esentire®

Overcoming Five Critical Cybersecurity Gaps

How Active Threat Protection Addresses the Problems that Security Technology Doesn't Solve

An eSentire White Paper

esentire®

Table of Contents

Executive Summary

A primary duty of senior management is to ensure that confidential information is protected. That's why the following statistics are unsettling:

- $46 billion was spent on cybersecurity in 2013[1].
- Yet 47,000 security incidents occurred and 44 million records were compromised in 2012 - the most recent year for which data is available[3]. Of these breaches:
    - 66% went undiscovered for months
    - 69% were discovered by external parties, not the business itself

These facts tell an uncomfortable truth: despite security spending, your network and confidential data could be compromised right now - while you are unaware of it.

Why?
Most enterprises operate with "set it and forget it" security automation; nursing the hope that multiple automated defense layers will solve the security problem.

But this hope disappoints. If automated security measures solved the problem, we wouldn't see 44 million compromised records in just one year.

Of course enterprises don't spend a collective $46 billion for nothing. Most security technology does what it is designed to do. But security automation by itself leaves critical gaps open, and cybercriminals have become adept at bypassing defenses to steal sensitive information.

This paper introduces the concept of Active Threat Protection™, which offers a way to close these gaps. Active Threat Protection combines advanced security software with human expertise. It goes further than traditional cyber security by protecting enterprises against previously unknown threats – even those that eluded other security defenses. Active Threat Protection also includes immediate intervention by security analysts to remediate incidents that technology alone can't handle.

Enterprises using "set and forget" security measures are exposed. They will be victimized if this is their sole approach to protecting their most crucial data. Active Threat Protection is the answer.

[1] ABI Research Study, July 2013

[2] Verizon RISK 2013 Data Breach Investigations Report

Traditional Cybersecurity Gaps

Cybersecurity solution providers are the first to admit that technology by itself doesn't solve the problem. Products tend to be programmed only for specific threat vectors. It always takes human intervention to restore systems to normal after a breach occurs. The damage suffered by an enterprise depends largely on how long the cyber threat remained undiscovered and unaddressed.

There are five gaps in the traditional approach to cybersecurity:

Protecting against the past

Most security products are designed to recognize attacks that have happened before. They automatically prevent reoccurrences because they are programmed with the threat signatures.

Unfortunately, the past isn't always a guide to the future. Threats morph all the time, as cybercriminals devise new ways to bypass security technology. Automated security systems are always one step behind. Enterprises need protection against previously unknown (called "zero-day") threats, not just yesterday's known threats.

Maginot line mentality

The Maginot Line was a series of concrete fortifications that France deployed along its border with Germany during the 1930s. The idea was to provide time for their army to mobilize in the event of an attack. But at the outset of World War II the Germans simply outflanked the Maginot Line, invading through Belgium.

Traditional cybersecurity is based on an outwardly-focused "prevention" mentality. But today's most damaging attacks elude existing defenses to take up residence inside the enterprise network. Once there, they bide their time – gathering information that will make the eventual attack more successful and damaging.

Preventing intrusions is necessary, but what happens when preventative measures fail? How do you even find out? Enterprises need to combat threats that may already exist inside the corporate network.

Malware myopia

Malware is a big problem, but it is just one threat vector. Only 40% of last year's attacks were based on malware. What do we do about the other 60%? Enterprises need protection against all possible threats, not just those that involve malware.

Alert overload

A big problem with security automation is that it's automated. When a potential threat is identified, an alert is sent. In no time at all, the IT staff is swamped with alerts – but which ones are really worth analyzing?

It's a constant challenge to tune these systems. Too tight, and you get flooded with alerts. Too loose, and you may not get that one alert you really needed. In practice, most enterprises err on the "too loose" side, because they simply don't have the resources to investigate all the false positives. Of course, this exposes them to greater risk.

Enterprises need a way to sift through the millions of network events that happen every day to zero in on those that may pose a true threat.

The “it’s not my problem” syndrome

When a real security breach happens, enterprises need immediate help. Cybersecurity has become an incredibly complex and specialized technology niche. Companies with limited IT budgets need access to that expertise.

Unfortunately, legacy Managed Security Service Providers (MSSPs) only deliver notifications of breaches. They do not provide remediation assistance (“it’s not my problem”). They are really Managed Security Alert Providers.

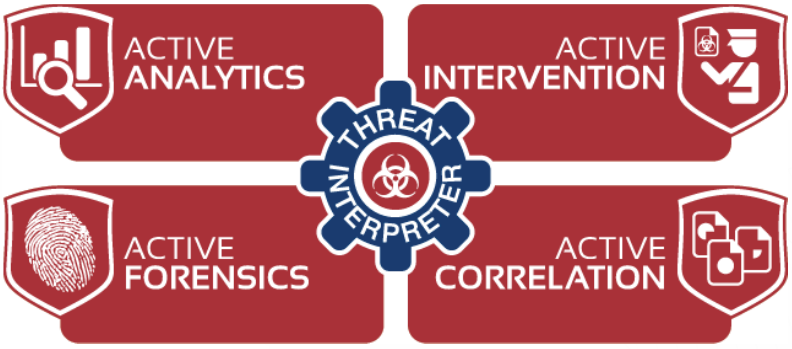
Other services do render help – if you are willing to pay a very steep a la carte price that is exacted right when a crisis is unfolding and you have no choice.

Enterprises need help that is immediate, competent, and cost effective. They need experts who will stick with the problem until it is fully resolved.

Active Threat Protection

Active Threat Protection closes the above gaps. It is the most comprehensive way to protect the organization's confidential information. To assist in describing the principles of Active Threat Protection, we will use eSentire's Network Interceptor™ as a practical example.

Figure 1: The eSentire Network Interceptor Active Threat Protection Platform



Four capabilities are essential to Active Threat Protection:

1. Better information about network events is needed. This means getting real-time data straight "from the wire." In Network Interceptor this is called Active Analytics, a capability that finds both known and previously unknown threats.
2. Active Forensics "operationalizes" event data. Software tools and dashboards weed out false positives while escalating bona fide threats.
3. Trained security experts do Active Intervention when a security incident happens. They operate as an extension of your IT team, rendering practical assistance when you need it the most.
4. The log-based data already being captured by traditional security automation is still important. Active Correlation increases its value by aggregating it into the Active Forensics Database.

This framework combines advanced detection technology with human expertise and is the only way to close gaps inherent to traditional security automation.

Drill down: How Active Threat Protection is different

Network Interceptor introduces a new level of cybersecurity protection. Here are some of its differentiating features:

Active Analytics

Network Interceptor's eSensors apply proprietary algorithms in real time, leveraging these capabilities:

Direct event scrutiny

There is no waiting for device logs to be aggregated and normalized. Network Interceptor sits "on the wire," gathering a richer set of traffic data, and supplying crucial information to the Active Forensics Database.

Behaviour-based detection

Threats reveal themselves by the way they behave. Network Interceptor identifies threatening behaviors, surveying the internal network as well as inbound traffic. This enables Network Interceptor to find threats other security systems miss.

Immediate interdictors

These are software "enforcers" that step in to stop attacks in their tracks by automatically applying prearranged remediation tactics.

Active Forensics

Active Forensics combines rich network event data and interpretive technology to pinpoint bona fide security threats. It is "operationalized" forensics – an advanced toolset that security experts leverage to rapidly research and remediate cyber threats:

Active forensics database

A repository of network event data that is a broader and richer source of valuable information for security systems and analysts. It is a key resource that even extends the capabilities of traditional security systems.

Intelligent threat interpreter

This dashboard-based facility applies software algorithms to the Active Forensics Database, eliminating false positives and highlighting events that truly need attention.

Network event traceability

This advanced tool is like having a record/rewind button on the network: a series of related events can be traced back to their origins to reveal actionable information that is otherwise unobtainable.

Active Intervention

The only way to really solve a security crisis is with the proactive help of security experts who have access to Active Forensics. Active Intervention extends the your IT team with deep subject matter expertise precisely when it is most needed.

Without Active Intervention, most enterprises trust in "set and forget" technology that can be bypassed. They may use MSSP services but get an "it's not my problem" message when a real attack emerges. Active Intervention closes these gaps and minimizes business risk.

Active Correlation

Traditional event logs have great value. Active Correlation cooperates with existing security products and device logs by aggregating information from many sources and feeding it into the Active Forensics Database. Active Correlation is provided by these services:

Log Sentry™

This service collects and monitors log events, detecting anomalies and providing data to the Active Forensics Database. It also is used to support compliance monitoring and reporting.

Asset Manager Protect

This service correlates threat data across a broad community of user companies, enabling Network Interceptor to prevent attacks from malicious sites when a threat emerges at just one community member's company.

Continuous Vulnerability Scanning

This service provides nonstop vulnerability management, combining regular scans and penetration testing. It closes the window left open by vulnerability assessments that are done only an annual or semiannual basis.

Conclusion

At eSentire, we're proud to be leading this new, broader cybersecurity paradigm. It's no accident that more than 500 businesses with more than $2.5 trillion in assets trust us with their cybersecurity. When a business is responsible for people's money it absolutely, positively needs active threat protection.

Active Threat Protection is the future of cybersecurity, because every enterprise deserves the most comprehensive protection possible.

About eSentire

eSentire® is a leader in continuous advanced threat protection solutions and managed cybersecurity services. The company's flagship offering, Active Threat Protection™, challenges legacy security approaches, combining behavior-based analytics, immediate mitigation and actionable intelligence on a 24x7x365 basis. Dedicated security experts continuously monitor customer networks to detect and block cyberattacks in real-time. Protecting more than $2.5 trillion in Assets under Management (AuM), eSentire is the trusted choice for security decision-makers in financial services, healthcare, mining, energy, engineering and construction, legal services, and technology companies. In late 2013, eSentire was named to the Deloitte Technology Fast 50 Companies to Watch and cited as a Canadian Innovation Exchange CIX Top 20 most innovative Canadian company.
For more information visit **www.esentire.com** and follow **@esentire**.

eSentire is named a Gartner 2015 Cool Vendor for Cloud Security Services in the 2015 Cool Vendors report by Gartner Inc.