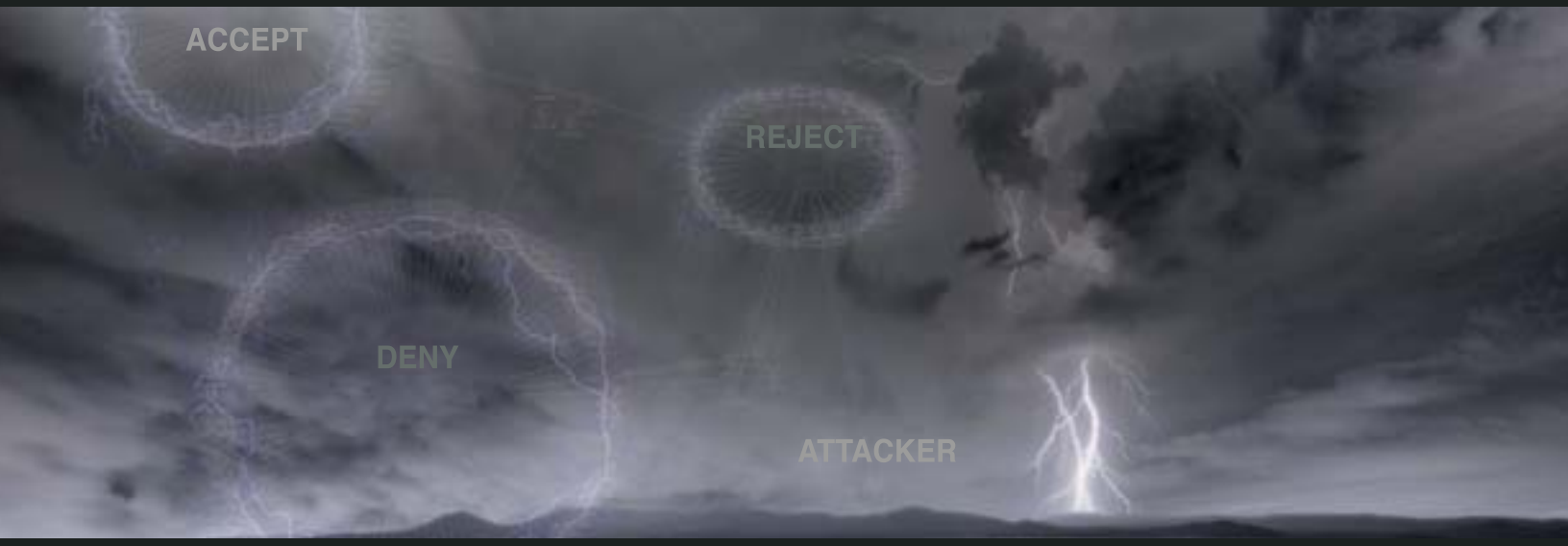
# SilentRunner Sentinel




## UNSURPASSED NETWORK FORENSICS with REAL-TIME DATA CAPTURE and ADVANCED VISUALIZATION

AccessData®
*A Pioneer in Digital Investigations Since 1987*

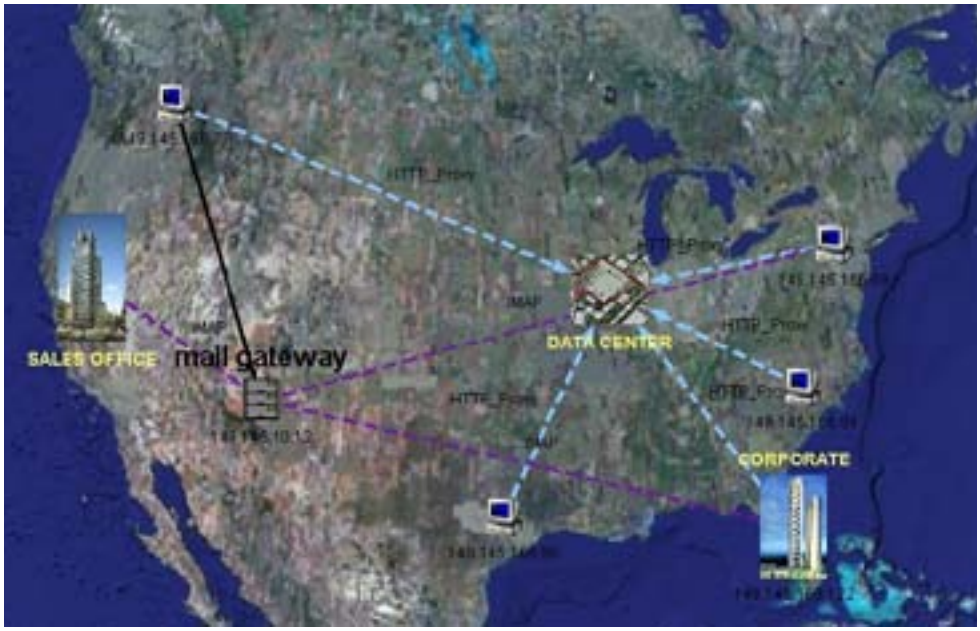
# Capture Real-time Network Data to Detect, Investigate and Properly Remediate Security Breaches, Data Theft and Policy Violations...

The success of organizations today relies significantly on the security and availability of their networks. However, networks are complex and their topographies are always changing, forcing you to react constantly. Security breaches are increasing steadily in number each year, the exploits are more sophisticated and many are perpetrated by authorized employees. Furthermore, organizations are under increasing pressure to comply with regulations and organizational policies. Given the broad spectrum of risk, organizations clearly require a network security investigation solution that can enable them to build network usage intelligence, identify suspicious patterns and expose weaknesses and anomalies.

SilentRunner™ Sentinel™ lets you know what's happening on your network by tackling the complicated tasks of capturing, analyzing and visualizing network and VoIP data. It's a passive network monitoring solution that creates a dynamic picture of communication flows to swiftly uncover break-in attempts, weaknesses, abnormal usage, policy violations and anomalies before, during and after an incident. Operating like a surveillance camera, SilentRunner Sentinel can play back events from thousands of communications to validate system threats and investigate security breaches. It identifies the offender and helps you mitigate the recurrence of the same security incident. In addition, it helps monitor infractions to regulatory controls and policy violations and provides comprehensive reports for auditing requirements, contributing to your ability to demonstrate compliance.

## A True Enterprise Cyber Security Solution

SilentRunner Sentinel captures real-time network traffic at full gigabit network line speeds, and it integrates with your existing cyber security infrastructure to provide actionable intelligence. Sentinel can target groups, buildings or entire networks. It allows you to watch sensitive corporate assets and proactively identify breaches and policy violations. Using SilentRunner Sentinel to visualize network data, from both internal and external networks, enables you to perform effective incident response and root cause analysis and perform comprehensive forensic investigations. Furthermore, you can leverage the intelligence you gain from Sentinel's graphical representations of your network activity to aid in network planning.




***ADVANCED VISUALIZATION:***
*Critical Path: Visualize nodal communications and expose patterns or hidden data relationships with geospatial accuracy to reflect physical asset locations.*

## Superior Analytics

SilentRunner Sentinel graphically illustrates network activity, allowing you to quickly identify and correlate relationships between users, resources, applications and data. Real-time data is recorded into a central knowledge base that can be queried. The time sequencing function allows you to identify network communication "habits", anomalies and specific events. Once a potential anomaly has been identified, you're able to drill down into the content to see exactly what is happening — for example credit card numbers being chatted outside the network or somebody visiting unauthorized websites. Incidents can be reconstructed and played back in real time, in the exact sequence in which they occurred, so you can identify the origin of the incident and understand how it propagates. You can leverage Sentinel to capture and analyze both network data and VoIP data. Processing, reconstruction and storage of data includes popular chat and webmail applications.

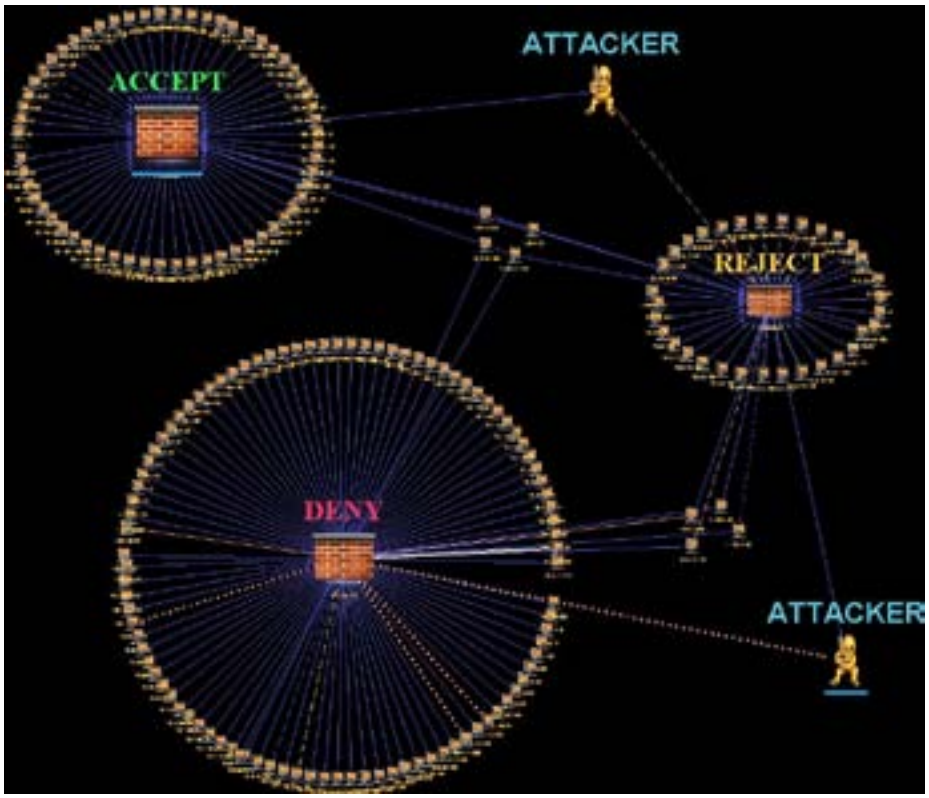
# The Benefits of Network Visibility…

### Reduce costs.
Automate complex network traffic recording and analysis processes that otherwise require many man-hours, additional headcount and expensive technical expertise.

### Reduce incident response time.
Reduce incident response time and perform efficient, granular security investigations — quickly finding the perpetrator(s) and reconstructing events exactly when, where and how they happened.

### Correlate Host and Network Data.
SilentRunner Sentinel integrates with AccessData Enterprise, providing a 360-degree view that allows you to correlate network data with host data. This gives you the investigative reach necessary to truly understand an exploit, isolate all affected nodes, and thoroughly remediate.

### Enforce regulatory compliance.
Robust auditing, analysis and reporting enable the detection of misuse and abnormal behavior and create valuable intelligence that supports demonstrable compliance to regulations and corporate policies.




***LOG ANALYSIS INVESTIGATION:***
*Visualize firewall events, with IDS alerts and pertinent network data surrounding a suspicious incident.*

### Quantify and mitigate risk.
Proactive network security analysis allows you to identify unknown security exposures and policy compliance issues.

### Enable security due diligence.
Gain critical information to help you answer difficult questions, such as Who is on your network? When are they there? What do they do? Where are the breaches? How is your network being exploited?

### Improve operational efficiencies.
Aggregate massive amounts of raw network data and transform it into actionable information, enabling the resolution of more investigations with less or the same amount of investigators.

### Obtain a solid ROI.
Save time and money in planning, deploying and maintaining security technologies and electronic assets.

## A Flexible and Simplified Architecture

- Appliance-based collectors mean you can simply “plug and play” with easy deployment and configuration.
- Red Hat Linux-based collection platform provides a significantly more stable operating system and is also a guarantee of complete packet captures.
- Oracle 11g integration and optimization means powerful processing and indexing, and faster insertions and extractions of data.
- SilentRunner Sentinel supports both mobile and enterprise deployments.
- This simplified architecture means that significantly less hardware is required for network deployments.

## Solution Highlights:

### *Real-time Network Traffic Recording and Advanced Visualization...*

- Captures network traffic at full **gigabit** network speeds.
- **VoIP** u-law/a-law capture and reconstruction.
- **Red Hat Linux-based collection platform** for complete packet captures and stability.
- Web-based interface for **centralized command** and control of the collection engines.
- **Unlimited** session content capture.
- SilentRunner® promiscuously monitors and records network traffic in **all seven layers of the Open Systems Interconnection (OSI) stack.**
- SilentRunner **monitors approximately 2,000 protocols and services** out of the box.
- Generate **interactive graphical representations** of the series of events, representing the propagation of an attack or other suspicious activity.
- Animate any graphical arrangement by **sequencing packet activity**.
- **Visualize audit logs and alerts**, and correlate actual network traffic.
- Efficiently analyze users, hosts, domains, applications, protocols and addresses to **detect changes or abnormalities** from established network baselines.
- Swiftly expose **anomalies, illegal connections** and **security and network problems**.
- Collections are **dynamically identified** by the packet information.
- **Schedule tcp dump captures** along with **immediate hashing** of the output files to ensure forensic integrity.

### *State-of-the-art Pattern and Content Analysis…*

- **Build "integrated maps"** of certain assets or users, such as **after-hours usage spikes**, and **mapping of virus and worm proliferation**.
- Determine the **root cause** of a security breach or quickly distinguish between diversionary and truly malicious incidents.
- **Evaluate similarities** within emails, documents, spreadsheets, etc.
- Independent of keyword or linguistic matching, **determine how proprietary or inappropriate information proliferated** from code servers, HR or financial databases, R&D labs and others.
- **Sawmill integration**.

### *Enterprise-class, centralized architecture for ease of use and efficiency…*

- Real-time network activity is recorded into a **central database that can be queried**.
- **Play back security incidents** in the exact sequence the events occurred.
- SilentRunner maintains a **millisecond clock** to record packet timing.
- Reconstruct events in their exact sequence to **immediately uncover the source** of an incident.
- Conduct **post-event analysis to prevent recurrence** of the same security incident.
- **Oracle 11g integration** for powerful processing and indexing, and faster insertions and extractions of data.
- **Instant Message Processing**.
    - Processing, reconstruction and storage of most popular chat applications.
    - Reporting based on chat handles, screen names, account types.
    - Contextual searching.
    - File transfer capture.
    - AOL-AIM, Yahoo, MSN, GoogleTalk, ICQ, IRC, Skype.
- **Webmail processing**.
    - Full processing, reconstruction and rendering of major webmail clients.
    - Reporting based on sender, recipient, attachment type, subject lines, etc.
    - Contextual searching capabilities.
    - Yahoo classic, Yahoo current, Gmail, Hotmail.