Executive Summary:

The Electronic On-Ramp, Inc. (EOR) team has developed leading edge methodologies that enable commercial enterprise organizations and government agencies to accurately track how many network data packets should be on a network at any given time. We have termed the core technique "eDATA" (Enterprise Data Analysis and Transactional Auditing). This technique has diverse application into banking, finance, or fortifying the security of large business driven network environments. This methodology enables large enterprises to adopt a new stance in their security posture to enable them to step away from traditional network baseline and anomaly based approaches to network security monitoring by taking into account the mathematics involved with actual business transactions. This new approach is much more realistic than the older quasi-utopian ideas associated with network baselines that were always plagued by the ever changing needs of business and the very nature of both the internal and external threats that evolve and surround enterprises today.

Background:

Traditionally, Intrusion Detection Systems (IDS) require very steep investments and continual resource overhead in developing human resources, training, and equipment while only being marginally affective at detecting intrusions. Human intervention and interaction provides situational and environmental awareness but is not always efficient at analyzing high volumes network traffic or at evaluating complex pattern analysis.

As the limitations of IDS technology are constantly being realized and highlighted in the press there has been a sensational push towards automated Intrusion Prevention technology (IPS). IPS solutions offer several advantages to the enterprise, a couple of which include reduced investment in human operators, and automated response mechanisms that work together to decrease reaction time while increasing productivity for the security teams. These advances in automated protection are a marked improvement over their IDS predecessors, but continue to be limited by their reliance on signatures and thresholds that loosely conform to predefined norms that aren't always tied closely enough to the traffic found on real networks. In addition, each new custom configuration or signature may cause accidental denials of service. These limitations and others become more apparent as new types of attacks are developed and deployed against global enterprises.

An alternative / supportive approach to IPS is Network Behavior based Anomaly Detection (NBAD). This process involves defining a comprehensive baseline of all network traffic considered, that a human believes to be normal at the time the NBAD is initially configured. After the initial configuration, statistical analysis is typically applied to the traffic in order to determine what might be considered to be abnormal activity. This process is very effective in detecting changes to network traffic, but does not fully address the perturbations that are introduced by dynamic changes in network traffic and it does not address statistics that can be manipulated remotely.

Solution:

The Advanced Concepts Team from EOR has developed a new approach to solving these inherent limitations with security solutions described above. This approach involves measuring the amount of bytes and packet transactions that it takes to complete a business transaction from the Web client to the front-end Web Server and then from front-end to the middleware server, then from the middleware to the Database server. By tracking the traffic between these dissimilar systems and then by validating the data processed by each parent service on the systems in question, the EOR team has been able to determine the exact amount of legitimate traffic that should be seen on a network at any given point in time. By specifically determining what transactional traffic on a network is legitimate, EOR can easily isolate and stop any traffic that is associated with costly, malicious, or otherwise unwanted traffic.

The methodology and the supporting tools will allow EOR to determine if any covert communication channels have been established and if any side-channel communication attempts have been made. This revolutionary approach, allows for EOR to identify, isolate, and eliminate the first sign of unwanted traffic. The techniques utilized by the EOR team have been successful in isolating anomalous traffic down to the first unwanted packet and stopping the source of the unwanted traffic before it gets started.

When completely implemented this new methodology allows for enterprises to develop stronger baselines that are tied to each transaction, which offers far more insight and protection, than is provided though static baselines and the limitations that are associated with static time-based metrics. Integrating agents on critical network servers and by implementing per process packet tagging enables eDATA based security systems to operate in its most optimum conditions and offers enterprises the elite style of support that the need when combating the threats of both today and the ones from tomorrow as well.

Outcome:

eDATA based security systems enable enterprises and governments to improve its level of insight, detection, accuracy, mitigation, and response times for previously unknown threats to a whole new level of protection that far outweighs those of predecessor technologies, like those described above. The eDATA solution and the IP Based Transactional Accounting Methodologies used by the EOR team, bring unprecedented levels of assurance to any organization that invests into Information Assurance and has a need to protect the data that transits its networks, while at the same time allowing the investment into good networks to be utilized by the packets that organizations prefer to allow onto their systems.

In short, EOR's new campaign to reunite the lost and orphaned packets of the world with their parents* enables new levels of performance and security that have not been experienced, nor achieved in the past. By focusing on both performance and security, EOR utilizes eDATA as a foundational component of the new Secure Network Operations Center (SNOC) framework, which can be further evaluated in other white papers that have been released by EOR.

**Parents defined as Packet Generating Process ID's (PID's)*