

Frontline Cyber Threat Risk Report Card™

Next Generation External Threat Alerts

Every day organizations are under attack. Many of them breached and unaware that their data has been compromised. According to industry reports, the average time to detect a breach is 256 days.

During this time, adversarial individuals are in your network slowly extracting data and using it to further breach your organization, employees or customers.

Solution Overview

Digital Defense's Cyber Threat Risk Report Card is a unique service that offers organizations visibility of their:

- Private employee information
- Intellectual property
- Stolen data
- Breached credentials
- Customer lists

Digital Defense's performs advanced, real-time data collection from the surface, deep and dark webs on behalf of our clients. Our reports offers insight into activity around your organization's digital assets.

Data Collected and Reported

During Digital Defense's research, we look at some critical points of exposure:

- Business Uptime - what is your overall risk of being targeted by hackers
- Access Risk - breaches of accounts or sensitive data
- Communication Risk - reputation of server and email practices
- Business Continuity Risk - hosted unidentified websites on your servers
- Theft & Fraud - website imitation vulnerability
- Publicly Exposed Servers - servers that may be easily accessed for hackers to steal information from

EVIDENCE OF ATTACKS

Technology Attack Surface

- Classless Inter-Domain Routing (CIDR)
- Public IP Space
- SSL Certificates
- Domain Names

Threat Vectors


- Adversary Groups
- Adversarial Online Sources for Monitoring
- Malicious Chatter

IP & Digital Assets

- Credentials
- Source Code
- Customers Lists
- Private Employee Information

Business Update Risk

Risk of being targeted by hackers. This is the most urgent category.




Active Hacking Campaigns 0

Hacktivists and other groups will sometimes advertise their exploits on the dark web.

We searched over **###** websites, forums or other sources to derive this number.

Access Risk

Database breaches containing sensitive information for individuals from your company.




Exposed Accounts 2

Compromised names, email addresses, phone numbers, physical addresses, employer, etc.

We searched over **2 Billion** exposed credentials or other sources to derive this number.

Business Continuity Risk

Sharing a server with other websites.




Websites Hosted With YouWith You 25

More websites hosted on your server increase the chance of an outage.


We searched over **###** websites, forums or other sources to derive this number.

Sample Cyber Threat Risk Report Card:




This Cyber Threat Risk Report Card is a summary of potential threats that could affect your organization. These are raw indicators of concern that require additional research to determine actual exposure and severity. <DATE>

<h4 style="margin: 0;">Intrusion Risk</h4> <p style="font-size: 8px; margin: 0;">Exposed credentials</p> <div style="text-align: right; color: #008080; font-weight: bold; font-size: 16px;">1,312</div> <p style="font-size: 8px; margin: 0;">Attackers who obtain credentials can infiltrate employee personal computers and company systems. These credentials can originate from the company and unrelated internet sites where employees used their company email to create an account.</p> <p style="font-size: 8px; margin: 0; color: #008080;">Over 2 billion records checked</p>	<h4 style="margin: 0;">Fraud Risk</h4> <p style="font-size: 8px; margin: 0;">Illicit domain registrations</p> <div style="text-align: right; color: #008080; font-weight: bold; font-size: 16px;">12</div> <p style="font-size: 8px; margin: 0;">Attackers register fraudulent domains to stealthily perpetrate attacks, fraud and crime with a look of legitimacy. Detecting registrations quickly is key in anticipating and defending these threats.</p> <p style="font-size: 8px; margin: 0; color: #008080;">Tens of millions of registrations checked</p>
<h4 style="margin: 0;">Availability Risk</h4> <p style="font-size: 8px; margin: 0;">Unexpected blacklisting</p> <div style="text-align: right; color: #008080; font-weight: bold; font-size: 16px;">0</div> <p style="font-size: 8px; margin: 0;">Attackers can misappropriate your corporate identity, leading to your legitimate systems being blacklisted on the internet. Your website and email systems may be rendered unavailable to the public, your customers and employees.</p> <p style="font-size: 8px; margin: 0; color: #008080;">Over 120 blacklists checked</p>	<h4 style="margin: 0;">Data Loss/Malware Risk</h4> <p style="font-size: 8px; margin: 0;">Exposure from internet security tools</p> <div style="text-align: right; color: #008080; font-weight: bold; font-size: 16px;">137</div> <p style="font-size: 8px; margin: 0;">Employees may inadvertently expose corporate data by submitting sensitive files to online malware scanning applications. These products can also indicate if malware may already be in your corporate network, and if attackers may be planning attacks targeted to your company.</p> <p style="font-size: 8px; margin: 0; color: #008080;">Millions of files checked</p>
<h4 style="margin: 0;">Vulnerability Risk</h4> <p style="font-size: 8px; margin: 0;">Potential security weaknesses</p> <div style="text-align: right; color: #008080; font-weight: bold; font-size: 16px;">71</div> <p style="font-size: 8px; margin: 0;">Even companies that invest in maintaining strong defenses can miss out of date software or fail to maintain strong configurations. These vulnerabilities are readily available to attackers, giving them a dangerous advantage in penetrating company defenses.</p> <p style="font-size: 8px; margin: 0; color: #008080;">Over 2 billion records checked</p>	<h4 style="margin: 0;">Confidentiality Risk</h4> <p style="font-size: 8px; margin: 0;">Corporate documents discovered online</p> <div style="text-align: right; color: #008080; font-weight: bold; font-size: 16px;">0</div> <p style="font-size: 8px; margin: 0;">Innocent or malicious employees, partners or third parties often post, share or otherwise publish non-public documents online. Exposure of these documents pose the risk of losing sensitive, restricted and proprietary information. Egregious cases amount to reportable data breaches.</p> <p style="font-size: 8px; margin: 0; color: #008080;">Broad-scope internet discovery</p>



For questions about this report or information on our Frontline Cyber Threat Assessment and 24/7 Frontline Cyber Threat Monitoring, please contact us at 888-273-1412 or sales@digitaldefense.com.

Let Us Help Identify Your Weaknesses

Contact us: sales@digitaldefense.com
 For more information visit: www.DigitalDefense.com



Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.