







DOCONTROL

Assessment Report • Jan 27, 2021

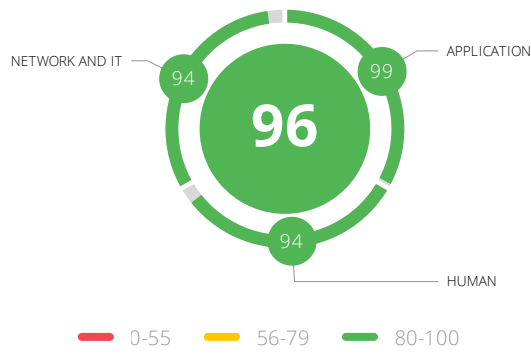
OVERVIEW

DoControl is currently in stealth mode.

- | | |
|--|--|
|  Computer & Network Security |  -- |
|  New York, NY, United States of America |  Privately Held |
|  -- |  1-10 employees |

Cyber Assessment

Cyber Posture Rating

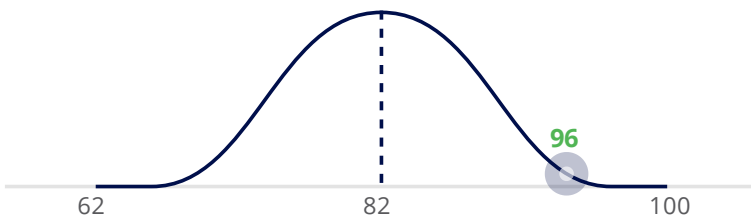


Posture By Categories

Application	99	Human	94	Network and IT	94
Application Security	100	Responsiveness	--	Asset Reputation	100
Domain Attacks	79	Employee Attack Surface	100	Cloud	100
Exposed Services	100	Security Team	100	DNS	75
Technologies	100	Social Posture	67	Mail Server	--
				TLS	95
				Web Server	91

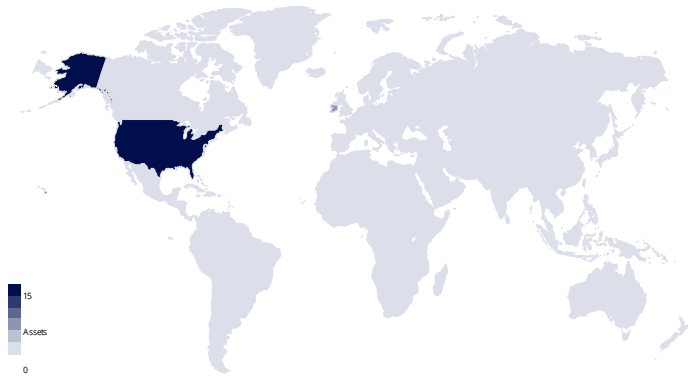
Industry Range

Computer & Network Security

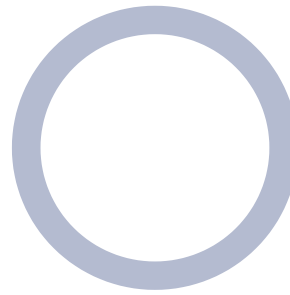


Assets

Geolocation

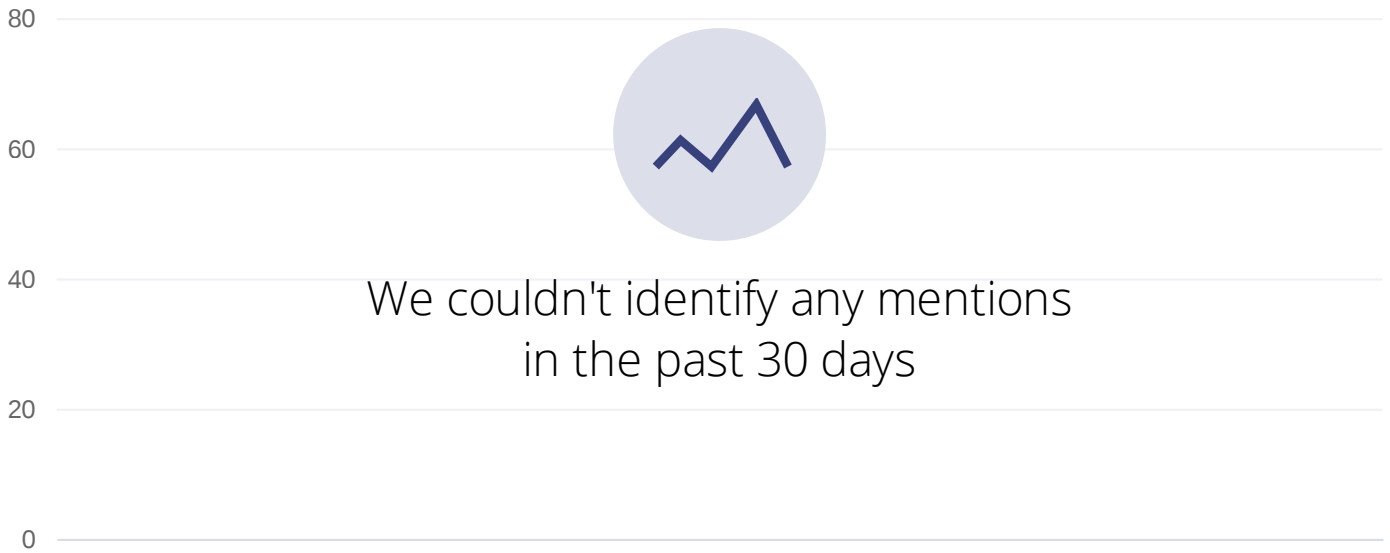


IPs Distribution

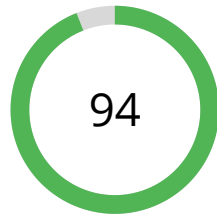


● Amazon.com, Inc. - 18

Dark Web Mentions



Network and IT



- Medium - 7
- Low - 9
- Info - 7

Issues By Sub-Category

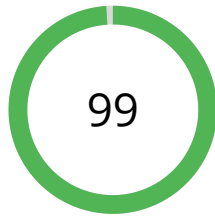
Asset Reputation		100
CRITICAL No Critical severity tests in this section		
HIGH Hosting malicious content N/A		
Hosting phishing sites No Issues		
MEDIUM Flagged as C&C servers No Issues		
Flagged as anonymizers No Issues		
Flagged as spammers No Issues		
Flagged malicious No Issues		
Hosting adult content N/A		
		LOW
		Suspicious URLs N/A
		Suspicious communication samples N/A
		INFO
		No Info severity tests in this section
Cloud		100
CRITICAL No Critical severity tests in this section		
HIGH Cloud private services exposed No Issues		
MEDIUM No Medium severity tests in this section		
		LOW
		Cloud single region No Issues
		INFO
		Cloud bucket hosting website No Issues
DNS		75
CRITICAL DNS zone transfer N/A		
HIGH Open DNS resolver N/A		
MEDIUM No Medium severity tests in this section		
		LOW
		DNS wildcard record No Issues
		DNSSEC configuration 1 issues
		INFO
		No Info severity tests in this section

Mail Server		N/A
<u>CRITICAL</u> No Critical severity tests in this section		
<u>HIGH</u> SPF existence		N/A
<u>MEDIUM</u> DKIM existence DMARC existence		N/A
		<u>LOW</u> DKIM configuration N/A DMARC configuration N/A SPF configuration N/A User enumeration N/A <u>INFO</u> No Info severity tests in this section

TLS		95
<u>CRITICAL</u> TLS vulnerabilities. critical		No Issues
<u>HIGH</u> HTTPS not supported TLS certificate untrusted TLS cipher suite issues. high TLS deprecated protocols TLS vulnerabilities. high		No Issues
<u>MEDIUM</u> Missing HTTP to HTTPS redirect TLS certificate validity too long TLS cipher suite issues. medium TLS unrecommended protocols TLS weak certificate keys		1 issues No Issues 1 issues 1 issues No Issues
		<u>LOW</u> TLS SCTs extension not implemented No Issues TLS certificate chain installation No Issues TLS configuration bad practices No Issues TLS renegotiation issues No Issues TLS vulnerabilities. low 4 issues <u>INFO</u> TLS anonymous authentication No Issues TLS certificate extended validation 6 issues TLS certificate upcoming expiration 1 issues

Web Server		91
<u>CRITICAL</u> No Critical severity tests in this section		
<u>HIGH</u> Missing WAF on significant asset		No Issues
<u>MEDIUM</u> Content-Security-Policy response header Versions exposed in web server headers		3 issues 1 issues
		<u>LOW</u> Missing WAF No Issues Set-Cookie response header No Issues XSS response headers 4 issues <u>INFO</u> No Info severity tests in this section

Application



Issues By Sub-Category

Application Security		100
<u>CRITICAL</u>		
No Critical severity tests in this section		
<u>HIGH</u>		
Insecure SNMP community string	N/A	
Open sensitive NTP commands	N/A	
SSH version 1 protocol	N/A	
Web app cross-frame scripting	No Issues	
Web app cross-site request forgery	No Issues	
Web app cross-site scripting	No Issues	
Web app improper access control	No Issues	
Web app open redirect	No Issues	
WordPress user data exposure	No Issues	
<u>MEDIUM</u>		
Vulnerable SSH MAC algorithms	N/A	
Vulnerable SSH ciphers	N/A	
Vulnerable SSH host-key algorithms	N/A	
Vulnerable SSH key exchange algorithms	N/A	
WordPress user enumeration	No Issues	
<u>LOW</u>		
Unrecommended SSH MAC algorithms	N/A	
Unrecommended SSH ciphers	N/A	
Unrecommended SSH host-key algorithms	N/A	
Unrecommended SSH key exchange algorithms	N/A	
<u>INFO</u>		
No Info severity tests in this section		
Domain Attacks		79
<u>CRITICAL</u>		
No Critical severity tests in this section		
<u>HIGH</u>		
Domain hijacking	No Issues	
<u>MEDIUM</u>		
No Medium severity tests in this section		
<u>LOW</u>		
Domain typosquatting		1 issues
<u>INFO</u>		
Domain upcoming expiration		No Issues

Exposed Services

100

CRITICAL

Exposed database services No Issues

Exposed vulnerable OS services No Issues

HIGH

Exposed cleartext management services No Issues

MEDIUM

Exposed console services No Issues

LOW

Exposed bad practice administration services No Issues

Exposed common gaming services No Issues

Exposed common trojan services No Issues

INFO

No Info severity tests in this section

Technologies

100

CRITICAL

CMS technologies. critical N/A

General technologies. critical N/A

Web application technologies. critical No Issues

Web server technologies. critical No Issues

HIGH

CMS technologies. high N/A

General technologies. high N/A

Web application technologies. high N/A

Web server technologies. high N/A

MEDIUM

CMS technologies. medium N/A

General technologies. medium N/A

Web application technologies. medium N/A

Web server technologies. medium N/A

LOW

CMS technologies. low N/A

General technologies. low N/A

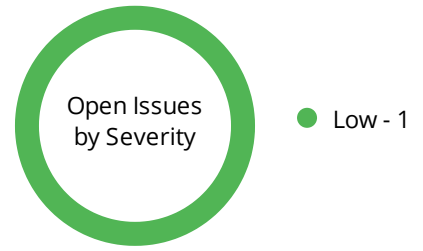
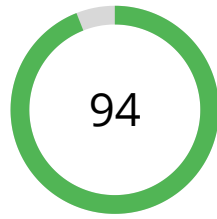
Web application technologies. low N/A

Web server technologies. low N/A

INFO

No Info severity tests in this section

Human



Issues By Sub-Category

Responsiveness N/A	
<p><u>CRITICAL</u> No Critical severity tests in this section</p> <p><u>HIGH</u> No High severity tests in this section</p> <p><u>MEDIUM</u> Critical Findings Resolution N/A Technologies Patching N/A</p>	<p><u>LOW</u> Asset Reputation Resolution N/A</p> <p><u>INFO</u> No Info severity tests in this section</p>
Employee Attack Surface 100	
<p><u>CRITICAL</u> No Critical severity tests in this section</p> <p><u>HIGH</u> No High severity tests in this section</p> <p><u>MEDIUM</u> Employee high attack likelihood No Issues</p>	<p><u>LOW</u> Employee high attack likelihood (top 10) No Issues Employee public digital footprint No Issues Employees in breached account dumps No Issues</p> <p><u>INFO</u> No Info severity tests in this section</p>
Security Team 100	
<p><u>CRITICAL</u> No Critical severity tests in this section</p> <p><u>HIGH</u> No High severity tests in this section</p> <p><u>MEDIUM</u> Presence of CISO No Issues Presence of dedicated information security team No Issues</p>	<p><u>LOW</u> Size of information security team No Issues</p> <p><u>INFO</u> No Info severity tests in this section</p>

CRITICAL

No Critical severity tests in this section

HIGH

No High severity tests in this section

MEDIUM

No Medium severity tests in this section

LOW

Facebook company profile

1 issues

LinkedIn company profile

No Issues

Twitter professional profile

No Issues

INFO

No Info severity tests in this section