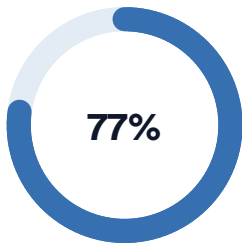


# Q3 2026 Security Review

PREPARED FOR

**Silveroak**



## SECURITY SCORE

Previous Security Score: 57%



PREPARED BY

**IT Pioneers**

28 Sep 2026

# Executive Summary

---

## OVERALL SECURITY POSTURE

---

Silveroak has established a solid security foundation across device protection, identity and access, email security, data protection, and security governance. These established protections support the business's overall security position.

The most significant opportunities for improvement are concentrated in threat monitoring, incident preparedness, access security, and additional email protection. Addressing these areas would strengthen the business's ability to identify and respond to security threats.

## KEY FINDINGS

---

- **Safe Links Policies are not deployed.** No Safe Links policies were found, meaning users do not currently benefit from this additional layer of protection against malicious links delivered by email.
- **Safe Attachments Policies are not deployed.** A Safe Attachments policy has been created but is not protecting any users, leaving a gap in email attachment protection despite the configuration work already completed.
- **Managed Detection & Response (MDR) is not deployed.** Silveroak does not currently have a managed service in place to continuously monitor for threats and respond on the business's behalf, which reduces the ability to identify and contain security incidents quickly.
- **Security Operations Center (SOC), Incident Response, and Privileged Access Management (PAM) are not deployed.** This leaves Silveroak without dedicated managed security operations, a formal incident response capability, and the additional protections provided by privileged access management.
- **Secure Remote Access / VPN is not deployed.** Remote connections to business systems are not protected through a managed secure access solution, which increases exposure when staff work outside the office.

## BUSINESS IMPACT

---

The gaps identified in this review create meaningful exposure across email security, threat detection, and operational resilience. The following areas represent the most significant business consequences.

- **Email Security.** Safe Links Policies and Safe Attachments Policies are not protecting users, meaning malicious email content could reach staff without the additional safeguards these protections provide, increasing the risk of a successful phishing attack or malware infection delivered through email.
- **Threat Detection & Response.** Without Managed Detection & Response (MDR), a Security Operations Center (SOC), or a formal Incident Response capability, Silveroak's ability to identify threats early and respond effectively to a security incident is limited, which could allow an attack to escalate further before it is contained.

- **Privileged Access.** Without Privileged Access Management (PAM), Silveroak lacks the additional protections specifically designed to secure accounts with elevated administrative access. This increases the potential impact of a compromised privileged account, despite the existing identity and access protections already in place.
- **Remote Working:** Without Secure Remote Access / VPN, Silveroak lacks the additional protection provided by a dedicated secure remote access solution. This could increase exposure to unauthorized access when staff connect to business systems from outside the office.

## RECOMMENDATIONS

---

The highest priorities for Silveroak are to address the email protection gaps identified in this review and to strengthen threat monitoring, incident response, and access security across the business.

- **Email Security:** Completing the deployment of Safe Links Policies and Safe Attachments Policies would provide additional protection against malicious email links and attachments, complementing the Mailbox Threat Protection already in place.
- **Threat Monitoring, Incident Response & Access Security:** Upgrading to the Complete Security Plan would strengthen continuous threat monitoring, incident response, privileged access security, and secure remote working. These improvements would help Silveroak identify and respond to threats more effectively while reducing the potential impact of security incidents.

# Understanding Your Security Score

---

Your **Security Score** of **77%** provides a clear snapshot of your current security posture. The score is based on three key areas:

**Coverage:** Measures how many key security controls are in place across your environment. Gaps in essential protections will lower your score and highlight areas that need attention.

**Risk:** Focuses on the most critical security items. Missing or partially implemented high-risk protections will have a significant impact on your score and should be prioritized.

**Governance:** Evaluates documented policies, user training, and recognized security frameworks to help ensure your security program is consistent and aligned with industry best practices.

Each Security Review Item is assessed as **Deployed**, **Partially Deployed**, or **Not Deployed**. Partially deployed controls contribute proportionally to your score, while any items marked as **Not Applicable** are excluded from the calculation.

Your Security Score provides an overall view of your current security posture, while the detailed findings in this report highlight the most important gaps and opportunities for improvement.

Addressing the identified gaps will improve your Security Score and help strengthen your organization's overall security posture.

We recommend reviewing these findings with your Account Manager to prioritize the most impactful next steps.

# Security Findings

|                                                                                                                                                                                                                                                                                                                                                                                        |                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <div><div>Essential Security</div><div>Provides the core security controls every organization should have in place to protect users, devices, email, and business data against common cyber threats.</div></div>                                                                                                                                                                       |                                            |
| <div><div>Endpoint Detection &amp; Response (EDR)</div><div>Continuously monitors computers and laptops to detect and respond to suspicious activity.</div><div><div>BENEFIT</div><div>Helps identify and contain threats before they can spread across your organization.</div></div><div><div>FRAMEWORK</div><div>NIST · DETECT · Continuous Monitoring · DE.CM-09</div></div></div> | <div><div>●</div><div>Deployed</div></div> |
| <div><div>Endpoint Patch Management</div><div>Automatically installs security updates and software patches on computers and laptops.</div><div><div>BENEFIT</div><div>Helps reduce security vulnerabilities by keeping devices up to date.</div></div><div><div>FRAMEWORK</div><div>NIST · PROTECT · Platform Security · PR.PS-02</div></div></div>                                    | <div><div>●</div><div>Deployed</div></div> |
| <div><div>Hard Disk Encryption</div><div>Encrypts data stored on computers and laptops to protect it from unauthorized access.</div><div><div>BENEFIT</div><div>Helps keep sensitive business data secure if a device is lost or stolen.</div></div><div><div>FRAMEWORK</div><div>NIST · PROTECT · Data Security · PR.DS-01</div></div></div>                                          | <div><div>●</div><div>Deployed</div></div> |
| <div><div>Web Protection / DNS Filtering</div><div>Blocks access to malicious, unsafe, or inappropriate websites on computers and laptops.</div><div><div>BENEFIT</div><div>Helps protect employees from online threats and reduces the risk of malware infections.</div></div></div>                                                                                                  | <div><div>●</div><div>Deployed</div></div> |

Mailbox Threat Protection

● Deployed

Protects mailboxes from malware, malicious attachments, and other advanced email threats.

BENEFIT Helps reduce the risk of cyber-attacks delivered through email.

Cloud Data Backup

● Deployed

Automatically backs up cloud-based business data.

BENEFIT Helps restore important business data quickly following accidental deletion, cyber-attacks, or service disruptions.

FRAMEWORK NIST · PROTECT · Data Security · PR.DS-11

Password Manager

● Deployed

Securely stores and manages passwords for business accounts and applications.

BENEFIT Reduces the risk of weak or reused passwords while making it easier for employees to sign in securely.

FRAMEWORK NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-01

## Advanced Security

Builds on the core security foundation with enhanced identity, endpoint, and email protection to reduce cyber risk and improve your overall security posture.

### Adaptive / Risk-Based Multi-Factor Authentication (MFA)

● Deployed

Applies additional identity verification when unusual or high-risk sign-in activity is detected.

|           |                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------|
| BENEFIT   | Provides stronger protection against account compromise while minimizing disruption for legitimate users. |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-03                       |

### Email Authentication (DKIM/DMARC/SPF)

● Deployed

Uses standard email authentication protocols to help verify that emails are sent from authorized sources.

|         |                                                                        |
|---------|------------------------------------------------------------------------|
| BENEFIT | Reduces the risk of fraudulent emails impersonating your organization. |
|---------|------------------------------------------------------------------------|

### Dark Web Monitoring

● Deployed

Monitors for business email addresses and passwords that may have been exposed online.

|           |                                                                                                |
|-----------|------------------------------------------------------------------------------------------------|
| BENEFIT   | Provides early warning of compromised credentials so they can be secured before being misused. |
| FRAMEWORK | NIST · IDENTIFY · Risk Assessment · ID.RA-02                                                   |

### Email Encryption

● Deployed

Encrypts email content to protect sensitive information during transmission.

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| BENEFIT   | Keeps confidential business information secure when shared by email. |
| FRAMEWORK | NIST · PROTECT · Data Security · PR.DS-02                            |

Secure Print Management

● Deployed

Controls how business documents are printed and accessed.

- BENEFIT

Helps protect sensitive documents and reduces the risk of unauthorized printing.
- FRAMEWORK

NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-05

Security Training for Staff

● Deployed

Educates employees on cybersecurity risks, common threats, and safe security practices.

- BENEFIT

Helps reduce the risk of human error by enabling employees to recognize and respond to cyber threats with confidence.
- FRAMEWORK

NIST · PROTECT · Awareness and Training · PR.AT-01

### Complete Security

Delivers a comprehensive, enterprise-grade security solution with continuous threat monitoring, advanced protection, and rapid incident response for maximum resilience against evolving cyber threats.



### Upgrade to the Complete Security Plan

Upgrade to the Complete Security Plan for comprehensive protection, combining advanced security controls, continuous threat monitoring, and expert response to help safeguard your business.

+17% pts

SECURITY SCORE

5

GAPS CLOSED

Learn More



### Managed Detection & Response (MDR)

● Not Deployed

Provides expert monitoring, threat detection, investigation, and response around the clock.

|           |                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| BENEFIT   | Provides continuous expert monitoring and response to help identify and contain threats quickly.                                                       |
| ADVICE    | Escalate to management                                                                                                                                 |
| FRAMEWORK | NIST · DETECT · Adverse Event Analysis · DE.AE-02<br>NIST · DETECT · Continuous Monitoring · DE.CM-09<br>NIST · RESPOND · Incident Analysis · RS.AN-03 |

### Security Operations Center (SOC)

● Not Deployed

Provides 24/7 monitoring and response to potential security threats.

|           |                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------|
| BENEFIT   | Helps identify and respond to cyber threats quickly, reducing the risk of business disruption.        |
| FRAMEWORK | NIST · DETECT · Adverse Event Analysis · DE.AE-02<br>NIST · DETECT · Continuous Monitoring · DE.CM-09 |

Incident Response

● Not Deployed

Provides expert support to investigate, contain, and recover from cybersecurity incidents.

|           |                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BENEFIT   | Helps minimize business disruption and restore normal operations as quickly as possible.                                                                         |
| FRAMEWORK | NIST · RESPOND · Incident Analysis · RS.AN-03<br>NIST · RESPOND · Incident Mitigation · RS.MI-01<br>NIST · RECOVER · Incident Recovery Plan Execution · RC.RP-02 |

Secure Remote Access / VPN

● Not Deployed

Provides secure remote access to business systems and resources from any location.

|           |                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------|
| BENEFIT   | Helps employees work securely from anywhere while reducing the risk of unauthorized access.                   |
| FRAMEWORK | NIST · PROTECT · Data Security · PR.DS-02<br>NIST · PROTECT · Technology Infrastructure Resilience · PR.IR-01 |

Privileged Access Management (PAM)

● Not Deployed

Secures and controls access to accounts with elevated administrative privileges.

|           |                                                                                        |
|-----------|----------------------------------------------------------------------------------------|
| BENEFIT   | Reduces the risk of unauthorized changes and helps protect your most critical systems. |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-05    |

## Security Configurations

Security configurations are technical settings that help strengthen your security posture by enforcing security policies, restricting access, and reducing the risk of compromise.

### Multi-Factor Authentication (MFA) Enforcement

● Deployed

Ensures multi-factor authentication is enabled for all applicable user sign-ins.

|           |                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| BENEFIT   | Helps protect user accounts from unauthorized access, even if passwords are compromised.                                                                 |
| NOTES     | Additional sign-in verification is required for all users through 3 Conditional Access policies, helping protect user accounts from unauthorized access. |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-03                                                                      |

### Conditional Access Policies

● Deployed

Controls access to business applications based on identity, device, and sign-in conditions.

|           |                                                                                                                                                                                                                                   |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BENEFIT   | Helps ensure only trusted users and devices can access business data.                                                                                                                                                             |
| NOTES     | 4 Conditional Access policies are enabled: Require multifactor authentication for admins, Block legacy authentication, Require multifactor authentication for all users, Require multifactor authentication for Azure management. |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-05                                                                                                                                               |

### Legacy Authentication Disabled

● Deployed

Disables outdated sign-in methods that do not support modern security protections.

|           |                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------|
| BENEFIT   | Reduces the risk of attackers exploiting older, less secure authentication methods.                      |
| NOTES     | Older sign-in methods are blocked for all users, helping protect user accounts from unauthorized access. |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-03                      |

Device Compliance Policies

● Deployed

Requires devices to meet security requirements before accessing business resources.

|           |                                                                                     |
|-----------|-------------------------------------------------------------------------------------|
| BENEFIT   | Helps prevent unsecured or non-compliant devices from accessing company data.       |
| NOTES     | 10 of 10 managed devices meet your organization's security requirements.            |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-05 |

BitLocker Enforcement

● Deployed

Ensures supported computers and laptops use full disk encryption to protect stored data.

|           |                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------|
| BENEFIT   | Helps protect sensitive business information if a device is lost or stolen.                                                 |
| NOTES     | 10 of 10 managed Windows devices have disk encryption enabled, helping protect business data if a device is lost or stolen. |
| FRAMEWORK | NIST · PROTECT · Data Security · PR.DS-01                                                                                   |

Safe Links Policies 

● Not Deployed

Automatically checks web links in emails and blocks access to malicious websites.

|         |                                                                                                                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------|
| BENEFIT | Helps protect users from phishing attacks and malicious websites.                                                                            |
| ADVICE  | Prioritize for next quarter                                                                                                                  |
| NOTES   | No Safe Links policies were found. This additional layer of protection against malicious links delivered by email is not currently in place. |

Safe Attachments Policies 

● Not Deployed

Checks email attachments for dangerous files before they reach users.

|         |                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------|
| BENEFIT | Helps stop harmful files and viruses from reaching users through email.                                      |
| ADVICE  | Prioritize for next quarter                                                                                  |
| NOTES   | Safe Attachments policies have been created (1 configured), but they are not currently protecting any users. |

External Sharing Restrictions

● Deployed

Controls how files can be shared with people outside your organization.

|           |                                                                                       |
|-----------|---------------------------------------------------------------------------------------|
| BENEFIT   | Helps reduce the risk of sensitive business information being shared inappropriately. |
| NOTES     | External file sharing is allowed only for authenticated external users.               |
| FRAMEWORK | NIST · PROTECT · Identity Management, Authentication, and Access Control · PR.AA-05   |

## Certifications & Frameworks

Certifications and frameworks help demonstrate your organization's commitment to security, compliance, and industry best practices.

### NIST Cybersecurity Framework (CSF) Assessment

● Deployed

Assesses the organization's cybersecurity practices against the NIST Cybersecurity Framework to identify gaps, risks, and areas for improvement.

|         |                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------|
| BENEFIT | Helps identify gaps in your cybersecurity practices and prioritize improvements using a recognized framework. |
| NOTES   | An assessment was carried out last month.                                                                     |

## FRAMEWORK ALIGNMENT

Framework alignment is based on the Security Review items included in this report. It is provided for guidance only and does not represent a complete framework assessment, compliance assessment or certification.

# Changes Since Last Review



Compared with the previous Security Review, Silveroak's overall security posture has improved significantly. A substantial number of important security measures have been introduced or completed since the last review, reducing business risk across several key areas. Some recommendations remain outstanding and are highlighted below, representing the next priority areas for the business to address.



## Improvements

- **Endpoint Detection & Response (EDR):** Endpoint protection has been strengthened with the deployment of SentinelOne Singularity across all devices, providing advanced threat detection and response capabilities to help protect the business from cyberattacks.
- **Adaptive / Risk-Based Multi-Factor Authentication (MFA):** Duo has now been deployed across the organization, adding an intelligent layer of identity verification that adapts to user behavior and reduces the risk of unauthorized account access.
- **Email Authentication (DKIM/DMARC/SPF):** Email authentication controls are now in place via DMARCLY, helping to prevent cybercriminals from impersonating your business domain and protecting both staff and customers from phishing and spoofing attacks.
- **Dark Web Monitoring:** Constella Dark Web Monitoring has been deployed, providing ongoing surveillance of criminal marketplaces and alerting the business if credentials or sensitive information linked to your organization are found to be exposed.
- **Email Encryption:** Mailbox encryption is now in place, ensuring that sensitive emails are protected in transit and reducing the risk of confidential business communications being intercepted.
- **Secure Print Management:** PaperCut has been deployed, bringing oversight and control to your print environment and reducing the risk of sensitive documents being left unattended or accessed by unauthorized individuals.
- **Security Training for Staff:** Proofpoint Security Training for Staff has been introduced, equipping employees with the knowledge to recognize and respond to common cyber threats such as phishing - one of the most effective defenses a business can invest in.
- **Device Compliance Policies:** All ten managed devices now meet the organization's security requirements, meaning only devices that satisfy your security standards are permitted access to business resources.

- **BitLocker Enforcement:** Disk encryption is now active on all ten managed Windows devices, ensuring that business data remains protected if a device is ever lost or stolen. This control was previously not applicable as no managed Windows devices were found, but has now been fully implemented following the addition of managed devices.
- **External Sharing Restrictions:** External file sharing has been tightened so that shared content is accessible only to authenticated external users, reducing the risk of sensitive business files being accessed by unintended recipients.
- **NIST Cybersecurity Framework (CSF) Assessment:** A NIST Cybersecurity Framework assessment was completed last month, providing the business with a structured understanding of its security posture against a recognized international standard.



### Outstanding Risks

- **Managed Detection & Response (MDR):** A managed detection and response service has not yet been implemented. Without this, there is no dedicated capability to continuously monitor for, investigate, and respond to threats on the business's behalf around the clock.
- **Security Operations Center (SOC):** A Security Operations Center has not yet been established. This leaves the business without a centralized function for ongoing security monitoring and threat management, increasing the time it may take to detect and contain an incident.
- **Incident Response:** A formal incident response capability has not yet been put in place. Without a defined plan and process, the business may be unprepared to respond effectively if a security incident occurs, potentially increasing its impact and recovery time.
- **Secure Remote Access / VPN:** A secure remote access solution has not yet been deployed. This means remote connections to business systems may not be adequately protected, posing a risk to sensitive data and internal resources.
- **Privileged Access Management (PAM):** Privileged access management has not yet been implemented. Without controls over high-level administrative accounts, there is an elevated risk of unauthorized access to critical business systems and data.



### Newly Identified Concerns

- **Safe Links Policies:** This item has been assessed for the first time in this review. No Safe Links policies were found, meaning this additional layer of protection against malicious links delivered by email is not currently in place.
- **Safe Attachments Policies:** This item has been assessed for the first time in this review. One Safe Attachments policy has been configured, but it is not currently protecting any users. The policy requires further configuration to provide the intended additional protection against malicious email attachments.