20 FORT DIGITAL SECURITY MEASURES



Fort Digital sets itself apart in the field of security, consistently staying ahead of the competition:

1. Location

Fort Digital Pte Ltd is a wholly 100% Singaporean Company with 100% of its Data and Directors based in Singapore. It uses a private cloud server instead of shared web hosting. Fort Digital employs AWS Private Cloud Server, the highest level of private cloud server available. For more information, visit https://bit.lv/3icEaXR.

2. Two-Factor Authentication (2FA)

Fort Digital is the first Singaporean SMS company to integrate 2FA (Two-Factor Authentication) Login into its web portal using the Google Authenticator App.

3. GeBIZ and Government Supplier

Fort Digital is a GeBIZ Supplier and Government Supplier Expenditure and Policies Procurement Unit (EPPU) No: EPU/CMP/10, EPU/CNE/10 at Financial Grade S7.

4. Server Separation

To minimize risk, Fort Digital separates its services across different servers with separate databases. This approach reduces the risk in the event of a security breach. Their servers and domains include: FortDigital.com.sg (Corporate Portal), MX.FortDigital.net (SMS & WhatsApp), SingaporeQ.com (QMS System), SingaporeRSVP.com (EMS System), SingaporeGuest.com (VMS System).

5. Email Server Separation

Understanding that email is a significant source of malware, spyware, and ransomware, Fort Digital uses a dedicated server for email, hosted by AXAC Pte Ltd.

6. CISCO DUO for Local PC

All local PC, Laptop and Server Login are secured with CISCO DUO and SMS OTP, requiring 2FA for access.

7. OWASP

Fort Digital uses the OWASP ModSecurity Core Rule Set (CRS) as its primary defense against web application attacks, effectively protecting against SQL Injection, Cross-Site Scripting, Local File Inclusion, and more.



8. DDoS Protection

Fort Digital employs Mod Evasive measures to counteract HTTP DoS or DDoS attacks and brute force attacks.

9. IP Whitelisting

The IP Whitelisting feature allows access only from designated IPs, with an Auto Suspend IP function that bans IPs attempting incorrect logins multiple times at the root level.

10. Country Code Whitelisting

This feature allows users to set certain country codes, blocking unauthorized SMS attempts from draining account credits.

11. Set Quota

The Set Quota feature lets users set a daily quota, preventing hackers from exhausting account credits.

12. Disable API

Users can disable API access to ensure security, allowing login only via the Web Portal with Google Authenticator 2FA.

13. Data Retention

Fort Digital does not retain data over 90 days old on live servers, archiving such logs to an offline server to limit the potential for significant data breaches.

14. ZOHO Monitoring

ZOHO monitors the website 24/7, ensuring rapid response to any issues. Live uptime status can be viewed at https://bit.ly/2WslfPa, with uptime consistently at 100%.

15. SSL Protection

All websites are protected with Secure SSL Certificates.

16. Penetration Testing

Regular penetration tests are conducted using various tools, including OWASP ZAP (Zed Attack Proxy).

17. cPHulk Protection

Servers are protected by cPHulk Brute Force Protection, which defends against brute force attacks on various services such as cPanel. WHM. mail services. FTP. and SSH.



18. ImunifyAV

ImunifyAV regularly scans for malware, notifying users of any detections and providing an additional layer of security.



19. IM8 Standard Compliance

Fort Digital strives to comply with stringent Singapore Government IM8 Security requirements and has successfully passed audits by Deloitte.

20. Restricted Staff Access

Access to internal systems and databases is limited to only two core team members.

VAPT and Penetration Test Audited by:

Certified By:

Credentials









Intruder is a member of the Cyber-security Information Sharing Partnership



Intruder is Cyber Essentials certified.



Compliance

Our reports are ISO 27001 and SOC 2 compliance ready.

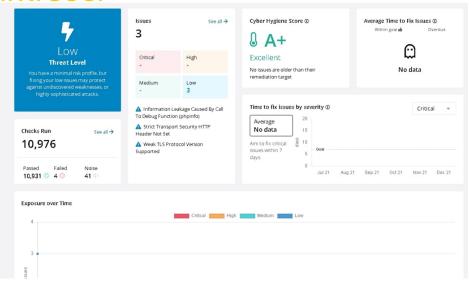
Contact

- <u>
 contact@intruder.io</u>
- www.intruder.io
- in linkedin.com/company/intruder

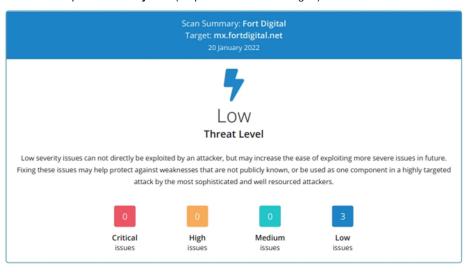
Cyber Hygiene Score as per 20th January 2022 (Request latest from Fort Digital): A+



intruder



Threat Level as per 20th January 2022 (Request latest from Fort Digital): LOW



Penetration Test Items: 10,976 20th January 2022 (Request latest from Fort Digital):

Please request from Fort Digital for Complete List



A SBO Licensed SMS Telecommunication Company

• GeBIZ Supplier and Government Supplier Expenditure and Policies Procurement Unit (EPPU) No: EPU/CMP/10,EPU/CNE/10 @ Financial Grade S7

• SBO License from IMDA (Infocomm Media Development Authority) PDPC/PDPA Compliance

• DigiCert® SSL2 EV3 Certified Company

• The Straits Times 2019 Fastest Growing Company 2019

• Established Since 2007

Legal Name of Company: Fort Digital Pte. Ltd.

Company Registration: 200718585C GST Registration: 200718585C

Email Address: sales@fortdigital.com.sg - support@fortdigital.com.sg

Enquiry Hotline: +65 6484 3863 Fax: +65 6722 8371

WhatsApp Support: +65 8151 5000 (WhatsApp Only)

Place Of Registration: SINGAPORE

Address: Da Jin Factory Building #03-04, 362 Upper Paya Lebar Rd,

Singapore 534963

Operating Hours: 09:00am to 6:00pm (Mon-Fri) , Lunch Time : 01:00pm to 2:00pm

SINGAPORE'S FASTEST- GROWING COMPANIES 2019 Publication Date 27th February 2019

THE STRAITS TIMES

statista 🗹



The Straits Times 2019 Fastest Growing Company 2019, 27th February 2019



Pioneer Company Developed SMS Technology: The Straits Times 25th February 2009