ANATOMYIT

What Every Practice Needs

Core Security Essentials & FAQs

Solution: Endpoint Detection and Response with Security Operation Center (SOC)

Protects against ransomware, malware, and unauthorized access through continuous monitoring and rapid response. Our SOC analysts review alerts in real time, isolate active threats, and guide your response—minimizing the impact on patient care and operations.

- **Why should we add EDR with a SOC if we already have antivirus?**
  - Traditional antivirus is limited to known threats. EDR uses behavior-based detection and expert analysis to catch zero-days, ransomware, and advanced attacks that AV can't stop.
- **How does this reduce our risk of a breach?**
  - The SOC team monitors alerts 24/7, investigates threats, contains active incidents, and provides expert guidance—reducing the chance of unnoticed breaches and improving response time.

Solution: Multifactor Authentication

Blocks unauthorized access even if passwords are compromised. MFA requires additional verification, like a push notification making it nearly impossible for attackers to access systems with just stolen credentials.

- **Why is MFA critical for our organization?**
  - Credential theft is the #1 cause of breaches. MFA stops attackers from accessing accounts—even if they have the right password—by requiring an extra layer of verification.
- **How does MFA protect against real-world attacks?**
  - It blocks phishing-based login attempts and unauthorized access from unfamiliar devices or locations, drastically reducing the risk of account compromise or business email compromise.

- **Will this interrupt our clinical workflow?**
    - MFA is designed to be quick and minimally disruptive. Most users verify with a mobile push in seconds—and stay signed in all day.

Solution: Security Awareness Training and Phishing Simulation

Empowers staff to recognize and avoid threats like phishing and social engineering. Includes engaging training content and simulated phishing tests to measure and improve real-world readiness.

- **Why do we need formal security training?**
    - Over 80% of breaches involve human error. Even the best security tools can't stop a user from clicking the wrong link unless they're trained to spot it.
- **How do phishing simulations help protect us?**
    - They provide safe, controlled tests that measure employee readiness and identify high-risk behavior before real attacks happen.

Solution: DNS Filtering

Blocks access to dangerous or unauthorized websites. Stops malware downloads, phishing pages, and command-and-control callbacks before they ever reach the device.

- **Why add DNS filtering to our environment?**
    - Users may accidentally visit dangerous websites. DNS filtering blocks access to known malicious domains, stopping threats before they can reach the device or network, regardless of where the user is working.
- **How does this help reduce cybersecurity risk?**
    - It helps prevent data exfiltration and patient data loss by stopping malicious connections early in the attack chain.

Solution: E-mail Security

Our advanced email security solution scans inbound and outbound messages for signs of phishing, malicious attachments, spoofing, and business email compromise (BEC). Leveraging real-time threat intelligence, sandboxing, and impersonation detection, it stops dangerous emails before they reach your staff, reducing the risk of breaches and fraud.

- **Why do we need dedicated email security if we already use Microsoft 365?**
    - Microsoft 365 includes basic email filtering, but it's not enough to stop advanced threats like zero-day malware or highly targeted impersonation attacks. A dedicated solution adds deeper inspection, real-time threat intelligence, and sandboxing to catch what built-in tools often miss.

- **How does this reduce our cybersecurity and compliance risk?**
    - Email is the most common channel through which electronic protected health information is leaked or stolen. Blocking phishing emails, malware-laced attachments, and BEC attempts at the gateway dramatically reduces the risk of credential theft, ransomware, and financial fraud. This also helps you meet HIPAA's requirements for access and integrity controls.

Solution: Extended Server Backup Retention

Provides long-term backup storage for critical servers beyond the standard retention period, ensuring compliance, disaster recovery readiness, and historical data availability.

- **Why is long-term backup retention important for security?**
    - Some threats, like ransomware or insider threats, may go undetected for weeks or months. Extended retention ensures historical recovery points are available when needed.

- **How does it reduce risk?**
    - It gives you more flexibility to recover clean data from before an incident, helping meet regulatory requirements and reduce downtime.

Solution: Advanced Microsoft 365 Backups

Backs up Microsoft 365 data including email, OneDrive, SharePoint, and Teams. Protects against accidental deletions, ransomware, and gaps in Microsoft's built-in retention policies.

- **Why back up Microsoft 365 if it's in the cloud?**
    - Microsoft's native data protection is limited. Microsoft focuses on availability, not full backup and recovery. It doesn't guarantee recovery from accidental deletion, ransomware, or policy gaps.
- **How does this help during an attack?**
    - You can restore lost or encrypted files, emails, or conversations quickly preserving care coordination and reducing disruption to operations.

Solution: Security Information and Event Monitoring (SIEM) with Identity Threat Detection & Response (ITDR)

Monitors and correlates security data across systems, users, and cloud platforms to detect and respond to complex attacks. Includes identity-focused analytics to catch unusual access patterns, compromised accounts, and privilege misuse.

- **Why do we need a SIEM if we have endpoint protection?**
  - Endpoint tools only see one piece of the puzzle. SIEM connects the dots across your network and cloud systems to reveal threats hiding in plain sight.
- **How does ITDR reduce our exposure?**
  - ITDR detects identity-based anomalies like logins from unfamiliar countries or after-hours activity so you can stop intrusions before data is stolen.

Solution: Internal Vulnerability Scanning

Scans your internal environment for risks like missing patches, misconfigurations, weak passwords, or insecure software. Generates prioritized reports with remediation guidance to fix issues before they're exploited.

By detecting these issues early, you gain the ability to proactively address risks before they turn into costly security incidents. The service provides detailed, prioritized reports highlighting critical findings along with practical remediation guidance, helping you strengthen your security posture and maintain compliance with industry standards.

- **Isn't patching our systems enough?**
  - Many systems still have hidden weaknesses even after updates. Scanning ensures nothing slips through the cracks—especially in hybrid and legacy environments.
- **How does this help reduce security risk?**
  - It helps you fix weak spots before attackers find them—making your environment more resilient and reducing your exposure. Internal vulnerability scans can also improve your compliance posture by providing documentation and remediation evidence for audits to support your security risk analyses.

Solution: External Network Penetration Testing

Simulates real-world attacks to find vulnerabilities before attackers do. Conducted by ethical hackers using a combination of automated tools and manual techniques to assess firewalls, cloud systems, and internet-facing services for exploitable weaknesses.

The service includes comprehensive reporting that prioritizes risks and provides actionable recommendations to strengthen your security posture, helping you reduce the likelihood of breaches and meet industry compliance requirements.

- **Why invest in a penetration test?**
  - It's the only way to know how an attacker would exploit your systems. Pen tests simulate real attacks to validate your defenses, uncover blind spots, and support compliance with HIPAA and cyber insurance policies.
- **How does this reduce breach likelihood?**
  - It identifies exploitable gaps you didn't know existed so you can close them before attackers find them. By identifying and remediating vulnerabilities before threat actors do, it strengthens your perimeter security and validates your defenses are working as intended.

General Security FAQs

Q: Will thesesecuritytools slow down patient care?

A: No. We focus on solutions that balance protection with usability. Our tools work behind the scenes or require only brief user interaction—keeping clinicians efficient and secure.

Q: Will this help us pass a HIPAA audit or meet cyber insurance requirements?

A: Absolutely. Our services are mapped to key HIPAA Security Rule requirements and align with the best practices recommended by OCR, HHS, and most cyber insurance providers.