# tracealert
powered by **SOD** SECURITY ON-DEMAND

**You have all the right defenses in place, but you know that isn't enough. You need to do more. You want to do more. You want to have the confidence that you will be able to detect a breach when it happens - not months later.**

But how? Attacks are impossibly sophisticated. They are built to sneak in under the radar, not setting off ay alarms. Attackers have an advantage and they know how to leverage it. New attacks are launched every day. There are patches and signature updates, but who can keep up with all of that? And what about the zero day attacks?

You're suffering from data overload. This isn't a problem you can solve with more people. There is just too much data flying at you, and without context, it doesn't make sense. You need an intelligent, automated way to pull it together and turn it into something meaningful. If you don't find a better way, it could take up to 259 days to detect a breach*.  You need TraceAlert, TraceSecurity's managed SIEM solution.

## How It Works

We collect and correlate data from all over your network into a single database. Next, we partner with you to tune SOD's threat analytics platform to develop a baseline of normal activity specific to your network and users. With this baseline established, TraceAlert uses powerful algorithms and big data analytics to identify real anomalies, which indicate a genuine threat. These are prioritized and escalated to our Information Security Analysts who work with you to respond to these threats in near real time.
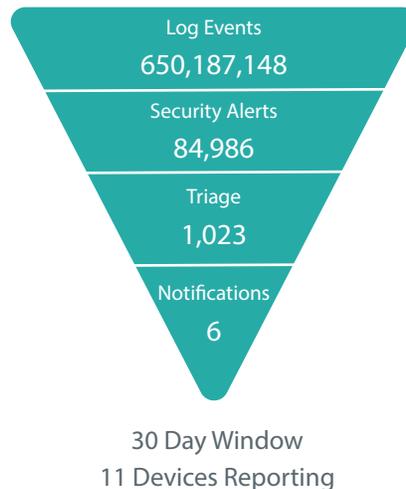
## With TraceAlert You Know:

- What devices are on your network
- What your users are doing
- Which assets are vulnerable to attack

- If and which assets are communicating with known bad actors
- If there are active threats on the network

### With TraceAlert You Will:

- Detect breaches faster
- Reduce the impact of a breach
- Minimize business interruptions
- Streamline security policies and procedures
- Improve breach investigation efficiency and reduce resolution time

### Real Customer Example:

Log Events
650,187,148

Security Alerts
84,986

Triage
1,023

Notifications
6

30 Day Window
11 Devices Reporting

### Situational Awareness With Actionable Data:

Our cutting edge correlation and analytics tools give your team the upper hand against cyber threats. Keep pace with high velocity data surges and the new breed of attackers.

**The Bottom Line:** All the noise from massive flows of log alerts is translated into a manageable stream of actionable notifications.

*2015 Cost of Cyber Crime Study, Ponemon Institute

# tracesecurity

877-275-3009          tracesecurity.com          sales@tracesecurity.com
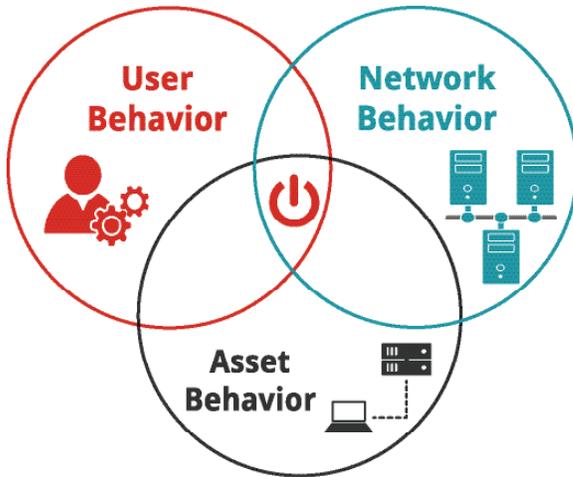
## Benefits of TraceAlert:

- Scale - By analyzing behavior, our technology does more of the threat identification work so we need fewer analysts to process alerts
- Visibility - Correlating all of the data means we see the big picture and can easily identify what doesn't belong
- Speed - We cut through the noise and bring forward YOUR critical threats in minutes, not weeks or months
- Compliance - We provide the required documentation of policies, retain audit trails, and deliver comprehensive compliance reporting capabilities
- Forensic Support - We store full log data, which is required for forensic examination of security incidents

## Features:

- 24/7 Coverage - Around the clock monitoring of all security event data and alerts, including alert triangle, analysis, and response assistance
- 3 Way Event Correlation with Behavioral Analytics - Integrates rules, risk, and behavior into a proprietary analysis decision system using patented algorithms and an advanced case management system
- TraceAlert integrates with SOD's cutting edge threat analytics platform with industry leading security analysis tools that can provide unique detection ability to discover advanced attack vectors
- Advanced Security Use Cases - Integrates logs from DNS, Active Directory, DHCP, Databases and Scans as optional data sources to enrich and improve detection ability
- Full Log Management - Big data analysis technology to parse, analyze, and store all log data in real-time
- Advanced Client Portal - Tools for threat and log analysis, interactive dashboards, and one-click visual drill-downs. Supports Master and Tiered Portals for organizations that need to provide departmental views
- Reporting - A comprehensive report library, regulatory compliance reports, threat analytics reports, and ad hoc query report tools

## TraceSecurity Can Help

Address Compliance Needs: Performs the required logging of devices required by PCI, HIPAA, and other regulatory acts. Provides a single pane of glass where you can generate the necessary compliance reporting.

Reduce Incident Response Times: By detecting threats faster and providing actionable notifications including threat summary, analysis details, and recommendations.

Improve Visibility & Control: Customized parent-child views in the portal allow management staff to look at trends across the whole business while individual departments only see the information relevant to their group.

Get started and request your 30 minute demo of TraceAlert today. Contact us at sales@tracesecurity.com.