



**SOC 2
TYPE II
CERTIFIED**



SOURCEPASS™

Guide to Managed Security

Stay secure, compliant, and vigilant.

Considering Outsourcing Your
Cybersecurity? See What
Managed Security Entails in This
Guide.



Managed Advanced Security Services

Empower Your Business with Advanced Security

Enhanced Protection, Reduced Risk, Seamless Management

Our Managed Advanced Security Services includes all Managed Security Services, plus additional services to further enhance your security posture.

These include 24x7x365 threat monitoring and response backed by our powerful SIEM platform, advanced endpoint protection, and detailed vulnerability scanning to meet compliance and insurance requirements.

Our cybersecurity professionals closely monitor your IT environment providing robust, around the clock oversight, rapid response to threats, and timely communication to keep your business safe.

24x7x365 SOC Monitoring

For Endpoints, Network, & Cloud

Our Security Operations Center (SOC) focuses on threat detection, response, and improving prevention capabilities by unifying and coordinating cybersecurity technologies and operations.

SIEM Platform & Threat Monitoring

For Endpoints, Network, & Cloud

Our Security Information & Event Management (SIEM) solution captures and analyzes data that enters your network to catch malicious threats that bypassed other preventative cybersecurity solutions.

Application Allowlisting & Ring Fencing, Endpoint Elevation Control

Provides control of which applications are permitted to run on all workstations and servers to fortify your business, prevent unauthorized access, reduce attack surfaces, and ensure secure, controlled user privileges.

Monthly Vulnerability Scanning

Identifies and mitigates security weaknesses, protecting your business from potential threats and ensuring compliance.

Cloud Backup & Data Protection

Powered by Acronis



Protect against data loss and costly downtime.

Data is the lifeblood of any modern business, and protecting that critical asset is of paramount importance. Data loss can be caused by security threats, device failures, theft, or simple human error.

Data loss resulting in downtime can put the business at significant risk, endangering your reputation with clients, vendors, and employees.

- ✓ 67% of ransomware targets are small and mid-sized firms
- ✓ 60% of companies who experience significant data loss shut down within six months
- ✓ 50% of companies experienced 8+ hours of downtime in the past year

Data protection for all of your platforms.

Our data protection platform, powered by Acronis, targets key areas throughout your company to ensure data, devices and critical business applications are protected.

The Acronis Cloud Backup platform protects data in Microsoft 365, Google Workspace, Mac, Linux, and Windows devices with advanced options for applications and recovery methods.

Our comprehensive approach protects your company against emerging security threats, equipment failure, and user error to ensure your data and applications remain available.



Keep your critical data safe from accidental deletion, malware attacks, and cyber threats



Protect everything from files and folders to individual email attachments



Restore data as needed in seconds, avoiding downtime and ensuring business continuity



Meet cyber insurance and industry compliance requirements

Compliance Support

Secure, Efficient, & Trustworthy Business Environments

Supporting Clients with Compliance Needs

As part of our Security Advisory Services, Sourcepass's team of cybersecurity experts provide support for various compliance (i.e., NIST, CIS, HIPAA, etc.) environments.

With expert guidance and deep technical expertise, we help ensure data security while mitigating legal and financial risks, helping clients avoid penalties and protect sensitive information. Our compliance services enhance operational efficiency and allow clients to build trust with customers by demonstrating a commitment to ethical practices and regulatory adherence.

Key Benefits

- ✓ **Regulatory Adherence:** Provide guidance on navigating complex regulatory landscapes, to ensure all necessary compliance requirements are met and hefty fines are avoided.
- ✓ **Risk Management:** Provide ongoing monitoring and assessments to identify and mitigate compliance risks, helping businesses maintain a secure and compliant environment.
- ✓ **Expertise & Resources:** Provide expert guidance and support with specialized knowledge, staying updated on the latest regulatory changes and best practices to ensure compliance.
- ✓ **Continuous Monitoring & Reporting:** Provide continuous monitoring and reporting services to ensure ongoing compliance. This includes regular audits, vulnerability assessments, and real-time alerts for any compliance issues, helping businesses stay proactive rather than reactive.
- ✓ **Data Protection & Privacy:** Implement robust security measures to protect sensitive data, ensuring that businesses comply with data protection laws and safeguard their customers' information.
- ✓ **Trust with Customers:** Help build trust with customers, partners, and stakeholders by demonstrating a commitment to security and ethical practices, which can enhance competitive edge.

Managed Backup & Disaster Recovery

Powered by Acronis

Integrated Data and Cybersecurity Protection

As part of a complete services platform, Sourcepass offers clients its Managed Backup & Disaster Recovery solution, powered by Acronis, that helps protect and secure your data.

The Sourcepass Managed Backup & Disaster Recovery solution safeguards businesses from disasters, human error, and malicious activity to promote business continuity with end-to-end encryption of data onsite, in transit, and in the cloud.

Business Benefits

Frequent & Reliable Backups

Quickly recover from disasters, accidental deletions, and malicious activity with multi-faceted backups (local, offsite, and Cloud virtualized)

Enhanced Threat Protection

Rest assured knowing that data is secure with encryption for all backup data at rest and in motion, while proactive anti-malware and ransomware threat protection protects files

24/7 Technical Support

Ensure quick resolution with enhanced technical support and 24/7/365 monitoring that alerts Sourcepass to quickly resolve any backup alerts

How It Works



Cloud backups are performed daily and retained for one year but can be customized to meet a client's needs.

Risk Assessments

Navigate Risks to Secure Outcomes

Proactive Measures to Reduce Risk

As part of our cybersecurity engagement, Sourcepass performs regularly scheduled security risk assessments to reduce risks and guard against threats.

Our team methodically identifies vulnerabilities, misconfigurations, and potential gaps in your security architecture, and creates an action plan to mitigate vulnerabilities and bolster your defenses.

By providing a snapshot of the overall security health of your IT environment, you can make informed decisions on policy, technology, and workflow that help to protect your company and contribute to compliance efforts and cyber insurance requirements.

Assess, Report, Mitigate, Succeed.

By establishing a rhythm of assessment, reporting, and mitigation, we strengthen your company's ability to withstand a cybersecurity threat, reducing downtime and risk, while protecting your company's reputation and avoiding costly data breaches.

Risk Assessment Process



Generate a Security Roadmap to Reduce Risk Levels

Penetration Testing

Proactive Security to Evaluate Risk Before Breaches Occur

Fortify Defenses

Penetration testing is an integral component of proactive security as its goal is to evaluate and prioritize risk before breaches occur.

Sourcepass provides penetration testing to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities and to provide guidance on how to reduce risks, close security gaps, and stay compliant with important security regulations.

A Clear View of Threats within Your Network

Through the exploitation of identified security vulnerabilities, penetration testing can effectively measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations.

Key Outcomes

- Identified Security Vulnerabilities**
Helps you discover security weaknesses before they can be exploited by attackers
- Improved Risk Management**
Shifts your risk management strategy from reactive to proactive, enhancing overall security
- Protection of Sensitive Data**
Safeguards sensitive data by identifying and mitigating potential security breaches
- Cost Savings**
By preventing security breaches, saves you from the potentially enormous costs associated with data breaches, including lost revenue and reputational damage

Our Process



Scope
Test Plan



Identify
Potential
Vulnerabilities



Attempt
Vulnerability
Exploitation



Document
Findings



Provide Detailed
Reporting &
Remediation
Steps



Populate Workflow
Management
Portal

Cybersecurity Awareness Training and Phishing Simulations

Powered by KnowBe4

Elevate Awareness, Eliminate Threats

Cybersecurity awareness training is crucial to educating your employees against social engineering attacks and may be required to meet compliance training regulations.

Included in our Standard and Advanced Security options, Sourcepass provides clients with a robust cybersecurity awareness training & phishing simulation solution to help reduce cybersecurity risk and meet cybersecurity insurance requirements.

Key Features



On-Demand Training

Educate your employees on how cyber criminals operate to create a unified security culture.



Simulated Phishing Tests

Test your employees' knowledge from the awareness training by sending simulated phishing emails. Failing to identify a phishing attack results in additional training.



Data-Driven Decisions

Make informed decisions for your security awareness plan by identifying risk at the user, group, and organizational level.



Advanced Tactics

Your users are a first line of defense. Continuously phish your users with more advanced tactics to keep security top of mind.

Training Process

1

Users go through interactive, on-demand training to learn about cybersecurity threats and best practices.

2

The system sends simulated phishing emails to employees to reinforce the training and measure improvement.

3

Reports show the progress of your business's security awareness, helping to reduce the overall risk of cyber threats.

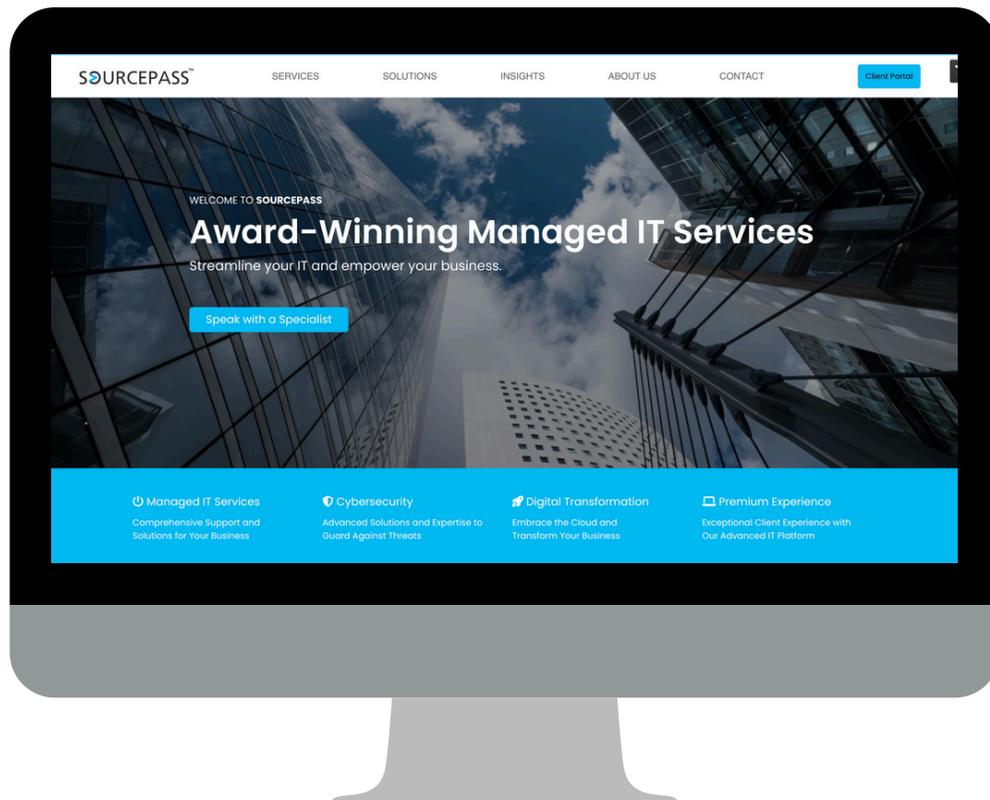


SOC 2
TYPE II
CERTIFIED



SOURCEPASS™

Take control of your digital universe.



Visit sourcepass.com to start your digital transformation journey today.

