S|3 SPECIALIZED SECURITY SERVICES

SCANNING FOR COMPLIANCE

SCANNING FOR COMPLIANCE

An Introduction to Compliance-Based Vulnerability Scanning

It's no secret that if your organization is going to succeed in today's digital world, you simply must protect your data assets from both internal and external threats while adhering to a broad variety of compliance requirements. But today's ever-evolving landscape can make that process increasingly challenging.

One solution often recommended by S3 Security is the process of compliance-based vulnerability scanning, which can provide significant benefits when it comes to maintaining robust security postures and meeting regulatory standards.

Simply defined, vulnerability scanning is a proactive, systematic approach to identifying, quantifying and ranking vulnerabilities in an IT system. It serves as a cyber "health check" for your infrastructure, uncovering potential weaknesses that attackers could exploit. By identifying these vulnerabilities, you can take preemptive action and patch them before they are exploited, significantly reducing the risk of a security incident. Regular vulnerability scanning is crucial as new vulnerabilities are continually discovered and added to the databases used by scanners.

There are two approaches to vulnerability scanning.

Unauthenticated Scanning: This scans your network and systems like a threat actor, looking for vulnerabilities that could be exploited without trusted access to the network.

Authenticated Scanning: This scan uses credentials to access your network and systems, providing specific permissions. This method offers insights into vulnerabilities that could be exploited by insider threats or a threat actor who gained access as a trusted user.

It's important to note that vulnerability scanning, while integral to cybersecurity, is distinct from *penetration testing*. Vulnerability scanning identifies known vulnerabilities, whereas penetration testing exploits them to assess their severity and potential impact.

THE IMPORTANCE OF VULNERABILITY SCANNING

There are two primary reasons why vulnerability scanning is essential.

Compliance Requirements: Many regulatory frameworks mandate regular vulnerability scanning as part of their compliance requirements. You must comply with these standards to avoid penalties and maintain trust with your stakeholders.

Network Security Evaluation: Vulnerability scanning helps evaluate vulnerabilities in new or changing networks. Detecting and mitigating vulnerabilities is crucial for protecting data assets from internal and external threats, making it a vital component of any information security program.

Types of Vulnerability Scanning

Vulnerability scanning can also be categorized into three main types.

Full Scanning: This type of scan involves a comprehensive assessment of all possible network or computer system vulnerabilities using every available tool. It is a thorough and often noisy process that probes every potential weakness.

Discovery Scanning: This type of scanning – also known as a quick or stealth scan – is used to gain an overview of a network's devices and potential vulnerabilities. It is typically quieter than full scanning and helps create a game plan for more detailed scans.

Compliance Scanning: Compliance scans audit your security to ensure it meets specific regulatory requirements. For example, PCI certification requires businesses to pass internal and external vulnerability checks to remain compliant. security program.

COMPLIANCE FRAMEWORKS REQUIRING VULNERABILITY SCANNING

Various compliance frameworks mandate regular vulnerability scanning to ensure robust security practices. This section provides an in-depth look at common frameworks – including NIST, ISO 27001, CMMC, GLBA, PCI DSS, HIPAA, and SOC 2 – highlighting their specific requirements and the importance of effective vulnerability management.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS is a set of security standards designed to protect cardholder data and ensure secure transactions. Organizations that handle payment card information must comply with PCI DSS requirements, which include rigorous security controls and regular vulnerability scanning.

The PCI DSS 4.0 framework introduces several significant changes to vulnerability scanning requirements, reflecting an evolving focus on enhancing security measures and adapting to emerging threats. Here's an overview of the key updates:

1. **Internal Vulnerability Scanning**:
    - **Authenticated Scanning**: PCI DSS 4.0 now mandates that internal vulnerability scans be performed using authenticated scanning methods. This means the scan must access internal system resources, such as registries and package versions, rather than just performing a network-based scan. This approach ensures that vulnerabilities within the system that are not exposed externally are also detected. This requirement is best practice until March 31, 2025, after which it becomes mandatory.
    - **Frequency**: Internal scans must be conducted at least once every three months. Additionally, scans must be performed after any significant change to the environment.
2. **External Vulnerability Scanning**:
    - **Regular Scanning**: External vulnerability scans must continue to be performed at least once every three months by an Approved Scanning Vendor (ASV). These scans are crucial for identifying vulnerabilities that could be exploited from outside the organization's network.
    - **After Significant Changes**: Like internal scans, external scans are required after any significant changes to the network, such as new system components or changes to firewall rules.
3. **Risk-Based Vulnerability Management:**
    - **Prioritization**: PCI DSS 4.0 introduces a new focus on risk-based vulnerability management. While vulnerabilities classified as high-risk or critical must still be addressed promptly, the framework now requires entities to assess and address other vulnerabilities based on the results of a targeted risk analysis. This approach allows organizations to prioritize remediation efforts according to the specific risks they face.
4. **Rescanning:**
    - **Confirmation of Remediation**: After addressing identified vulnerabilities, organizations must perform rescans to ensure that the vulnerabilities have been successfully remediated and that the system meets the PCI DSS requirements for a passing scan.

These changes reflect PCI DSS 4.0's emphasis on more comprehensive and rigorous vulnerability management, ensuring that organizations can better protect cardholder data against evolving cyber threats.

NIST (National Institute of Standards and Technology)

The National Institute of Standards and Technology (NIST) provides comprehensive guidelines for vulnerability management under its various cybersecurity frameworks; most notably the NIST Cybersecurity Framework (CSF) and NIST Special Publication (SP) 800-53.

- **NIST Cybersecurity Framework (CSF):** This voluntary framework consists of standards, guidelines and best practices for managing cybersecurity risks. It focuses on vulnerability management, recommending regular scans to identify and address vulnerabilities as part of the "Identify" and "Protect" functions. This framework emphasizes the importance of continuous monitoring and assessment to detect and mitigate vulnerabilities promptly.
- **NIST SP 800-53:** This publication provides a catalog of security and privacy controls for federal information systems and organizations. It outlines specific controls related to vulnerability scanning, such as:
  - **RA-5:** Requires organizations to scan for vulnerabilities in the information system and hosted applications, analyze the results and remediate any identified vulnerabilities.
  - **CA-7:** Emphasizes continuous monitoring, including regular vulnerability scanning, to ensure ongoing awareness of information security, vulnerabilities and threats.

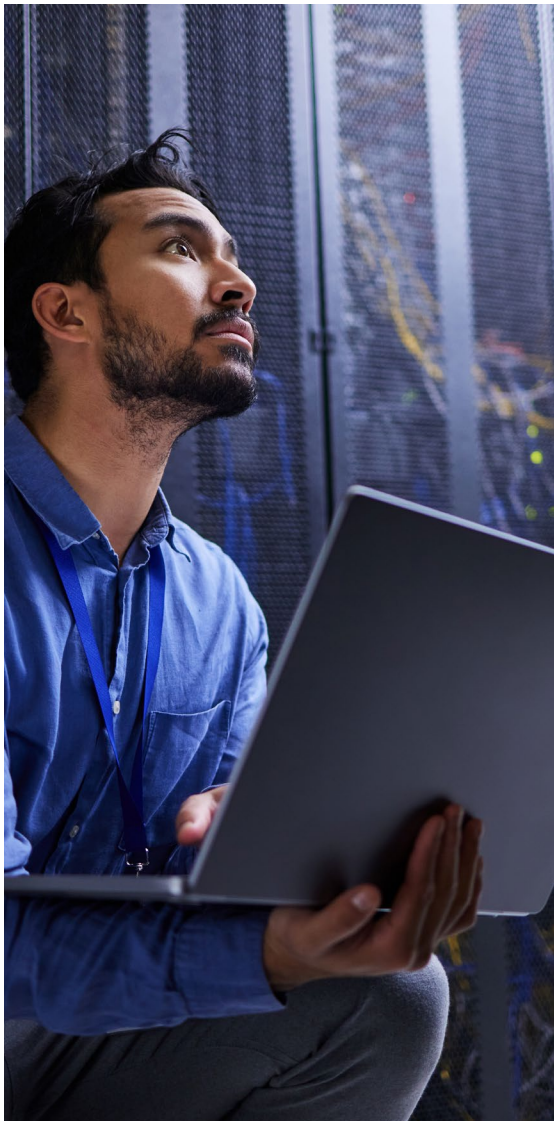
- **NIST SP 800-171**: This publication is specifically designed to protect Controlled Unclassified Information (CUI) in non-federal systems and organizations. It is often required for contractors working with the U.S. Department of Defense and other federal agencies.
  - **Requirement 3.11.2 (Vulnerability Remediation)**: Organizations must "periodically scan for vulnerabilities in the information system and applications" and "remediate vulnerabilities in accordance with risk assessments." This requirement ensures that organizations regularly identify and address vulnerabilities that could jeopardize the security of CUI.
  - **Security Requirements**: NIST SP 800-171 includes 110 security requirements across 14 families, with several controls related to vulnerability management. These controls emphasize the need for continuous monitoring, timely remediation of identified vulnerabilities, and ensuring that systems handling CUI are secure.

These guidelines ensure that you have robust processes to detect, analyze, and remediate vulnerabilities, enhancing your overall security posture.

ISO 27001

ISO 27001 is an internationally recognized standard for information security management. It provides a systematic approach to managing sensitive company information so it remains secure. The standard includes requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

- **Risk Management:** ISO 27001 requires regular risk assessments, which include identifying vulnerabilities in your information systems. Vulnerability scanning is a key component of these assessments, helping identify potential weaknesses that attackers could exploit.
- **Control Objective A.12.6:** Specifically addresses technical vulnerability management. It mandates that you obtain timely information about technical vulnerabilities, evaluate your exposure and take appropriate measures to address the associated risk. This involves:
  - **Regular Vulnerability Assessments:** Conducting periodic scans to identify vulnerabilities in systems and applications.
  - **Timely Remediation:** Implementing measures to remediate vulnerabilities based on their severity and potential impact on your organization.



By adhering to ISO 27001 standards, you can ensure a comprehensive approach to information security, including proactively identifying and mitigating vulnerabilities.

CMMC (Cybersecurity Maturity Model Certification)

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is the latest iteration of the CMMC framework implemented by the U.S. Department of Defense (DoD) to ensure defense contractors adequately protect controlled unclassified information (CUI).

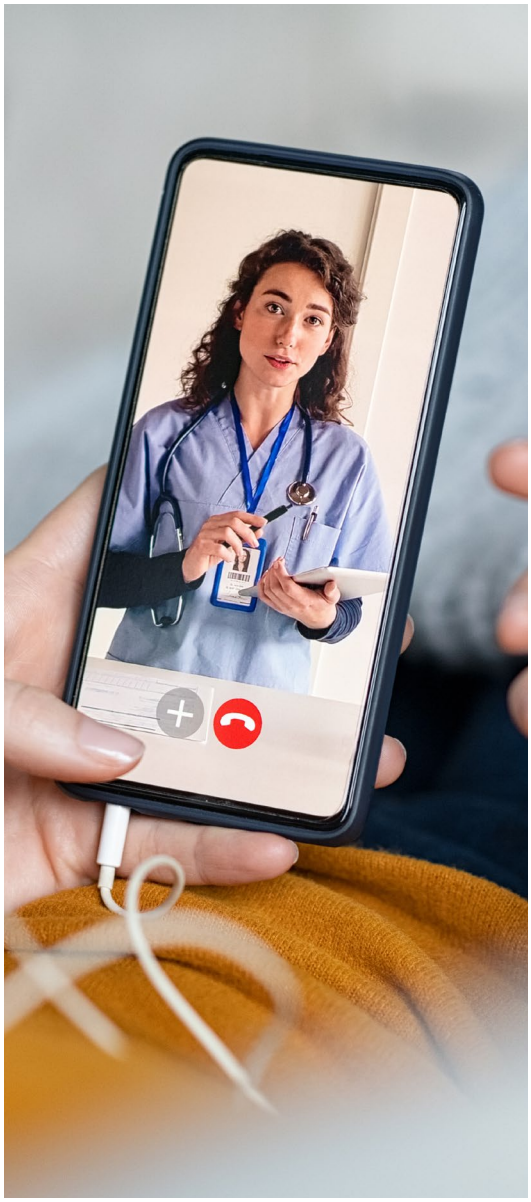
- **CMMC Levels:** CMMC 2.0 simplifies the original model, reducing the levels from five to three, each of which includes increasing requirements for safeguarding CUI. Vulnerability management practices, including regular vulnerability scanning, are integral to achieving higher maturity levels.
  - **Level 1 (Foundational):** Requires you to perform regular vulnerability scans and address identified vulnerabilities to maintain adequate protection of CUI.
  - **Level 2 (Advanced):** Emphasizes advanced and proactive cybersecurity practices, including continuous monitoring and automated vulnerability scanning, to identify and mitigate real-time vulnerabilities.
  - **Levels 3 (Expert):** Based on a subset of NIST SP 800-172 requirements, this level demands advanced cybersecurity practices and will require government-led assessments.

Adhering to CMMC requirements can ensure you meet cybersecurity standards to protect sensitive information and maintain eligibility for DoD contracts.

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a federal law that requires healthcare providers, health plans and their business associates to protect the privacy and security of health information. Under HIPAA, you must implement technical safeguards to ensure the confidentiality, integrity and availability of electronically protected health information (ePHI).

- **HIPAA Security Rule:** This rule specifically addresses the need for vulnerability scanning. It requires covered entities to conduct regular security risk analyses and implement measures to reduce risks and vulnerabilities to a reasonable appropriate level. Vulnerability scanning plays a critical role in these efforts by identifying potential weaknesses criminals could exploit to gain unauthorized access to ePHI.



Key Aspects of HIPAA-Related Vulnerability Scanning

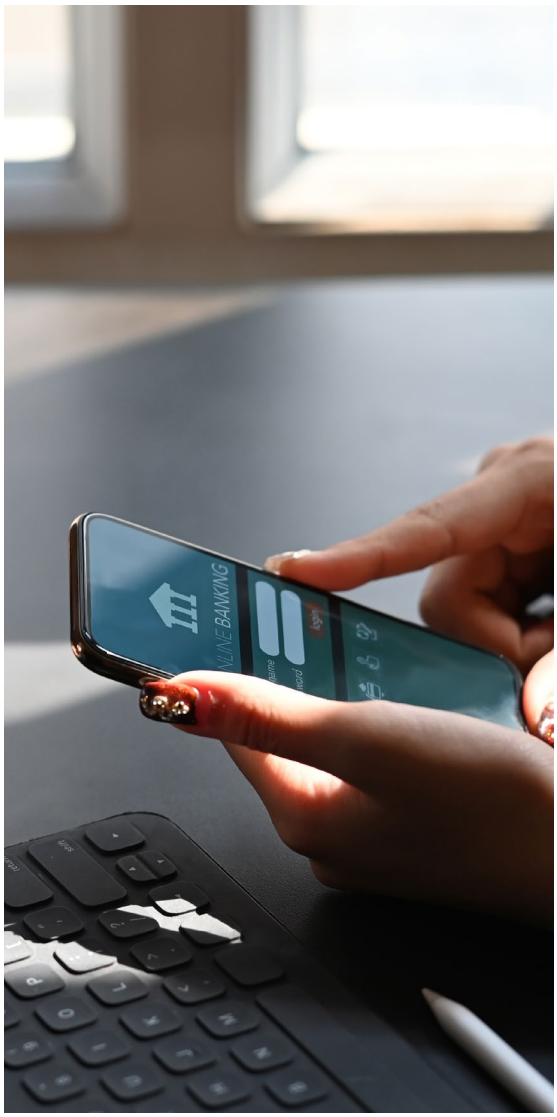
- **Regular Scans:** To identify potential vulnerabilities, conduct regular vulnerability scans of all systems that store, process or transmit ePHI.
- **Risk Assessment:** Incorporate vulnerability scan results into your overall risk assessment and management process.
- **Remediation:** Promptly address and mitigate identified vulnerabilities to reduce the risk of a data breach.
- **Documentation:** Maintain detailed records of vulnerability scans, risk assessments and remediation efforts as part of HIPAA compliance documentation.

By implementing regular vulnerability scans, healthcare organizations can ensure they're taking proactive steps to protect ePHI and comply with HIPAA's technical safeguard requirements.

GLBA (Gramm-Leach-Bliley Act)

The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions implement robust security measures to protect customer information. The GLBA Safeguards Rule specifically addresses the need for vulnerability scanning as part of your information security program.

- **Safeguards Rule:** Financial institutions must develop, implement and maintain a comprehensive information security program that includes administrative, technical and physical safeguards. Key aspects related to vulnerability scanning include:
  - **Risk Assessment:** Conduct regular risk assessments to identify vulnerabilities in systems and applications handling customer information.
  - **Security Controls:** Implementing appropriate security controls to address identified vulnerabilities, including regular vulnerability scanning to detect and remediate weaknesses.
  - **Continuous Monitoring:** Ensuring ongoing monitoring and testing of the effectiveness of security controls, including periodic vulnerability scans to identify new threats and vulnerabilities.

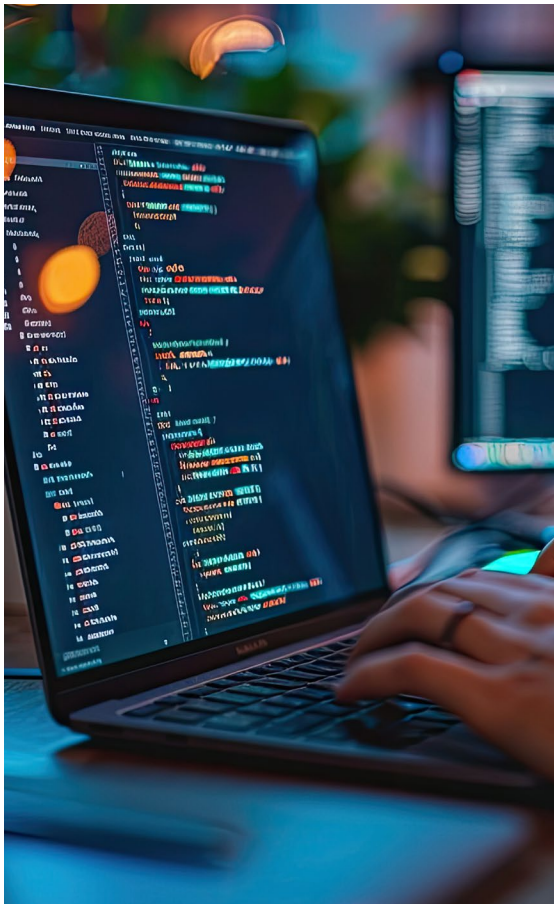


Compliance with the GLBA helps financial institutions protect sensitive customer information, maintain consumer trust and avoid regulatory penalties.

SOC 2 (Service Organization Control 2)

SOC 2 is a framework for managing customer data based on five “Trust Service Criteria” – Security, Availability, Processing integrity, Confidentiality and Privacy. While SOC 2 does not explicitly require vulnerability scanning, this process significantly enhances security practices by providing evidence of proactive measures against potential cyber threats.

- **Trust Services Criteria (TSC):** SOC 2 reports are based on the TSC, which include:
  - **CC7.1:** This criterion requires you to implement detection and monitoring procedures to identify changes that introduce new vulnerabilities and susceptibilities to newly discovered vulnerabilities.
  - **Point of Focus:** Conduct periodic vulnerability scans designed to identify potential vulnerabilities or misconfigurations after any significant change in the environment and take action to remediate identified deficiencies promptly.



Regular vulnerability scanning helps demonstrate your commitment to maintaining a secure environment, complying with SOC 2 requirements, safeguarding customer data, and enhancing trust.

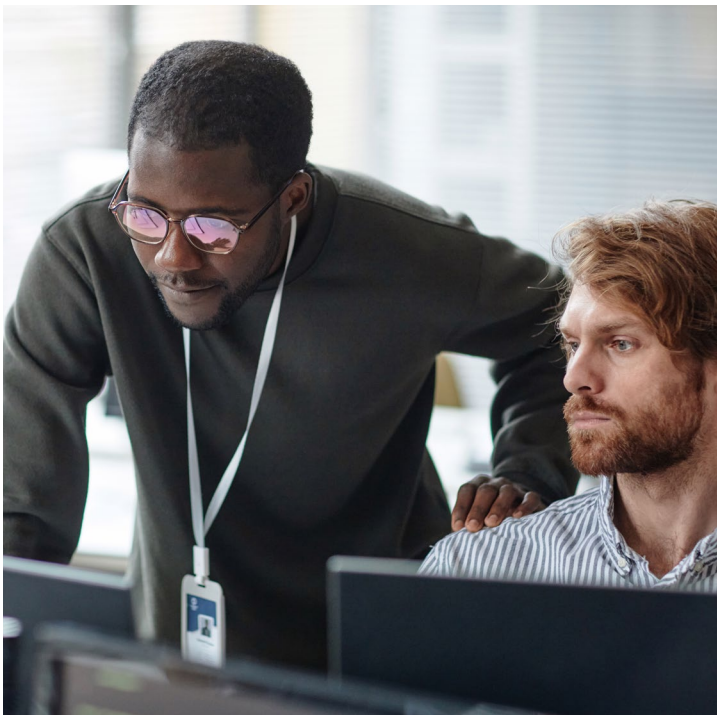
CHALLENGES WITH COMPLIANCE SCANNING

Despite its importance, compliance scanning faces several challenges.

False Positives: Compliance scanning often reports numerous false positives, leading administrators to ignore reports or improperly dismiss findings.

Operational Disparity: The broad acceptance of compliance scanning can cause a gap between compliance and actual system management, making periodic scanning a broken and frustrating process.

Need for Integration: You should integrate compliance into modern deployment and configuration management practices to ensure that security controls are part of the configuration files.



IMPLEMENTING EFFECTIVE VULNERABILITY SCANNING

To implement an effective vulnerability scanning program, you should:

Run Regular Scans: Conduct both internal and external scans regularly – preferably quarterly – and after any significant network changes.

Act on Findings: Quickly address any discovered vulnerabilities and rescan to validate that they have been successfully remediated.

Use Qualified Personnel: Ensure that scans are conducted by qualified individuals independent of the systems being scanned to avoid conflicts of interest and ensure objective results.

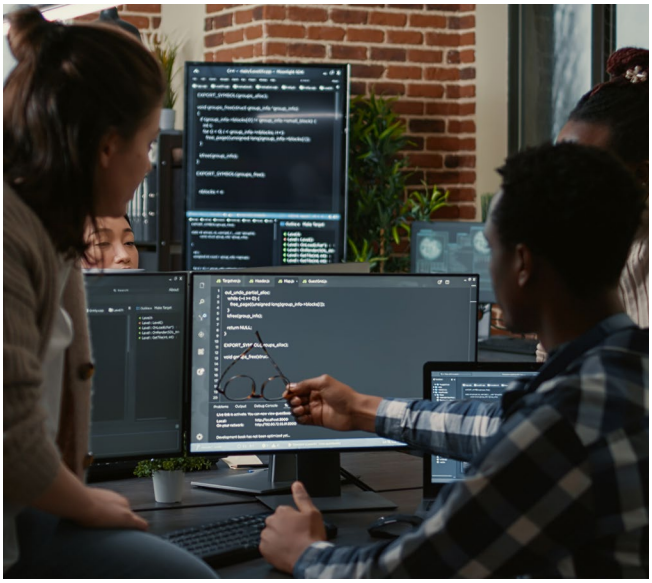
Automate Scanning: Using automated tools to schedule and perform scans ensures consistent and frequent assessments.

ACHIEVE COMPLIANCE WITH VULNERABILITY SCANNING BY S3 SECURITY

Understanding your vulnerabilities and how attackers could exploit them is crucial for enhancing your security program. At S3 Security, we specialize in compliance-based vulnerability scans that protect your networks, applications, devices and people against real-world threats – thus demonstrating the security level of your critical systems and infrastructure. In short, we show you precisely what is needed to fortify your defenses and maintain compliance.

Our elite team of engineers brings world-class expertise to the task of overcoming your cybersecurity challenges. They hold industry-respected certifications – including ASV, OSCP, CISSP, CEH, PCIP, GSEC, GCIH, GWAPT and Security+ – and have extensive experience conducting vulnerability scans for a diverse range of clients, from emerging businesses to Fortune 500 corporations.

At S3 Security, we adopt a comprehensive approach to compliance-based vulnerability scanning, combining advanced tools, cutting-edge methodologies and a deep understanding of the latest cybersecurity threats. Our scanning frameworks align with stringent industry standards and regulatory requirements – including NIST, PCI, HIPAA, CMMC, FISMA, ISO 27001, SOC 2, and GLBA/FFIEC – ensuring your organization meets or exceeds compliance and security expectations.



Best of all, we're dedicated to understanding your organization's unique challenges and providing customized solutions that address your specific needs and business goals. As your partner in cybersecurity, we're passionate about helping you navigate the evolving threat landscape and setting your organization up for greater success.

Engage with S3 Security today. and Let our experts help you build validation and testing protocols that will satisfy your requirements and actively combat ongoing threats.

LEARN MORE ABOUT VULNERABILITY SCANNING
S3SECURITY.COM | 972-378-5554