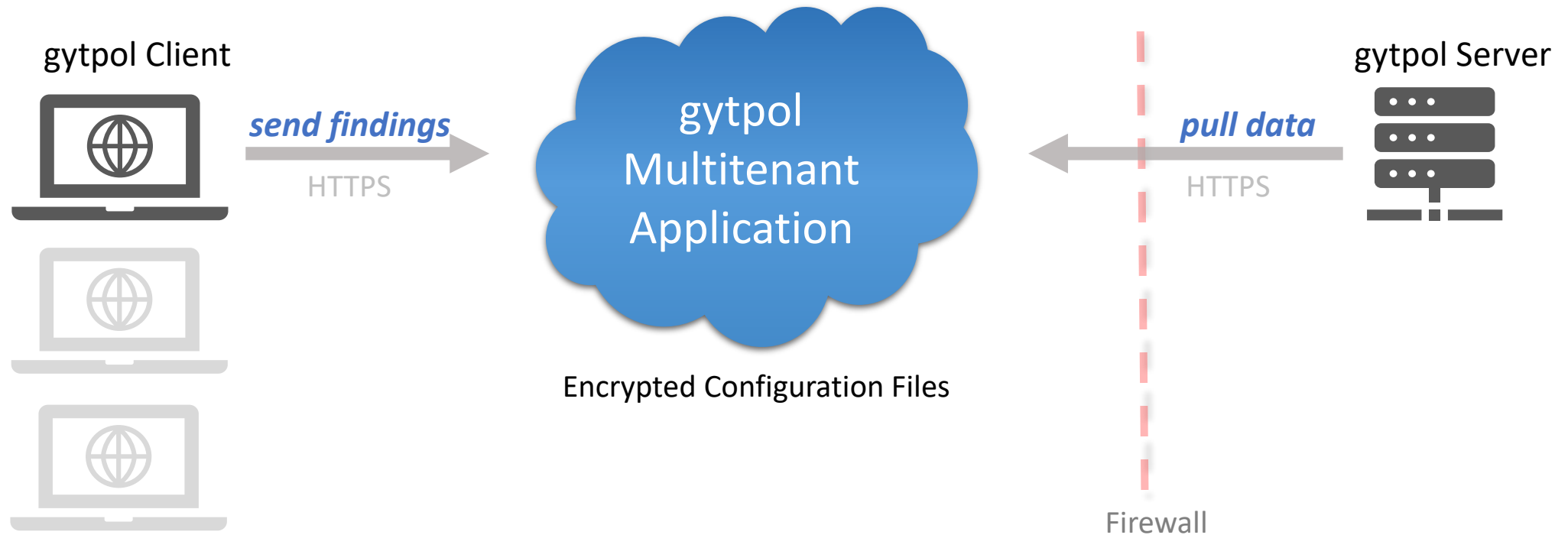


Remote Employees E2E Encryption Architecture

Remote Employees

Public Cloud – MS Azure

Customer Internal NW



Integration with SIEM



- ✓ Group Policy Discrepancies
- ✓ Host Threats
- ✓ Unpatched Hosts
- ✓ Root Cause for Long Login

IBM QRadar

splunk>

LogRhythm™

ArcSight

And others...

Validator Major Roadmap Features



0-3 months

- M365
- Azure AD
- MacOS



3-6 months

- Microsoft Intune
- Compliance
- Customized Audit
- Multi-language
- Executive Reporting export
- Linux



6-12 months

- Multiple Domains
- Advanced Policy Analysis
- IOS
- Android

Free PoC offer

Free Trial includes the follows:

- Validator Analytics Server
- Validator Dashboard
- Lightweight Endpoint Semi-Agent
- Endpoint Threat Analysis Module
- Remote Workforce Module
- Compliance & Audit Module
- Policy Validation Module
- Endpoint Performance Module
- Security Updates Verification
- Windows PC & Windows Server

DASHBOARD SCREENSHOTS

- ENDPOINTS
- Policy Validation
- Misconfigurations
- Remote Employees
- Login Profiler
- GROUP POLICY ACTIVE DIRECTORY
- Security
- Maintenance
- Compliance
- Auditing
- KnowHow

Win Server 2016 Standard	236
Win Server 2008 R2 Standard	25
Win Server 2012 R2 Standard	123
Win 7 Enterprise	19

Computer-No-AV/Win10	26	303
Computers-NoPolicy/Win10	9	188
Servers	5	84
N/A	232	

Threats and Suggested Solutions

Severity	Computers	Topic	Subject
High	22 / 1,001	Group Policy Service	Group Policy Elevation of Privilege Vulnerability
High	846 / 230	Internet Service	Computer is providing an Internet service
High	1,041 / 134	SMB Version	Vulnerable SMB v1 Network File Sharing
High	1,136 / 39	Service Account	Service using unsafe account
High	1,141 / 30	SMB Shares	Computer is providing Network File Shares
High	260 / 23	IIS Credentials	IIS web service using unprotected credentials
High	266 / 17	Connection String Password	Connection String contains sensitive data
High	1,118 / 7	Task Credentials	Scheduled Task includes unsafe user credentials
High	1,125 / 4	Antivirus Inactive	Antivirus engine inactive or not present
Medium	1,175	TLS / SSL Version	TLS / SSL version has security flaws
Medium	8 / 1,167	PowerShell Version	PowerShell v2.0 installed and vulnerable
Medium	1,100	Device Guard	Windows Defender Credential Guard disabled
Medium	25 / 1,098	Local Admins	Local administrator on computer

SMB v1 active

IIS Webservice running

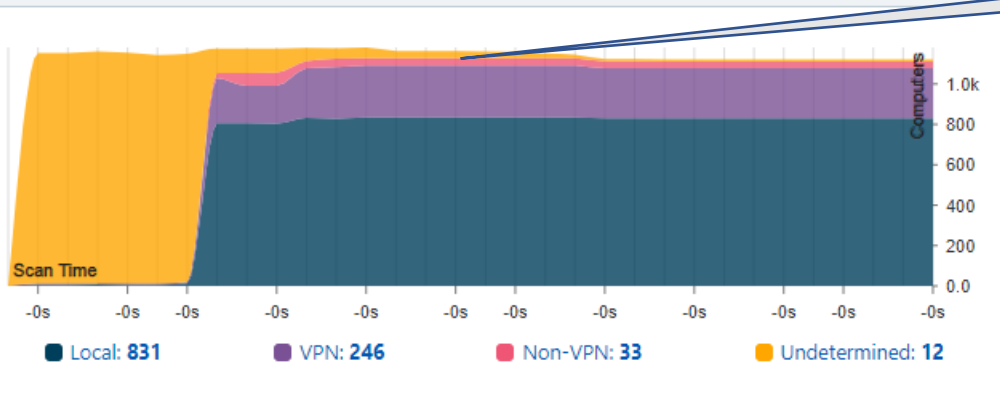
Username and passwords in clear text

Anti-virus inactive or non approved AV applied

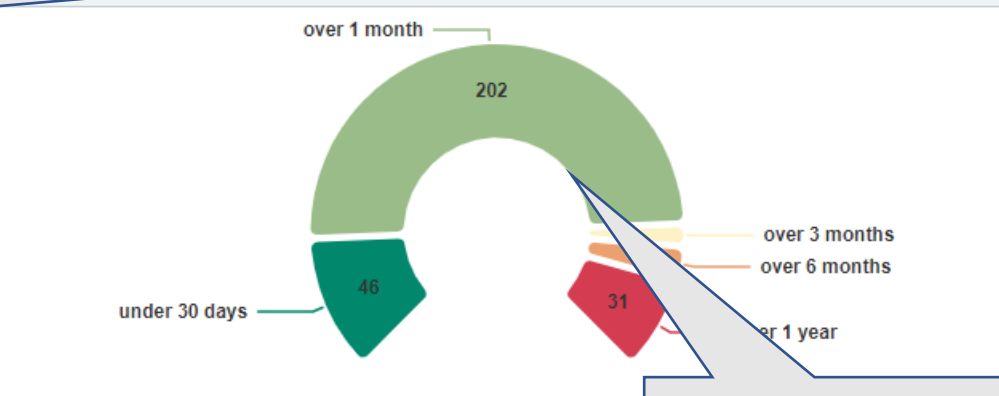
- ENDPOINTS
- Policy Validation
- Misconfigurations
- Remote Employees
- Login Profiler
- GROUP POLICY ACTIVE DIRECTORY
- Security
- Maintenance
- Compliance
- Auditing

Remote Employees

Endpoint Connectivity to Domain

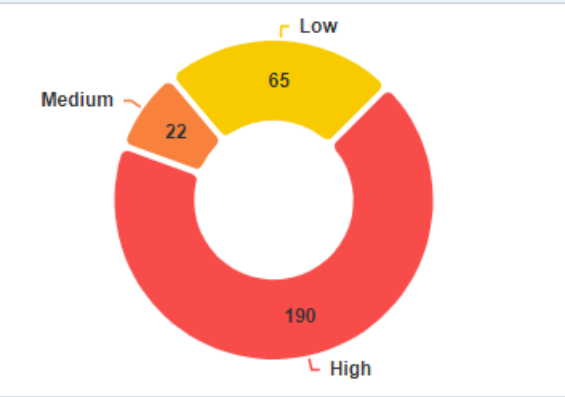


Latest OS Update on Remote Computers

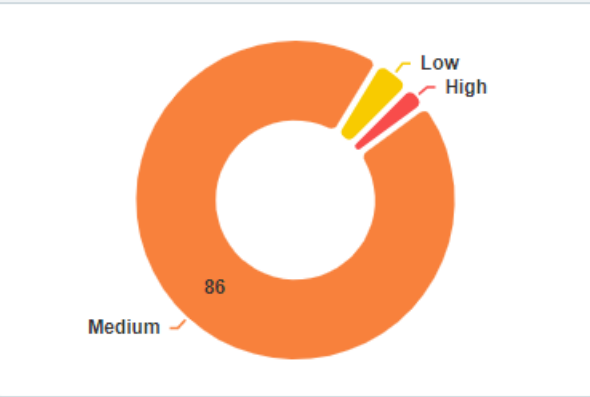


How the endpoint reported

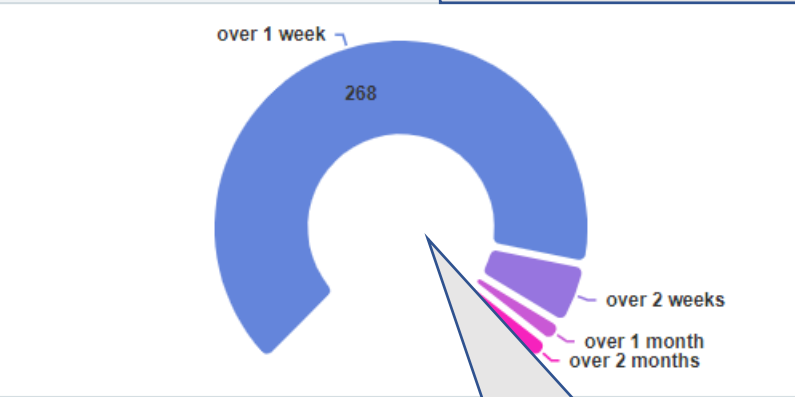
'Computer' Group Policy Violations



'User' Group Policy Violations



Last Policy Refresh on Remote Computer



When latest OS update was applied

Remote Computer Vulnerabilities - Remote Specific Metrics

Severity	Computers	Topic	Subject
Medium	293	Remote Desktop	Remote Desktop service active
Medium	293	Windows Update...	Windows Updates or WSUS are misconfigur...

Remote Computer Vulnerabilities - General Metrics

Severity	Computers	Topic	Subject
High	293	Group Policy Serv...	Group Policy Elevation of Privilege Vulnerab...
High	276	Internet Service	Computer is providing an Internet service

When latest policies were applied

- ENDPOINTS
- Policy Validation
- Misconfigurations
- Remote Employees
- Login Profiler
- GROUP POLICY ACTIVE DIRECTORY
- Security
- Maintenance
- Compliance
- Auditing
- KnowHow

Computers with Policy Alerts by Org. Unit

Org. Unit	Failures	Comput...	GPOs
Win10/Computer-No-AV	219 32 76	197	11
Win10	121 14	123	5
Win10/Computers-NoPolicy	337 1	39	5
UsersGeneral/IT Users	179	10	4
W7-8/Computers-NoPolicy	74	5	4

[View All](#)

Users with Policy Alerts by Org. Unit

Org. Unit	Failures	Users	GPOs
UsersGeneral/Standard-Users/UsersA	13 195 3	140	9
UsersGeneral/Standard-Users/UsersX	319 1	8	9
UsersGeneral/Programmers	11	9	1
UsersGeneral/IT Users	8	2	1
UsersGeneral/HD Users	3	2	1

[View All](#)

Computers with Policy Alerts by GPO

GPO	Failures	Comput...
GP-App	176 7	182
Security-GP	130	130
Local Group Policy	95	84
FW_Log	71	14
Default Domain Policy	13	13

[View All](#)

Users with Policy Alerts by GPO

GPO	Failures	Users
Office 2010	166	124
Old Default Domain Policy	25	22
(see Addl. Info)	16	16
Warning: The setting refers to a non-existing GPO	13	7
GP-App	82	9

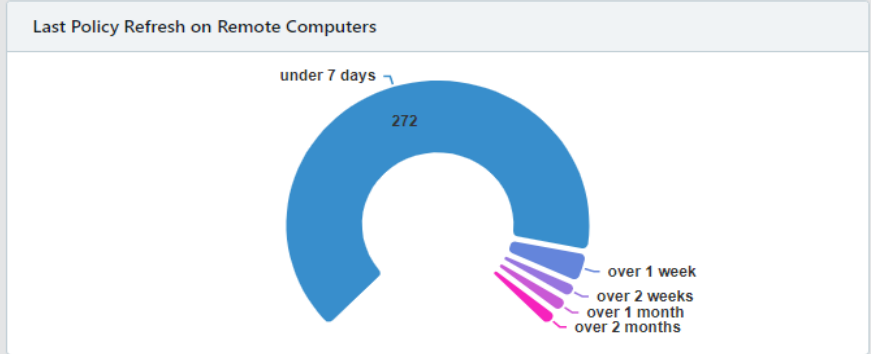
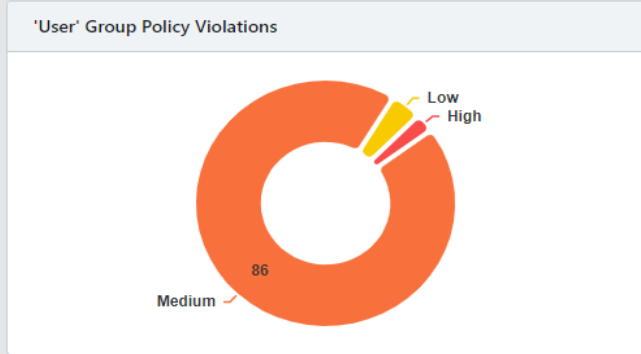
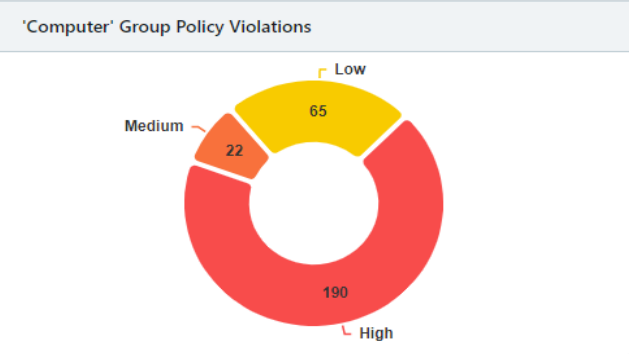
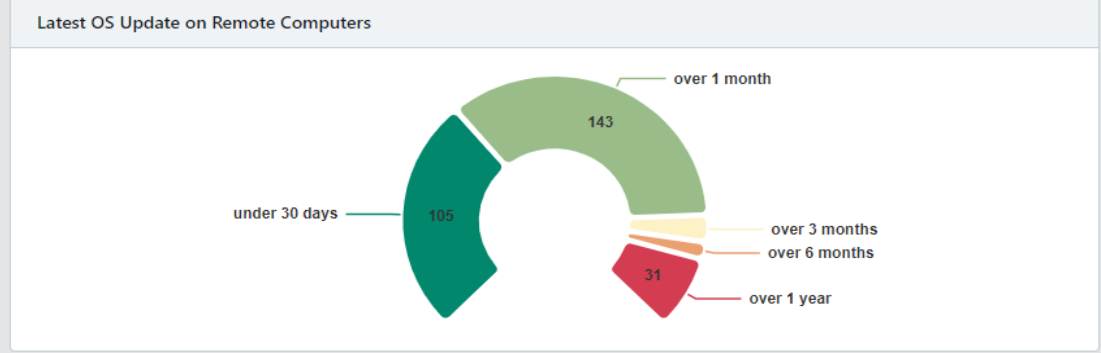
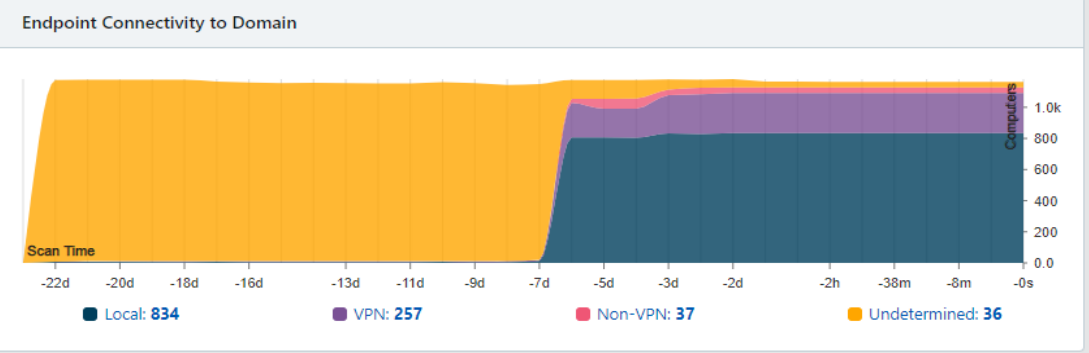
[View All](#)

Computers with Policy Alerts by OS

OS	Failures	Scanned
Windows 10	93 376 50	1056
Windows 7	1411 2	20
Windows Server 2016	2	37
Windows Server 2012	2	24
Windows Server 2008	2	18

- ENDPOINTS
- Policy Validation
- Misconfigurations
- Remote Employees
- Login Profiler
- GROUP POLICY ACTIVE DIRECTORY
- Security
- Maintenance
- Compliance
- Auditing
- KnowHow

Remote Employees



Remote Computer Vulnerabilities - Remote Specific Metrics

Severity	Computers	Topic	Subject
Medium	293	Remote Desktop	Remote Desktop service active
Medium	293	WSUS	Windows Updates are misconfigured
Medium	292	BitLocker	BitLocker disabled on system drive
Medium	262	WiFi Auth	Weak WiFi authentication type
Medium	130	WiFi Pwd	WiFi password is weak
Medium	248	43 Windows Updates	Windows has not been updated in the last 60 days
Medium	284	9 Firewall	Alerts if the "other networks" in the local firewall are on
Complied	293	Proxy	Internet Proxy setting is overridden
Complied	293	SmartScreen	Windows SmartScreen is off or bypassed

Remote Computer Vulnerabilities - General Metrics

Severity	Computers	Topic	Subject
High	293	GpSvc	Group Policy Elevation
High	276	17 Internet Service	Computer is providing an Internet service
High	286	1 Antivirus Inactive	Antivirus engine inactive
Medium	293	Local Admins	Local administrator
Medium	293	TLS / SSL Version	TLS / SSL version has security flaws
Medium	PowerShell Version	PowerShell v2.0 installed and vulnerable	
Medium	287	Device Guard	
Medium	192	101 Intel Management Engine	IME active and puts

Active RDS on endpoints

Is BitLocker available and the disk encrypted

Home WiFi password & encryption strength

ENDPOINTS

- Policy Validation
- Misconfigurations
- Remote Employees
- Login Profiler
- GROUP POLICY ACTIVE DIRECTORY
- Security
- Maintenance
- Compliance
- Auditing
- KnowHow

Endpoint Login Profiler

Worst Computer Startup Times

Computer	Duration	Last Boot
C_SPARE142	871.1s	(invalid)
C_SPARE58	589.7s	(invalid)
C_SRENANAG	536.9s	(invalid)
C_SPARE148	497.3s	(invalid)

Worst User Login Times

User	@ Computer	Duration	Last Lo...
U_mOrnaD	C_MORNAD	537s	(invalid)
U_sNoamS	C_SNOAMS-H	396s	(invalid)
U_mSmadarZ	C_SPARE146	338s	(invalid)
U_mMichalP	C_MMICALP-H	300s	(invalid)

Computer Startup Time by Extension

Extension	GPOs	On	Average Startup Time	Max
Group Policy Infrastructure	12	1124	9.6s	714s
Group Policy Registry	9	1006	1.1s	290s
Group Policy Files	4	1003	1s	38s
Group Policy Passwords	1	1002	0.1s	16s

User Login Time by Extension

Extension	GPOs	On	Average Login Time	Max
Group Policy Infrastructure	19	838	39s	533s
Registry	18	606	3.8s	145s
Group Policy Folders	1	81	3s	14s
Group Policy Registry	16	69	4.2s	14s

Computer Startup Time by Org. Unit

Org. Unit	On	Average Startup Time	Max
Win10	463	8.3s	97s
Win10/Computer-No-AV	361	40s	871s
Win10/Computers-NoPolicy	197	6.8s	41s

User Login Time by Org. Unit

Org. Unit	On	Average Login Time
UsersGeneral/Standard-Users...	636	41s
UsersGeneral/Standard-Users...	149	47s
UsersGeneral/Programmers	12	64s

Worst Endpoint start-up times

Worst User Login-in times

QUESTIONS?

Visit us at gytpol.com



<https://www.linkedin.com/company/gytpol>



<https://twitter.com/gytpol>