DETECT THREATS THAT GET PAST TRADITIONAL SECURITY TOOLS

Real-time network threat detection and response for the protection of critical business assets

Defense against evolving cyber threats requires an “assume breach” security mentality. But for many small and medium-sized organizations with limited security expertise and toolsets, shifting to a more proactive approach to threat detection can be fraught with questions on where to begin. Increasingly, the answers point to an integrated set of functions, cost-effectively managed by experts at the ready.

Highlights

- Threat detection anomalies and events
- Continuous security monitoring for your network and logs
- Detection and response procedures to reduce or eliminate emerging threats
- Open threat intelligence ecosystem to process threat intel from multiple sources
- Security orchestration to quickly respond to any incident
- Efficient solutions for regulatory and compliance requirements

THE CHALLENGE

Many small and medium-sized organizations rely on firewalls and antivirus tools to protect their networks and consider it good enough. This “prevention-based” approach works at blocking threats that can be readily identified. Unfortunately, overreliance on prevention exposes the organization to unknown threats adept at slipping past preventative controls, rendering the business vulnerable to a data breach or ransomware attack. In an age where IT teams must anticipate a breach, defense in depth calls for use of detection-based capabilities for discovery of threats you didn’t know were there.

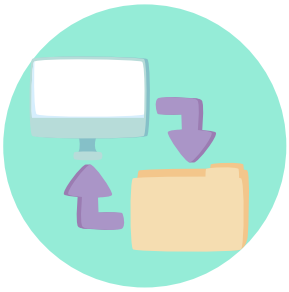
THE SOLUTION

Limited defense in depth? We've got you covered. Limited security expertise? Say hello to your extended IT security team! Our network threat detection and response team delivers real-time intelligence and visibility into events occurring within your environment. We provide rapid investigation and remediation—all managed 24/7 by Security Operations Center (SOC) staff skilled at quickly discerning what's real from the white noise of false positives.

For organizations that must adhere to regulatory controls and policies for the protection of sensitive data, centralized collection of all log and event data (and related retention) streamlines processes for improved and more cost-effective compliance reporting, from HIPAA to PCI-DSS.

Detect what's eluded your defenses

Boost defense, not headcount



Gain early warning on trending threats

We deliver everything you need for comprehensive threat detection and analysis, including intrusion detection, threat intelligence, log storage with configurable retention, and managed SOC services. By removing the necessity of having multiple security products and the related costs and complexity, you gain a stronger security and compliance posture, and ease of operation. The result: You're free to focus on what you do best–running your business!

KEY BENEFITS

Gain the expertise and coverage of a 24x7 SOC

You gain the power of 24x7 monitoring of your environment without the staffing costs and expertise required of a dedicated SOC. Our team of analysts does all the tedious work for you, chasing down the real threats from the noise and creating a force multiplier for your IT team, who is now free to focus on your IT operations.

Remove the Cost and Complexity of Solution Deployment and Management

As a managed service, we remove the costs and complexities of deployment and ongoing management associated with enterprise software. You gain always-on threat detection and response protection of your most critical assets. Implementation is super-fast, and as your environment changes, we work with you to adapt—fine-tuning configuration for optimal control and visibility.

Demonstrate Compliance

From patient health information to confidential financial information, government regulations and industry mandates require organizations managing sensitive information to have appropriate security measures in place to ensure data remains protected. Through centralized collection and retention of network and log data, you will have fast and effective means to demonstrate adherence to any number of security controls. For governmental bodies, compliance adherence extends to frameworks such as the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF).

Enhance Threat Visibility

Real-time threat intelligence feeds, from various authoritative sources, deliver up-to-date cyber insights into your environment. This powerful capability, typically reserved for large enterprises with expert staff, provides improved defense in depth through visibility into anomalies, policy violations, and threat data.

NEXT STEPS

Contact us for more information about threat detection solutions that can protect your business assets.

INTELLIGENT TECHNICAL SOLUTIONS

www.itsasap.com

I2880 Meade Ave #350
Las Vegas, NV 89102
Phone: (702) 605-6670