

Network Logging and Monitoring

According to the 2010 Verizon Data Breach Report,* 86% of security breaches can be detected in application and system logs. However, most logs are not monitored properly, allowing security incidents to go unnoticed for months. Logging alone is not enough to prevent breaches. The logs must be reliably monitored to identify attacks.

Two Monitoring Options

The least expensive solution is automated monitoring. However, as automated monitoring is based on signatures developed from previously observed attacks, it will never be as effective as real-time monitoring by dedicated and trained individuals.

Although it is more expensive, the best security comes from a trained 24/7 security staff. Due to the variety in malicious attacks, humans are able to identify unusual events at a higher reliability level than automated monitoring alone. Regrettably, the people capable of analyzing security events are often more expensive to hire and retain than the average business finds affordable. A managed service allows an organization to gain the highest quality security analysts available without having to absorb the cost of staffing a security operations center.

Our Solutions

Alliance offers two solutions for network logging and monitoring:

Feature	Automated Device	Managed Service
Detect Security Events	✓	✓
Correlate Events	✓	✓
Monitor Existing Devices	✓	✓
Monitor Existing Servers	–	✓
8/5 Daily Review Option	✓	–
24/7 Ongoing Review Option	✓	✓
Weed Out False Positives	–	✓
Defense in Depth Option	–	✓
Self-Monitored	✓	–

Depending on your needs, either solution might be a good fit for your organization. Please contact us today and schedule a meeting, so we can discuss your environment and determine which is right for you.

* Report available at http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf