SYNTAX

Syntax Security Services Overview

This multi-layered security posture is your best counteroffensive to cybercriminals' relentless attacks

There Is No "If" in Cybersecurity, but "When" and "How Often"

No longer can you ask if you'll be hacked because it's a virtual certainty. Then it's a question of how often. And the odds have only gone up with the rapidly increasing rate of zero-day exploits and the commercialization of malware toolkits. So, if you haven't been targeted yet, it's only a matter of time.

Add Layers to Protect Against Cyberattacks

There are six elements of a comprehensive security strategy, and when implemented together, they form an effective security framework. Each pillar functions as a countermeasure along possible pathways that cybercriminals use to gain access to your organization. These successive barriers together are designed to stymie determined attempts to compromise your mission-critical systems and data.

These 6 pillars are coordinated on a 24x7x365 basis by our Security Operations Center to provide business continuity protection. Their entire focus is on anticipating, detecting and responding to cyber threats and events, allowing you to focus on your operations. With Syntax's Security Services, you can also be confident that your security posture stays at the forefront of the latest technology, which helps you avoid the risk of exposure to new vulnerabilities.

3 Advantages to the Multi-Layered Syntax Security Posture

- ✓ **Real-time Threat Detection:** Seconds count when you are under attack, and nothing beats real-time notification for putting countermeasures into effect.
- ✓ **Centralized Management:** The Syntax Security Operations Center manages all your identified vulnerabilities from one dashboard as part of our managed service.
- ✓ **Cloud-Enabled Scalability:** Syntax Security Services are cloud-based solutions, which means the changing needs of your operations dictate what they can scale to.

The 6 Pillars of the Multi-Layered Syntax Security Posture

How Do the 6 Pillars of the Syntax Security Posture Work?

1 | Perimeter Security

This first pillar is designed to create a Zero Trust Network Architecture (ZTNA) - an encrypted end-to-end secure tunnel, for secure user access to all your on-premises, SaaS and web applications that allows you to:

- Eliminate lateral movement possibilities from connection through application thus minimizing exposure by shrinking your attack surface, including to internal risks.
- Allow the ability to scale Zero Trust effortlessly, by protecting critical applications or highest risk user groups first, then expanding internet-native ZTNA to your entire operation.
- Foster a stronger employee experience by allowing teams to securely communicate and collaborate while facing fewer security gateways that might get in their way.

2 | Endpoint Protection

This pillar offers you protection and response capabilities at the endpoint layer of individual devices connecting to your network of your corporate environment (including those of remote users). This robust managed endpoint detection and response (MDR) function includes threat intelligence with proactive threat hunting capabilities that also integrates with other security infrastructures.

3 | Vulnerability Management

This third pillar of Syntax security services is designed to provide you with a superior level of protection at the operating system layer by accommodating the complexity of your operating environment today, which will only get more complex. Containers, DevOps, mobility, cloud computing, and so many other innovations have blurred the perimeter of IT environments, and the trends will only continue.

4 | Proactive Testing

The function of this pillar of Syntax's security solution is to preemptively identify vulnerabilities and security weaknesses before an attacker exploits them. Offensive cybersecurity teams actively test your network's defenses and find vulnerabilities through threat hunting and penetration testing.

5 | SIEM/SOAR

These consolidated functions of Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) are designed to manage all your security content and provide forensics in the event of a security event. It comes with the capability for tailored reports tied to your business metrics and key performance indicators.

6 | End User Protection

This sixth pillar of Syntax Security services provides you with a detailed audit trail of all privileged account activity. That layer of protection helps you meet compliance standards for multiple regulatory standards. It can also protect against insider threats and simplify various functions of user access management so your team can focus on other critical administrative functions.