Security Report

Prepared for	California Florals
Website	calflorals.com
Date	January 20, 2022

at bay

Security Summary

CALIFORNIA FLORALS

Professional, Scientific, and Technical Services - calflorals.com (+4 other domains)

Scanned on January 20, 2022

Critical issues must be resolved to bind.

▼ 36% below industry average

Required to Bind

2 Critical issue(s)

- **Close all exposed RDP ports to prevent ransomware.**
  This issue is critical and must be resolved to bind your policy.
- **Update software with Log4j patch to prevent ransomware.**
  This issue is critical and must be resolved to bind your policy.

May Impact Premium or Terms

4 Important issue(s)

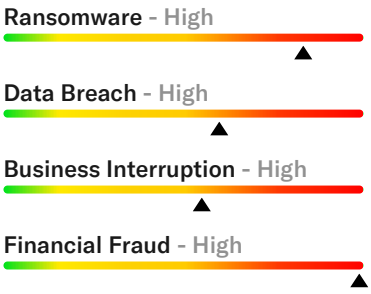
- **Implement an SEG to protect against email-based attacks.**
  This issue is important and may impact your premium or coverage.
- **Implement MFA at all sensitive access points to prevent ransomware.**
  This issue is important and may impact your premium or coverage.
- **Implement MFA on VPN to prevent ransomware.**
  This issue is important and may impact your premium or coverage.
- **Implement and configure SPF records to strengthen email security.**
  This issue is important and may impact your premium or coverage.

Action Recommended

4 Moderate issue(s)

For more information, see Security Details.

WHAT AM I AT RISK FOR?



RANSOMWARE COST ESTIMATE

$254K

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

Close all exposed RDP ports to prevent ransomware.
Remote Desktop Protocol (RDP) is a protocol that allows users to remotely connect to other computers over a network. Compromised RDP is the leading cause of ransomware attacks, and an RDP port that is open externally to the public internet signals easy access to attackers.

We discovered at least one exposed RDP port on your system.

Example Port: 3389, test.calflorals.com, IP: 1.2.3.4

At-Bay requirement: Close all exposed RDP ports to prevent attackers from gaining access to your system. If an open RDP port is necessary for business operations, reinforce it with additional security measures so it is not exposed to the public internet.

For more information, see Remote Access.

Update software with Log4j patch to prevent ransomware.
Log4j is an open source Java library developed and maintained by the Apache foundation. The widely-adopted library is used in many commercial and open-source applications as a logging framework for Java. A serious vulnerability in the Log4j library allows attackers to launch ransomware attacks that can encrypt, destroy, and expose sensitive data.

We discovered that software on your network is vulnerable to the recent Log4j exploit.

Example Domain: test.calflorals.com, IP: 1.2.3.4

At-Bay requirement: Update your organization's software to versions patched for the Log4j vulnerability, in order to prevent attackers from launching a ransomware attack.

For more information, see Network Security.

Implement an 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.

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

For more information, see Email Security.

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

Gustafson & Company, a Portland accounting firm, experienced a malware attack in January 2020. After the company paid for data breach investigation and restoration, the Oregon Department of Justice alleged the company didn't notify consumers in time. The company settled for $50,000 in September 2021.

READ FULL STORY

Gustafson & Company Incident

RECOMMENDED READING

How to Close an Exposed RDP Port
at-bay.com/articles/high-risk-ports/

How to update Log4j
https://www.at-bay.com/articles/security-alert-log4j/

Secure Email Gateway: A Firewall for Your Inbox
at-bay.com/articles/seg

Security Details

Email Security

01 EMAIL AUTHENTICATION

Implement and configure SPF records to strengthen email security.
We discovered at least one of your domains is not protected by SPF. At-Bay recommends implementing an SPF record for all domains, even those that are not used for email. Wherever possible, configure SPF records using the "-all" statement to prevent unauthorized emails. For non-email domains, configure SPF records using the following syntax — "v=spf1 -all" — to improve security.

Learn how to implement and configure an SPF record.

Unprotected domains:
Domain: calflorals.com

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 use 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: calflorals.com

02 EMAIL TECHNOLOGIES

Detected email technologies:
google

Implement an SEG to protect against email-based attacks.
We discovered your organization does not use an SEG on all email domains. At-Bay recommends implementing an 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.

Strengthen Gmail security settings to prevent email compromise.
We discovered your email service provider is Gmail. At-Bay recommends implementing best practices and regular checks to ensure strong security controls are in place, such as using a dedicated administrative account, enabling multi-factor authentication (MFA), and disabling automatic email forwarding. We also recommend reviewing the security settings on a regular basis to ensure they are always up to date.

Learn how to strengthen security settings for Gmail.

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 an SPF Record
at-bay.com/articles/spf

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

Secure Email Gateway: A Firewall for Your Inbox
at-bay.com/articles/seg

Email Security (cont.)

Domains with Gmail:
calflorals.com

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.

Remote Access

01 PORTS

Close all exposed RDP ports to prevent ransomware.
We discovered at least one exposed RDP port on your system. At-Bay requires closing all exposed RDP ports to prevent attackers from gaining access to your system. If an open RDP port is necessary for business operations, hide it behind a secure gateway, such as a virtual private network (VPN), and enable multi-factor authentication (MFA). If you do not have in-house resources to address this vulnerability, please contact your IT provider.

Learn how to close an exposed RDP port.

Exposed RDP ports:
Port: 3389, test.calflorals.com, IP: 1.2.3.4

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 Close an Exposed RDP Port
at-bay.com/articles/high-risk-ports/

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

Network Security

01 DATABASE PORTS

No issues detected.

02 OTHER VULNERABILITIES

Update software with Log4j patch to prevent ransomware.
We discovered that software on your network is vulnerable to the recent Log4j exploit. At-Bay requires updating software with Log4j patches to prevent attackers from gaining access to your network and launching a ransomware attack. If you do not have in-house resources to address this vulnerability, please contact your IT provider.

Learn how to update Log4j

Servers running software vulnerable to Log4j exploit:
Domain: test.calflorals.com, IP: 1.2.3.4

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 Log4j
https://www.at-bay.com/articles/security-alert-log4j/

Access Controls

01 DATA ENCRYPTION

No issues detected.

02 DATA BACKUPS

No issues detected.

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

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 expired certificate:
vpn.calflorals.com
Domains with self signed certificate:
test.calflorals.com
vpn.calflorals.com

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