caveloFlash

One-time risk assessments designed for prospecting

Accelerate Your Security Service Offering with Cavelo Flash

Demonstrate risk. Drive momentum

Cavelo Flash delivers point-in-time scans for MSPs and MSSPs to prove value to customers and prospects before any commitment -

No agent required

WHY CAVELO FLASH

Stronger Security Conversations

Get a quick snapshot of your prospect and customer's vulnerabilities, misconfigurations, and data risk - without deploying anything.

Get Turnkey, Instant Value

Deliver limited one-time risk assessments for prospecting quickly — no agents, no integrations, no heavy lift.

Accelerate Security Maturity

Demonstrate the value of enhanced security monitoring and services by quickly showing prospects risk in their environment.

Simplify Risk Conversations

Use your prospect/client's data to offer insights into where they stand and what actions are needed to strengthen their security posture.

Powerful risk insights, built for easy prospecting.

Use the QR code to check out more information on Cavelo Flash.

caveloFlash

CAPABILITIES

What to expect

With Cavelo Flash, service providers can quickly evaluate customer environments, showcase actionable risk insights, and open the door to continuous DSPM and ASM through the full Cavelo 360 platform.

Feature	Cavelo Flash	Cavelo 360
Scanning Frequency	Single scan - snapshot in time	Continuous and comprehensive DSPM and ASM capabilities
Deployment	On premises only	On premises and cloud
Reporting	Flash audit report designed for prospecting*	Various customizable reports
Vulnerability Management	Host-based and external vulnerability scanning	Vulnerability management (host-based, internal, external, credentialed, and non-credentialed)
Configuration Management	CIS benchmark scanning for hosts	CIS benchmark scanning for endpoints and cloud with custom baselining
Data Discovery	Data discovery**	Full data discovery with duplicate file detection
Permission Management	No permission management	Permission management — Active Directory compatible
Asset Discovery	No asset discovery	Asset discovery
Compatibility	Compatible with Windows	Compatible with Windows, Linux and Mac (servers and desktops)

*Limited to 20 reports per calendar month, 5 hosts per report

**Limited to local disk only, 100 000 files (or 60 minutes), default PII types (IBAN, passport, SSN, SIN, credit card, AWS key)

cavelo

Cavelo helps MSPs and MSSPs deliver data security posture management (DSPM) services to their customers. Its agent-based platform provides complete visibility of sensitive data, continuous risk assessment and actionable insights that enable MSPs to strengthen security postures, meet compliance mandates, and drive new revenue streams. Built for channel scalability, Cavelo empowers partners to deliver value-added services that address today's most pressing security challenges.

Learn more at **www.cavelo.com**

JANUARY 2026

Flash Audit Report

SAMPLE

Prepared: January 7, 2026

cavelo

Table of Contents

Summary

Flash Status

Source	Domain Scan	External Vulnerability
Organization	✓ Success	! Not Started

Source	Software	PII Inventory	CIS Benchmarks	Vulnerabilities
GSD-E14-002	✓ Success	✓ Success	✓ Success	✓ Success
GSD-TB15-001	✓ Success	✓ Success	✓ Success	✓ Success

Endpoint Vulnerabilities

TotalVulnerabilities 22

9	2	1	8	2
Very Low	Low	Medium	High	Very High

Hostname	Total	Very Low	Low	Medium	High	Very High	Agent Risk
GSD-E14-002	21	9	2	1	8	1	Very High
GSD-TB15-001	1	0	0	0	0	1	Very High

Remote Vulnerabilities

0	0	0	0	0
Very Low	Low	Medium	High	Very High

	Total	Low Severity	Medium	High	Critical	Total Risk
Organization	0	0	0	0	0	None

Host Address	Total	Low Severity	Medium	High	Critical	Host Risk

CIS Benchmarks

	Total	Failed	Passed	Fail Rate	Total Risk
All Benchmarks	898	794	104	88.4%	Very High
Implementation Group 1	275	261	14	94.9%	Very High
Implementation Group 2	740	669	71	90.4%	Very High
Implementation Group 3	745	672	73	90.2%	Very High

Hostname	Total	Failed	Fail Rate	IG1 Fails	IG2 Fails	IG3 Fails	Agent Risk
GSD-E14-002	320	280	87.5%	93.8%	89.7%	89.4%	Very High
GSD-TB15-001	578	514	88.9%	95.5%	90.8%	90.6%	Very High

PII Inventory

All PII Types	Instances	Liability	Total Risk
AWS Key, Bulk Names, SIN, Credit Card	77	$889,372	High

Hostname	PII Types	Instances	Liability	Agent Risk
GSD-E14-002	AWS Key, Bulk Names	58	$886,256	High
GSD-TB15-001	SIN, Credit Card	19	$3,116	Low

Software Inventory

	Total	Vulnerable	Total Risk
Organization	70	2	Very High

Hostname	Total	Vulnerable	Agent Risk
GSD-E14-002	37	2	Very High
GSD-TB15-001	33	0	Very High

Domains

Name	Type	Record Type	Record Value
GSD.com	Domain		
↳ connect.GSD.com	Subdomain	CNAME	GSD-connect-space.so
↳ 104.18.39.141	Host		
↳ 172.64.148.115	Host		
↳ www.GSD.com	Subdomain	CNAME	cdn.webflow.com
↳ 198.202.211.1	Host		

Host Address	City	Country	Open Ports	CVEs
104.18.39.141	San Francisco	United States	13	0
172.64.148.115	San Francisco	United States	13	0
198.202.211.1	Berlin	Germany	13	0

Endpoint Vulnerabilities

GSD-E14-002

TotalVulnerabilities 21

9	Very Low
2	Low
1	Medium
8	High
1	Very High

7.6 CVSS 0.79411 EPSS VulnCheck CISA

WinVerifyTrust Signature Validation Vulnerability

Vulnerability Risk: 3.9 (High)
Associated CVEs: CVE-2013-3900

8.0 CVSS 0.00680 EPSS VulnCheck CISA

Git Symlink Vulnerability in Visual Studio and Git

Vulnerability Risk: 0.8 (Very Low)
Associated CVEs: CVE-2025-48384

4.1 CVSS 0.00123 EPSS

Timing side-channel vulnerability in ECDSA signature computation in Dell BIOS, OpenSSL, Libssl, Libcrypto, Oracle MySQL Server, and Oracle Database Server

Vulnerability Risk: 0.7 (Very Low)
Associated CVEs: CVE-2024-13176

8.8 CVSS 0.00119 EPSS

Use after free vulnerability in Media Stream in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)
Associated CVEs: CVE-2025-13638

8.8 CVSS 0.00119 EPSS

Use after free vulnerability in Digital Credentials in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)
Associated CVEs: CVE-2025-13633

8.8 CVSS 0.00119 EPSS

Multiple vulnerabilities in Google Chrome via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)

Associated CVEs: CVE-2025-13630, CVE-2025-13631, CVE-2025-13632, CVE-2025-13633, CVE-2025-13634, CVE-2025-13720, CVE-2025-13721, CVE-2025-13635, CVE-2025-13636, CVE-2025-13637, CVE-2025-13638, CVE-2025-13639, CVE-2025-13640

8.8 CVSS 0.00089 EPSS

Type Confusion vulnerability in V8 in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)

Associated CVEs: CVE-2025-13630

8.8 CVSS 0.00089 EPSS

Bad cast vulnerability in Loader in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)

Associated CVEs: CVE-2025-13720

8.8 CVSS 0.00088 EPSS

Inappropriate implementation vulnerability in Google Updater in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)

Associated CVEs: CVE-2025-13631

7.5 CVSS 0.00079 EPSS

Race vulnerability in V8 in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.8 (Very Low)

Associated CVEs: CVE-2025-13721

4.3 CVSS 0.00076 EPSS

Inappropriate implementation vulnerability in Split View in Google Chrome or Microsoft Edge via unspecified vectors

Vulnerability Risk: 0.7 (Very Low)
Associated CVEs: CVE-2025-13636

GSD-TB15-001

TotalVulnerabilities 1

0 Very Low	0 Low	0 Medium	0 High	1 Very High

7.6 CVSS 0.79411 EPSS VulnCheck CISA

WinVerifyTrust Signature Validation Vulnerability

Vulnerability Risk: 3.3 (High)

Associated CVEs: CVE-2013-3900

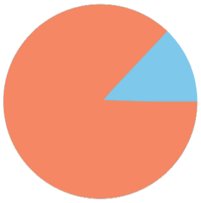
CIS Benchmarks

GSD-E14-002

Total Benchmarks 320

Total Failed280

Total Passed40



Failed Benchmarks

(L1) Ensure "Configure security policy processing: Process even if the Group Policy objects have not changed" is set to "Enabled: TRUE" IG3 IG2 IG1

(L1) Ensure "Windows Firewall: Private: Firewall state" is set to "On (recommended)" IG3 IG2 IG1

(L1) Configure "Accounts: Rename administrator account" IG3 IG2 IG1

(L1) Configure "Accounts: Rename guest account" IG3 IG2 IG1

(L1) Ensure "Interactive logon: Don''t display last signed-in" is set to "Enabled" IG3 IG2 IG1

(L1) Ensure "Interactive logon: Machine inactivity limit" is set to "900 or fewer second(s), but not 0" IG3 IG2 IG1

(L1) Ensure "Interactive logon: Smart card removal behavior" is set to "Lock Workstation" or higher IG3 IG2 IG1

(L1) Ensure "Block user from showing account details on sign-in" is set to "Enabled" IG3 IG2 IG1

(L1) Ensure "Microsoft network server: Server SPN target name validation level" is set to "Accept if provided by client" or higher IG3 IG2 IG1

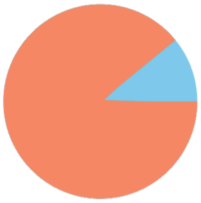
(L1) Ensure "Network Security: Allow PKU2U authentication requests to this computer to use online identities" is set to "Disabled" IG3 IG2 IG1

GSD-TB15-001

Total Benchmarks 578

Total Failed 514

Total Passed 64



Failed Benchmarks

(L1) Ensure "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" is set to "Enabled"	IG3	IG2	IG1
(L1) Ensure "Accounts: Guest account status" is set to "Disabled"	IG3	IG2	IG1
(L1) Configure "Accounts: Rename administrator account"	IG3	IG2	IG1
(L1) Configure "Accounts: Rename guest account"	IG3	IG2	IG1
(L1) Ensure "Interactive logon: Don"t display last signed-in" is set to "Enabled"	IG3	IG2	IG1
(L1) Ensure "Interactive logon: Machine inactivity limit" is set to "900 or fewer second(s), but not 0"	IG3	IG2	IG1
(L1) Ensure "Interactive logon: Smart card removal behavior" is set to "Lock Workstation" or higher	IG3	IG2	IG1
(L1) Ensure "Allow Input Personalization" is set to "Block"	IG3	IG2	IG1
(L1) Ensure "Microsoft network server: Server SPN target name validation level" is set to "Accept if provided by client" or higher	IG3	IG2	IG1
(L1) Ensure "Network Security: Allow PKU2U authentication requests to this computer to use online identities" is set to "Disabled"	IG3	IG2	IG1

GSD-E14-002

Total Liability $886,256

PII Type	Instances	Liability
AWS Credential Key	4	$656
Bulk Names	54	$885,600

C:\Users\PennyBlack\.vscode\extensions\shd101wyy.markdown-preview-enhanced-0.8.18\out\web\extension.js

Data Liability:	$656	**PII Instances:**	4
PII Types:	AWS Key (4)		

C:\Users\PennyBlack\OneDrive - GSD\Channel Daze 2025 Final Lead List.csv

Data Liability:	$16,400	**PII Instances:**	1
PII Types:	Bulk Names (1)		

C:\Users\PennyBlack\OneDrive - GSD\FCTampa2024 List 3.csv

Data Liability:	$16,400	**PII Instances:**	1
PII Types:	Bulk Names (1)		

C:\Users\PennyBlack\OneDrive - GSD\ExcelExport.xlsx

Data Liability:	$16,400	**PII Instances:**	1
PII Types:	Bulk Names (1)		

C:\Users\PennyBlack\OneDrive -GSD\FC Atlanta 2023 Full list.csv

Data Liability:	$16,400	**PII Instances:**	1
PII Types:	Bulk Names (1)		

C:\Users\PennyBlack\OneDrive - GSD\FC Atlanta 2023 Full list.xlsx

Data Liability:	$16,400	**PII Instances:**	1
PII Types:	Bulk Names (1)		

C:\Users\PennyBlack\OneDrive - GSD\Channel Daze Upload 2024.xlsx

Data Liability: $16,400 **PII Instances:** 1

PII Types: Bulk Names (1)

C:\Users\PennyBlack\OneDrive - GSD\FCTampa2024 List 4.csv

Data Liability: $16,400 **PII Instances:** 1

PII Types: Bulk Names (1)

C:\Users\PennyBlack\OneDrive - GSD\IT Nation MSP List - Nov 2024.csv

Data Liability: $16,400 **PII Instances:** 1

PII Types: Bulk Names (1)

C:\Users\PennyBlack\OneDrive - GSD\Channel Daze 2025 Final Lead List FINAL THIS TIME.csv

Data Liability: $16,400 **PII Instances:** 1

PII Types: Bulk Names (1)

GSD-TB15-001

Total Liability $3,116

PII Type	Instances	Liability
Social Insurance Number (Canada)	18	$2,952
Credit Card	1	$164

C:\Users\KathyWalker\OneDrive\Reports\PII 2025-10-02.pdf

Data Liability: $984 **PII Instances:** 6
PII Types: SIN (6)

C:\Users\KathyWalker\OneDrive\Reports\Sensitive Data Report.xlsx

Data Liability: $492 **PII Instances:** 3
PII Types: SIN (3)

C:\Users\KathyWalker\OneDrive\Reports\Sensitive Data Report 2.xlsx

Data Liability: $492 **PII Instances:** 3
PII Types: SIN (3)

C:\Users\KathyWalker\OneDrive\Reports\PII Discovery Report 2025-10-02.csv

Data Liability: $328 **PII Instances:** 2
PII Types: SIN (2)

C:\Users\KathyWalker\OneDrive\Reports\PII Discovery Report 2025-10-02 (1).xlsx

Data Liability: $328 **PII Instances:** 2
PII Types: SIN (2)

C:\Users\KathyWalker\OneDrive\Reports\PII Discovery Report 2025-10-02.xlsx

Data Liability: $328 **PII Instances:** 2
PII Types: SIN (2)

C:\Users\KathyWalker\OneDrive\Receipts\THIRD PARTY CC AUTH FORM.docx

Data Liability:	$164	**PII Instances:**	1
PII Types:	Credit Card (1)		

Software Inventory

GSD-E14-002

TotalApplications 37

Vulnerable Applications 2

Application	Version
Git	2.49.0
↳ *This application is vulnerable* 8.6 0.00710 VulnCheck CISA	
Google Chrome	142.0.7444.177
↳ *This application is vulnerable* 8.8 0.00101	
Level	d72a408
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	10.0.60724
Microsoft 365 Apps for business - en-us	16.0.19426.20170
Microsoft OneDrive	25.216.1104.0002
Microsoft OneNote - en-us	16.0.19426.20170
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.42.34433	14.42.34433
Logi Tune	3.12.193.0
Cavelo Agent	01.0195.0000
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	10.0.60729
Office 16 Click-to-Run Licensing Component	16.0.19029.2020
Office 16 Click-to-Run Extensibility Component	8
Microsoft Teams Meeting Add-in for Microsoft Office	16.0.19426.20170
Adobe Acrobat (64-bit)	1.25.28902
Microsoft Update Health Tools	25.001.20937
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.42.34433	5.72.0.0
Airtame 4.5.2	14.42.34433
Microsoft Edge	4.5.2
	143.0.3650.66

GSD-TB15-001

TotalApplications 33

Vulnerable Applications 0

Application	Version
Level	2314d4a
Microsoft 365 Apps for business - en-us	16.0.19426.20218
Microsoft OneDrive	25.222.1112.0002
Microsoft OneNote - en-us	16.0.19426.20218
Cavelo Agent	01.0195.0000
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.40.33810	14.40.33810
Office 16 Click-to-Run Licensing Component	16.0.19029.20208
Office 16 Click-to-Run Extensibility Component	16.0.19426.20170
Microsoft Teams Meeting Add-in for Microsoft Office	1.25.28902
Adobe Acrobat (64-bit)	25.001.20997
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.40.33810	14.40.33810
Microsoft Update Health Tools	5.72.0.0
Adobe Creative Cloud	6.8.1.856
Adobe Genuine Service	9.1.0.52
Google Chrome	143.0.7499.170
Adobe InDesign 2025	20.5.1
Adobe InDesign 2026	21.1
Lenovo Now	4.0.2.39
Microsoft Edge	143.0.3650.96
Microsoft Edge WebView2 Runtime	143.0.3650.96

Domains

GSD.com

Domain

connect.GSD.com

Subdomain

Type	CNAME
Value	GSD-connect-space.so

104.18.39.141

Location	San Francisco, United States	🇺🇸
Organization	Cloudflare, Inc.	
Internet Service Provider	Cloudflare, Inc.	
Open Ports	80/tcp, 443/tcp, 2052/tcp, 2053/tcp, 2082/tcp, 2083/tcp, 2086/tcp, 2087/tcp, 2095/tcp, 2096/tcp, 8080/tcp, 8443/tcp, 8880/tcp	
Potential Vulnerabilities	None	

172.64.148.115

Location	San Francisco, United States	🇺🇸
Organization	Cloudflare, Inc.	
Internet Service Provider	Cloudflare, Inc.	
Open Ports	80/tcp,443/tcp, 2052/tcp, 2053/tcp, 2082/tcp, 2083/tcp, 2086/tcp,2087/tcp, 2095/tcp, 2096/tcp, 8080/tcp, 8443/tcp, 8880/tcp	
Potential Vulnerabilities	None	

www.GSD.com

Subdomain

Type	CNAME
Value	cdn.webflow.com

198.202.211.1

Location	Berlin, Germany
Organization	Webflow, Inc
Internet Service Provider	Cloudflare London, LLC
Open Ports	80/tcp, 443/tcp, 2052/tcp, 2053/tcp, 2082/tcp, 2083/tcp, 2086/tcp, 2087/tcp, 2095/tcp, 2096/tcp, 8080/tcp, 8443/tcp, 8880/tcp
Potential Vulnerabilities	None