Security Report

Prepared for	Open Research Institute
Website	openresearch.institute
Date	August 1, 2023

at bay

Security Summary

OPEN RESEARCH INSTITUTE

Technology - openresearch.institute

Scanned on August 1, 2023

Resolve issues to unlock best rates and coverages.

▼ 5% below industry average

Required to Bind

0 Critical issue(s)

No issues detected.

May Impact Premium or Terms

4 Important issue(s)

Implement a recommended SEG to protect against email-based attacks
This issue is important and may impact your premium or coverage.

Implement MFA at all sensitive access points to prevent ransomware.
This issue is important and may impact your premium or coverage.

Back up sensitive data to avoid business interruption from ransomware.
This issue is important and may impact your premium or coverage.

Encrypt sensitive data to reduce the impact of a cyber attack.
This issue is important and may impact your premium or coverage.

Action Recommended

5 Moderate issue(s)

Update Nginx End-Of-Life Version on all systems to reduce ransomware exposure.
This issue is moderate and should be resolved to improve security.

Update OpenSSH End-Of-Life Version on all systems to reduce ransomware exposure.
This issue is moderate and should be resolved to improve security.

WHAT AM I AT RISK FOR?

Ransomware - Medium

Data Breach - Medium

Business Interruption - Medium

Financial Fraud - Medium

RANSOMWARE COST ESTIMATE

$23.1K

Calculation based on industry, revenue, and At-Bay data. Try our Ransomware Cost Calculator to estimate the cost of an attack.

at-bay.com/ransomware-calculator

Top Security Issues

Implement a recommended SEG to protect against email-based attacks
A secure email gateway (SEG) is software that protects against phishing and other email-based attacks. Phishing is among the most common methods to initiate a ransomware attack, and an SEG can protect your business by reviewing and blocking malicious emails.

We discovered your organization does not use an SEG on all domains.

Example Domain: openresearch.institute, MX Record: mx2.mailchannels.net.

At-Bay recommendation: Implement a recommended SEG on all email domains to protect against email-based attacks.

For more information, see Email Security.

Implement MFA at all sensitive access points to prevent ransomware.
Multi-factor authentication (MFA) is a security setting that requires users to provide more than one method of verification to gain access. Attackers often use stolen usernames and passwords to access systems and deploy ransomware. Adding an additional verification method that cannot be stolen can help prevent an attack.

We determined your organization does not have MFA implemented at all sensitive access points.

At-Bay recommendation: Implement MFA at all sensitive access points to prevent ransomware.

For more information, see Email Security.

Back up sensitive data to avoid business interruption from ransomware.
Backups are copies of business data. Attackers often encrypt business data in a ransomware attack and demand payment for its release. Restoring data from backups is a reliable solution and helps avoid lost revenue due to business interruption. Without data backups, a business that experiences a ransomware attack can face the difficult decision of whether to pay the ransom or risk greater loss by refusing.

We determined your sensitive data and critical systems are not backed up.

At-Bay recommendation: Back up sensitive data and critical systems to prevent business interruption from ransomware. To ensure your backups address all critical data, audit all data locations to ensure nothing is excluded from the backups.

For more information, see Access Controls.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

CASE STUDY

Capture Rx, a health IT company, reported unusual file activity in February 2021. Patient records with names, birthdates, and prescription details were allegedly compromised, affecting approximately 2.4 million people across 14 hospital systems. The company is now facing a class-action lawsuit.

READ FULL STORY

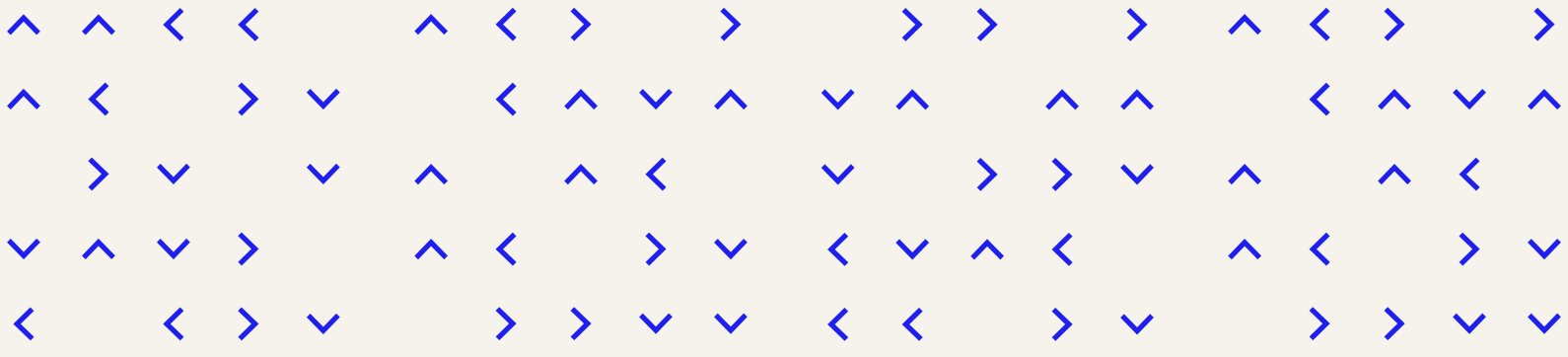
Capture Rx Incident

RECOMMENDED READING

MFA is the Easiest Way to Protect Against Cyber Attacks
at-bay.com/articles/mfa

Follow the 3-2-1 Rule When Creating Data Backups
at-bay.com/articles/data-backups

Security Details



Email Security

01 EMAIL AUTHENTICATION

Implement a recommended SEG to protect against email-based attacks
We discovered your organization does not use an SEG on all email domains. At-Bay recommends implementing a recommended SEG on all email domains to protect against phishing and other email-based attacks. Look for SEG software with these features: anti-malware, anti-spoofing, data loss protection, sandboxing, secure encryption, and threat intelligence and protection

Learn how to implement an SEG

Higher risk SEG vendor MX records:
Domain: openresearch.institute, MX Record: mx2.mailchannels.net.
Domain: openresearch.institute, MX Record: mx1.mailchannels.net.

Implement and configure DMARC records to improve email security.
We discovered at least one of your domains is not protected by DMARC. At-Bay recommends implementing a DMARC record for every domain you own, even those that are not used for email, and configuring the DMARC record in accordance with your email service provider.

Learn how to implement and configure a DMARC record.

Unprotected domains:
Domain: openresearch.institute, mx2.mailchannels.net.
Domain: openresearch.institute, mx1.mailchannels.net.

02 EMAIL TECHNOLOGIES

No issues detected.

03 EMAIL SECURITY

Implement MFA at all sensitive access points to prevent ransomware.
We determined your organization does not have MFA implemented at all sensitive access points. At-Bay recommends implementing MFA for email, internal applications, remote network access, and any external-facing systems. The most common and safest verification method is an authenticator application, such as Google Authenticator, which is recommended over text messages or phone calls. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to implement MFA on Email.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

Implementing and Configuring a DMARC Record
at-bay.com/articles/dmarc

MFA is the Easiest Way to Protect Against Cyber Attacks
at-bay.com/articles/mfa

Remote Access

01 PORTS

No issues detected.

02 VPN

Implement MFA on VPN to prevent ransomware.
We determined your organization does not have MFA implemented on VPN. At-Bay recommends implementing MFA on all systems accessible from the public internet, including VPN. The most common and safest verification method is an authenticator application, such as Google Authenticator, which is recommended over text messages or phone calls. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to implement MFA on VPN.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

How to Implement MFA on VPN
at-bay.com/articles/mfa-vpn

Network Security

01 DATABASE PORTS

No issues detected.

02 OTHER VULNERABILITIES

Update Nginx End-Of-Life Version on all systems to reduce ransomware exposure.

We discovered your organization is running an end-of-life version of Nginx. At-Bay requires upgrading your Nginx to the latest version. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to update Nginx end-of-life.

Servers running End Of Life Nginx Version:
Port: 80/TCP, Domain: mysql.openresearch.institute, IP: 208.113.244.167, Version: 1.18.0
Port: 8088/TCP, Domain: www.sandiego.openresearch.institute, IP: 70.95.76.225, Version: 1.14.2
Port: 10443/TCP, Domain: www.sandiego.openresearch.institute, IP: 70.95.76.225, Version: 1.14.2

Update OpenSSH End-Of-Life Version on all systems to reduce ransomware exposure.

We discovered your organization is running an end-of-life version of OpenSSH. At-Bay requires upgrading your OpenSSH to the latest version. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to update OpenSSH end-of-life.

Servers running End Of Life OpenSSH Version:
Port: 22/TCP, Domain: www.openresearch.institute, IP: 208.113.149.76, Version: 8.2p1
Port: 22/TCP, Domain: lists.openresearch.institute, IP: 69.163.136.34, Version: 8.2p1

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

How to Update Nginx End-Of-Life Version
https://docs.nginx.com/nginx-management-suite/admin-guides/installation/upgrade-guide/

How to Update OpenSSH End-Of-Life Version
https://www.openssh.com/openbsd.html

Access Controls

01 DATA ENCRYPTION

Encrypt sensitive data to reduce the impact of a cyber attack.
We determined the sensitive data stored on your servers and devices is not encrypted. At-Bay recommends encrypting all sensitive data to reduce the potential impact of a cyber attack, including data stored on servers, laptops, mobile devices, and other portable media. We also recommend implementing strong passwords, enabling multi-factor authentication wherever possible, and reinforcing email and cloud encryption.

Learn how to encrypt sensitive data.

02 DATA BACKUPS

Back up sensitive data to avoid business interruption from ransomware.
We determined your sensitive data and critical systems are not backed up. At-Bay recommends creating backups to avoid business interruption in the event of a ransomware attack. To ensure your backups address all critical data, audit every data location to ensure nothing is excluded from the backups. When creating data backups, we recommend following the 3-2-1 Rule: Make 3 copies of the data, store the data across 2 different mediums, and keep 1 copy of the data off-site. To protect against ransomware, make sure the offsite backup is segregated from the business network. At-Bay also recommends performing frequent backups and practicing data restoration to ensure quick resolution in the event of an attack.

Learn how to create data backups.

03 PASSWORD MANAGEMENT

Implement a strong password policy to avoid email compromise.
At-Bay recommends implementing a password policy that follows cyber security best practices, such as prompting employees to use special characters and prohibiting dictionary words. We also recommend forcing employees to change their passwords every 3-6 months to minimize the impact of a potential cyber attack, as well as blocking users after multiple failed password attempts to protect against brute force attacks.

Learn how to implement a strong password policy.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

Encrypting Data Can Minimize the Impact of a Cyber Attack
at-bay.com/articles/data-encryption

Follow the 3-2-1 Rule When Creating Data Backups
at-bay.com/articles/data-backups

How to Implement a Strong Password Policy
at-bay.com/articles/password-policy

Website Security

01 **CERTIFICATES AND SSL**

Update website security certificates to prevent spoofing.
We discovered at least one of your domains has an outdated certificate or is not signed by a CA. At-Bay recommends immediately renewing any expired certificates one month prior to expiration. We also recommend using a certificate from a trusted CA, rather than a self-signed certificate. Self-signed certificates are not vetted in a trustworthy process and cannot be revoked by a CA, and they pose a serious risk when compromised.

Learn how to get a website security certificate.

Domains with self signed certificate:
Domain: www.openresearch.institute

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

How to Implement Website Security Best Practices
at-bay.com/articles/website-security-best-practices

FAQ

01 What does my security score mean?

Your security score reflects the strength of your business' cyber security. Scores range from 0 to 100. A high score means your business already has strong security controls in place, while a low score means the strength of your security can be enhanced.

02 How was my security score calculated?

We conduct a non-invasive security scan of your business to collect data from multiple sources. Your security score is based on the findings of our scan. The findings are divided into five categories: ports, vulnerabilities, email, access controls, and website. Each category is scored separately, though some categories are weighted more heavily than others, and the final total is your security score.

03 What should I do with my security report?

Please review your security report to see all of the potential issues identified by our security scan. Critical issues (labeled red) must be resolved to bind your policy with At-Bay, while Important and Moderate issues (orange and yellow) are recommended improvements from our security team. We also recommend sharing your security report with relevant team members, such as the Chief Information Security Officer (CISO), security teams, and IT vendors.

04 What if the security scan missed an issue?

Your security report only reflects the findings of our security scan, which means the issues are visible from an external view. Your organization may have issues that were not discovered by our scan, and we recommend that you maintain security best practices.

05 How did you source the case study?

The case study referenced in your security report was selected based on similarities to your industry and business size. All of our case studies are compiled using publicly available information, and none of the businesses are current At-Bay customers.

06 What if I need help addressing a security issue?

We encourage you to first read through our Recommended Reading section, which provides information and instructions on how to resolve the issues. You can also find more support articles in our Broker Knowledge Center. If you require more help or have additional questions, please contact our Security Team.

CONTACT OUR SECURITY TEAM

Security Team
security@at-bay.com

Appendix

01 GIVEN DOMAINS

openresearch.institute