eSentire Targeted Retrospection Analysis Platform (TRAP)™

How Do You Know if You've Been Breached by a Zero-Day Threat?

Mid-sized organizations now represent 54% of all cybersecurity breaches[1]. The surge in attacks has been largely attributed to the perception that they have less IT security defenses in place, providing attackers with an effortless target while at the same time, offering an easier channel into larger, and potentially more lucrative organizations. Most organizations aren't aware that 85% of cyber attacks could have been avoided if PC's alone were up-to date with current security patches.

There's no easy solution for this with limited IT resources. As a result, attackers take advantage of vulnerabilities as an entry way into an organizations network where they go undetected for days, weeks, months and even years. Dwell Time (the average time a breach goes undetected) is approximately 98 days for financial firms, giving these zero-day exploits a large window to lodge themselves in networks, poke around for data, spread across your network, and slowly begin data exfiltration that eventually leads to a large scale cybersecurity breach.

TRAP Finds Security Breahes That Dwell in Your Network

The Targeted Retrospection Analysis Platform (TRAP) service uses the latest known vulnerabilities and threat intelligence to continuously scan against a full archive of your historical network traffic to identify if you were previously compromised. Alerts are investigated by our team of cybersecurity analysts to validate when, where and how a breach occurred and then work with you on remediation. The industry's first fully managed service of its kind, TRAP represents a big step forward in cybersecurity. It enables us to go back-in-time to minimize dwell time of zero-day threats, ultimately helping to prevent large scale breaches and the financial, brand and reputational damage that comes with them.

The industry's first fully managed service of its kind, TRAP helps you:

- Know your breach status before it's too late
- Minimize the potential cost and impact of a breach by catching them sooner
- Exceed regulatory compliance, board and public disclosure requirements

[1] Verizon, Data Breach Investigations Report, 2015

eSentire Targeted Retrospection Analysis Platform (TRAP)

Threat intel meets cybersecurity time machine

Using full packet capture, TRAP immediately begins building a detailed archive of your historical network traffic. From there, industry-leading threat intelligence rule sets covering more than 40 different threat categories are automatically scanned against this archive to catch the zero-day threats that by-passed your security defenses and now sit in your network.

Automatic scanning and reportingStay secure

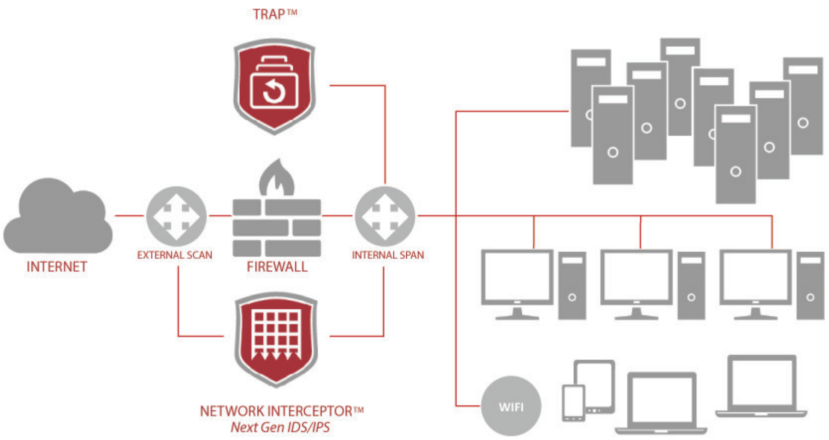
TRAP scans your network traffic archive every week using the latest in threat intelligence to find previously undetected security breaches. We even run adhoc scans when a major critical event occurs. When we find something, you'll be sent an alert immediately. You'll even receive weekly reports that provide scan statistics so you're always on top of your breach status.

Fully managed by our 24X7 Security Operations Center

You won't have to sift through hundreds of alerts. Our security analysts investigate and validate events so you'll only receive true, actionable ones, including steps to remediate. Fully monitored, maintained, managed and delivered as a service, TRAP manages your cybersecurity so you can remain focused on managing your business.

Key Capabilities

- Advanced Threat Intelligence Rule Sets Include:
    - Network behaviors, malware command and control, DoS attacks, botnets, informational events, exploits, vulnerabilities, SCADA network protocols, exploit kit activity and more
- Full Packet Capture
- Stores Months of Archived Traffic
- Zero Network Latency
- Weekly Scanning
- Weekly Breach Reports Include:
    - Volume of data scanned
    - Summary of alerts by snort <classtype>
    - Summary of affected IPs and number of associated alerts
- Alert Investigation and Remediation by Security Analysts
- Delivered as a Turn-key Managed Service


TRAP™
INTERNET
EXTERNAL SCAN
FIREWALL
INTERNAL SPAN
NETWORK INTERCEPTOR™
Next Gen IDS/IPS
WIFI