



demo.com

CYBERSECURITY ASSESSMENT

June 21 - June 30

Prepared For:

Sam Doe

Prepared By:

Jesus Vicente



Demo



Demo.com|Analyzed domain



Health Care|Industry



16 | Employees

EXECUTIVE SUMMARY

Demo.com is currently exposed to significant HIPAA-related cybersecurity risks due to unprotected sensitive data, technical control gaps, and partially implemented compliance safeguards. The estimated compliance coverage is ~38%, reflecting key vulnerabilities in data protection, access control, and incident response. Immediate remediation is required to address external data exposure, insider threats, and endpoint risks.

KEY FINDINGS

- **Parked Data Risk:** ~ \$2.5M unprotected PHI/ePHI (9,007 files; 96,186 records)
- **Top Endpoints:**
 - WINDOWS Device: \$1.36M risk
 - LAPTOP: \$593K risk
 - MACBOOK: \$275K risk
- **Technical Gap:** ~ 31% Compliance Gap resolvable with technical controls.
- **Current Compliance Coverage:** ~ 38%
 - Sensitive Files Downloaded: 186
 - Sensitive Files Uploaded to Cloud: 3,853
- **1,188** Total Security Detections
- **1** Suspicious Emails
- **1,048** Public Links
- **136** External Shares
- High Risk Applications
- High Risk Operating Systems

ROADMAP

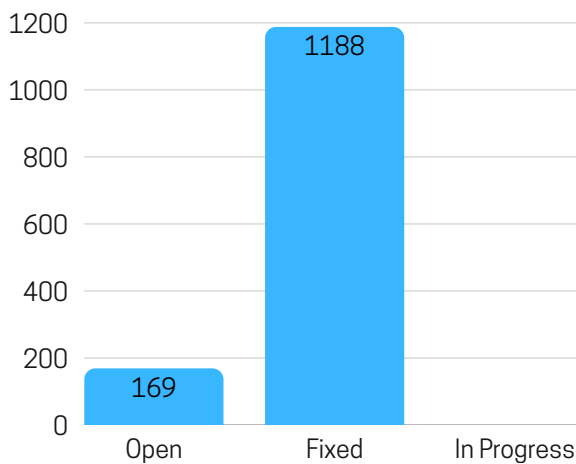
Cyber Attacks cripple businesses. Our service leverages AI and advanced technologies to protect and prevent these attacks, saving you money through reduced downtime and improved IT Security.

Using the combination of Industry Leading and HIPAA compliance as a Framework, Castile Security can provide coverage of the following on an ongoing basis:

- **23 Total Requirements**
 - **11 Technical**
 - **11 Administrative**
 - **1 Physical**



OPEN ISSUES



Critical Open Issues *

- 23 Compliance Requirements
- Sensitive Data Risk
- Anti-Malware Software
- High Risk Software
- High Risk Operating Systems
- Vulnerability Management
- Policy Development

*Criticality based on Compliance Requirements

Recommendations

Our comprehensive managed security service can help Demo.com create a strong foundation for cyber attack protection. We recommend the following:

- 1 Encrypt and Monitor Sensitive Data** - Encrypt and monitor sensitive files across endpoints and cloud services to prevent unauthorized access or data leaks.
- 2 Implement Access Control** - Enforce multi-factor authentication and ensure user access is promptly updated based on employment status.
- 3 Establish Cybersecurity Policies** - Develop HIPAA-compliant security policies and train staff regularly to support secure business operations.

Benefits

- 1 Regulatory Compliance** - Alignment with HIPAA and Industry leading frameworks (NIST).
- 2 Data Protection** - protection from cyber threats like ransomware, malware, and data breaches.
- 3 Cost Effective** - Flexible service tiers to fit your budget while delivering maximum value.
- 4 Reputation and Customer Trust** - Protecting customer data and maintaining trust can provide a competitive advantage.



21 Jun - 21 Jun

Detailed Findings

Demo


 Demo.com | Analyzed domain

 Health Care | Industry

 16 | Employees

This assessment report was prepared by

Castile Security

 8338227845

 castilesecurity.com

 support@castilesecurity.com

SECURED ASSETS

3

IPs & Domains

16

Employees

15 Increase

0

Devices

20

Cloud Drives

16

Mailboxes

0

Browsers

FINANCIAL EXPOSURE

~ \$15,000

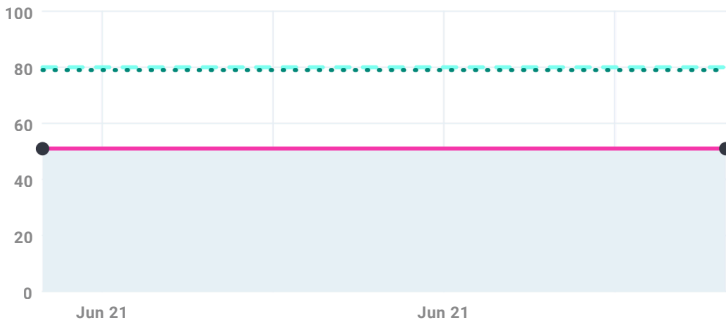
Possible Financial Loss

0% no changes from last period

\$0

Possible Financial Loss- This data estimates potential financial losses based on internal and external scans, user risk, vulnerabilities and overall security posture, factoring in industry, company size, digital assets and attack surface.

SECURITY SCORE



51

Current Score

No Changes

79

Industry benchmark

51

Starting Score

80

Insurance threshold

Security Score- The Security Score is based on coverage (activated security controls) and the volume and severity of issues within each control.



Financial loss due to cybersecurity incidents in Hospital & Health Care

A typical data breach carries an average price tag of 4.5 million but in specific industries can go as high as \$10 million, a clear indicator of the towering financial stakes involved.

Mishandled customer data could lead to hefty regulatory fines across all industries. Regulations such as GDPR, for instance, could impose penalties as severe as €20 million, or 4% of the company's annual global turnover. For example, the 2017 WannaCry ransomware attack caused operational disruptions and financial losses in diverse sectors around the globe.

DETECTIONS & RESPONSES

1,180

Total Detections

0

Fixed

0

Ignored

0

Archived

0

In Progress

1,180

Open

ITDR 0%

Phishing Simulations 0%

Awareness 0%

Cloud Data 0%

Dark Web Monitoring 0%

Endpoint Protection 0%

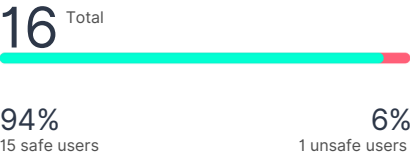
External Footprint Scan 0%

Email Protection 0%

Secure Browsing 0%

User Posture

SAFE VS RISKY USERS

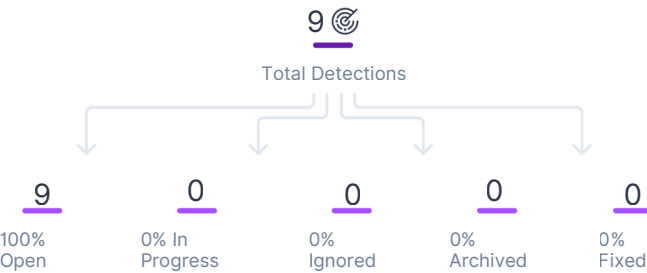


TOP RISKY USERS

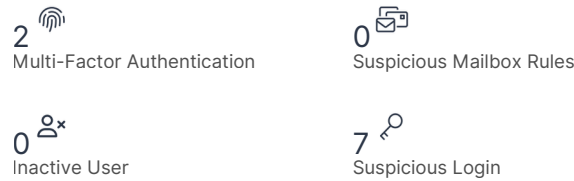
admin@demo.com High

Risky Users- This score for each user is a combination of role, amount of detections and their type and severity.

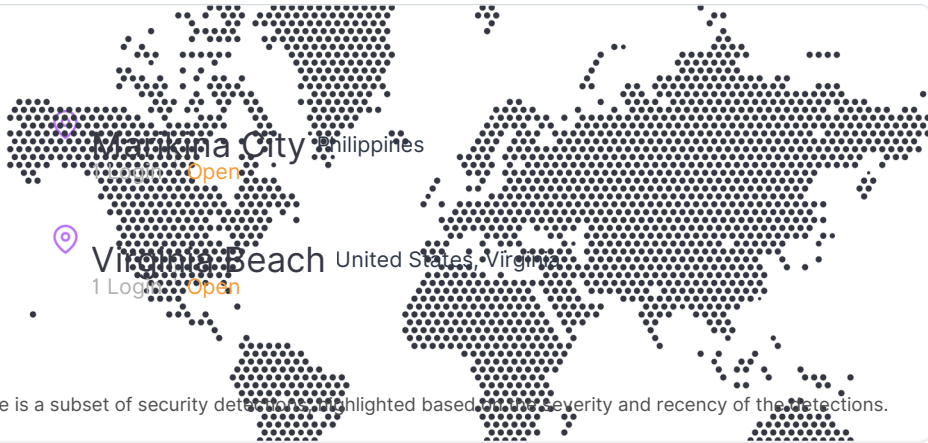
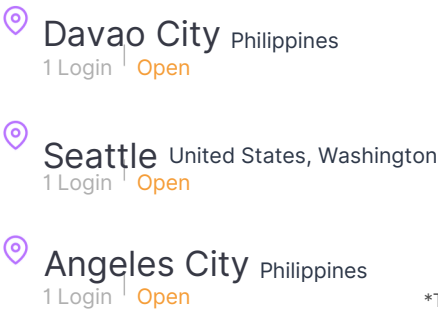
IDENTITY THREAT DETECTION & RESPONSE



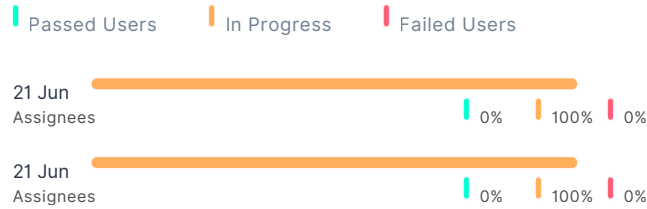
IDENTITY THREAT DETECTIONS BY TYPE



TOP SUSPICIOUS LOGINS



PHISHING SIMULATIONS



MOST FAILED USERS

#

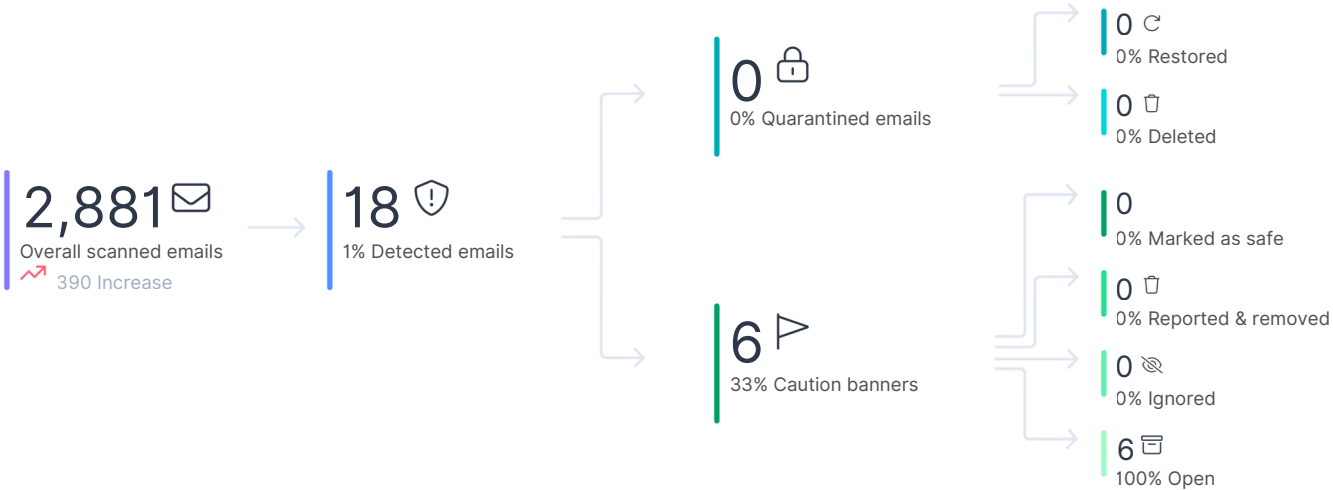
AWARENESS CAMPAIGNS



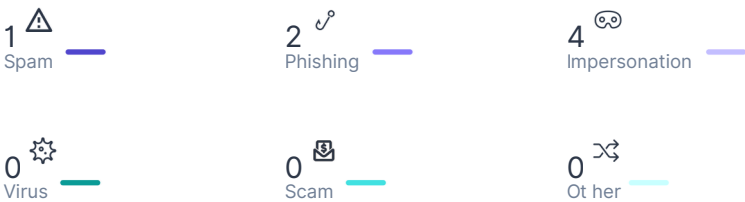
No campaigns to report

Email Protection

DETECTIONS & RESPONSES



ATTACK TYPE BREAKDOWN



TOP TARGETED USERS # of detections



External Assets

RISKY ASSETS

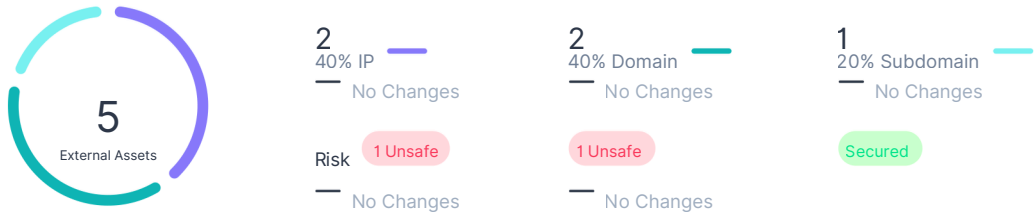
Asset	Type	Geo-Location	Issues
demo.com	Domain	United States	1
192.168.1.1	IP	United States	1
demo.com/test	Domain		
www.demo.com/test	Subdomain	United States	

EXTERNAL FOOTPRINT DETECTIONS & RESPONSES



No detections to report

INTERNET ASSETS TYPES



Cloud Data Protection

