eSentire Network Interceptor™

Detect and Prevent Advanced Targeted Attacks

Midsized organizations now represent 54%[1] of all cybersecurity breaches and what's troubling is that you might not even be aware that you're a prime target. These attacks are becoming more sophisticated and much harder to detect. Yet traditional cybersecurity technologies haven't evolved at the same pace and as a result, fail to effectively protect you from today's sophisticated attacks. Now more than ever, your organization needs protection against more than just signature-based attacks. It needs holistic protection that's also capable of defending against zero-day targeted attacks and advanced persistent threats (APTs).

Protection Against Both Known and Unknown Threats

At the core of the Managed Detection and Response™ service is Network Interceptor, a next-gen IDS/IPS designed for midsized enterprise. It fuses robust threat intel to deliver real-time signature-based threat detection and prevention, while introducing the unique ability to identify unknown cyber threats through behavior-based anomaly detection and attack pattern analysis. With always-on full traffic capture, our team of highly skilled threat analysts get the full picture they need to hunt, investigate, identify and escalate unique threats in real-time, always. Completely customizable to your specific business context and policies, Network Interceptor is redefining cyber protection for midsized organizations in the face of today's constantly evolving cyber threat landscape.

Detects threats that technology alone can miss

Network Interceptor operates in real-time, using industry leading threat intelligence to protect your organization from today's known threats. It also extends far beyond traditional IDS/IPS with its unique ability to establish your network's baseline activity to detect abnormal behavior or unusual patterns. This triggers a real-time forensic investigation where our certified cybersecurity analysts confirm and manage threats through to resolution.

Powered by elite threat hunters

Our 24x7 team of elite cybersecurity intelligence analysts live inside Network Interceptor, know where and what to look for when it comes to the latest cyber threats. They use highly sophisticated forensics tools - crafted and fine-tuned over 10 years - to investigate and respond to odd or suspicious behavior flagged by Network Interceptor, and then they lock-it-down, within seconds.

Comprehensive, tailored protection for midsized enterprise

Network Interceptor isn't the old-school automated appliance that generates thousands of alerts for you to sift through. It's completely customizable to your business policies and procedures, and delivered as a service that includes monitoring, investigation and threat remediation through our elite team of cybersecurity analysts. Network Interceptor is designed to keep you protected from the latest cyber threats. It absorbs the complexity of cybersecurity management, so you can focus on managing your business.

[1] Verizon Breach Report, 2015

Trusted by over 500 midsized financial services, legal services, extractive, and healthcare organizations, Network Interceptor provides:

Protection against both known and unknown cyber threats including malicious software, botnets, phishing, data exfiltration, zero-day threats, Advanced Persistent Threats (APTs), and more.

A world-class, 24X7 global SOC that monitors, hunts, investigates, and remediates threats in real-time.

Alignment with industry governance measures including finance, legal, healthcare, and beyond.

- Always-on full traffic capture with complete traffic visibility for Security Operations Center (SOC) forensic investigation
- Real-time blocking of signature-based threats (phish, malware, botnets, etc.) using thousands of rules in 40+ threat categories
- Unknown/APTs/zero-day threat detection via attack pattern and behavior-based analytics including bandwidth usage analysis, geo-location reputation, unusual protocol, port scanning and more
- SSL decryption addresses the growing concern of threats that are hidden inside of encrypted SSL traffic
- Whitelisted executables
- Bad reputation geo-IP blacklisting
- Custom rules and signatures such as blocking access to social media, geo-IP, IP ranges and more
- Fully managed and monitored by our world class, 24X7 global SOC
- Rapid forensic investigation and holistic threat response from our elite cybersecurity analysts
- Network based TCP/IP reset enables immediate kill of malicious connections

esentire