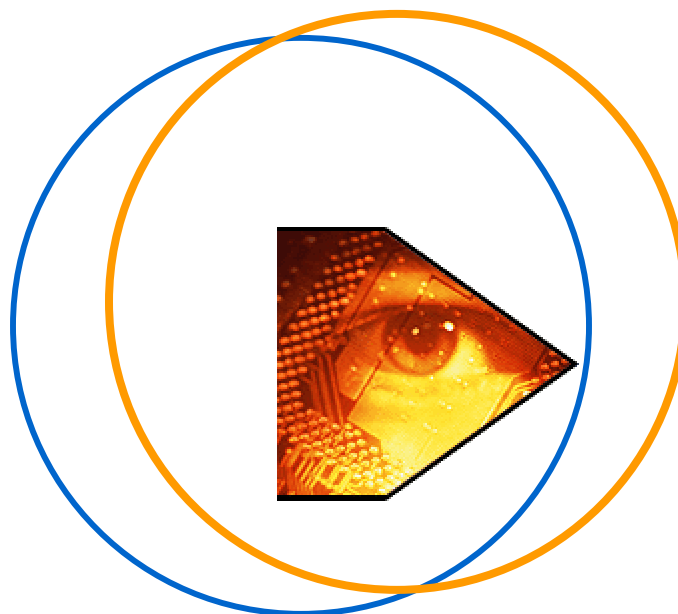


ThreatVision™: Security Event Management System

Unified Threat Management solution maximizes investment in security



Value Delivered:

Organizations can now have a unified view of threat across multi-platform and multi-vendor network and security environment

ViewTrust Security Threat Management System

OBJECTIVE

The objective of this paper is to give a brief overview of the ViewTrust ThreatVision™ Security Event Management System (SEMS) and its capabilities. The paper first describes the problem ThreatVision™ product solves for organizations and then provides its product and service description.

What is an Intrusion Detection System?

Intrusion Detection Systems (IDS) inspect and analyze all inbound and outbound packets on a network. Intrusion Detection Systems identify any suspicious patterns or features of packets that might indicate that an attack on your network is underway or that misuse of your network is occurring. Once a network attack or misuse is identified, the Intrusion Detection System alerts its operator so that the appropriate response can be initiated—IDS can also be configured to automatically respond to network activity of a predefined type, source, or severity.

Network-based Intrusion Detection Systems are deployed at the perimeter of your corporate network and monitor network traffic packet-by-packet to determine if that traffic conforms to predetermined threat detection signatures.

Threat Detection Signatures. Intrusion Detection Systems include a database of known threat detection signatures. A signature is an indicator that a packet or packets may represent a network attack or misuse. Signatures may be based upon packet patterns or upon packet content, protocol, port destination, or source. The Intrusion Detection System will compare each packet to known signatures stored in its database. The signatures in the IDS database are updated frequently. Many Intrusion Detection Systems also provide the ability to create custom threat detection signatures.

Attack Signatures. Attack signatures are a type of threat detection signatures that indicate that someone may be engaged in malicious, unauthorized, or otherwise undesirable activity involving the data on your systems or network. Attack signatures based upon packet patterns might look for activity that matches attempts to modify system files or that resembles pre-attack reconnaissance probes such as SATAN or unauthorized access attempts such as Brute Force Login. Attack signatures based upon port destination often watch for attempts to connect to network ports associated with servers that are often vulnerable such as Web or file servers. Attack signatures based upon packet content may look for packets with malformed or illogical headers—often attackers will use these packets

to simultaneously request to open and close a TCP connection resulting in a Denial of Service (DoS) attack.

Misuse Signatures. Misuse signatures are a type of threat detection signatures that indicate undesirable, non-attack activity. Non-attack activity is behavior that violates stated security or appropriate use policies or that appears to violate patterns of normal user or system activity. Many IDS systems can be configured to conform to your organizations network security or usage policies—some systems permit the creation of user-defined misuse signatures. Intrusion Detection Systems also recognize anomalies in network traffic patterns. Network users and systems develop patterns of normal activity that are specific and unique. Intrusion Detection Systems can be configured to compare current network activity to the normal baseline of traffic load, breakdown, protocols, and packet sizes—any deviation from that baseline activity is recognized as a threat worthy of investigation.

Why a signature based IDS system not a complete solution?

The signature based IDS systems are limited by the signatures contained in the database. These systems depend on the product vendor or the open source community such as SNORT community to update the signature database with latest signatures. What happens if the signature of latest attack worm is not available? Valuable time is lost before the attack is known.

Why firewall is not a complete Threat Management Solution?

Firewalls and VPN's are the most common methods for securing access to intranets, extranets, and e-commerce application servers however they are only part of a complete Internet security solution.

Perimeter defenses based on firewalls are still important—they will protect your organization's perimeter from outside attackers or unauthorized users—but more sophisticated security systems are needed. Firewalls enforce general entry and exit rules for a network and are not designed to look for attack patterns. The main purpose of a firewall is to keep undesirable traffic off your network and typically this traffic is identified only by source or destination address and protocol type. Skillful intruders understand how to elude detection by firewalls and how to cover their tracks once they've breached your network security. Attackers take advantage of open ports on firewalls, misconfigured firewalls, or newly created attack methods that evade the firewall's defenses. Only IDS can detect packets that are designed to be overlooked by a firewall's rule set.

What about a multi-vendor router, firewall, VPN and IDS environment?

Today's multi-vendor environment presents a challenge to the network and security administrators. The typical network may have Cisco, 3COM, Intel or Juniper routers on the edge, while the firewall mix may consist of CheckPoint, Cisco, SonicWall, Netscreen, Raptor

or Gauntlet platforms to name a few. The IDS sensors themselves may be from Cisco, Internet Security Systems™, SNORT, Enterasys Dragon or Network Flight Recorder (NFR), again to name a few. Each system comes with its own management systems, its own log analysis tools to assess the data gathered from its own environment. Add to this the information being received from server logs, SNMP traps, system alerts, which all happen to have their own syslog or binary formats. The problem of threat management is further compounded not simplified.

How does ThreatVision™ solve this problem?

ThreatVision™ provides a centralized data gathering, analysis and correlation engine that takes input from multiple sources in multiple formats and helps in identifying the root threat to the environment. It combines the log analysis, IDS signature analysis with a unique behavior based intrusion analysis. The data received from multiple devices is normalized and stored in a relational database system (RDBMS) for analysis. Each vendor receives an adapter for the data normalization process. Please refer to Figure 1 for a high level view of the ThreatVision™ architecture.

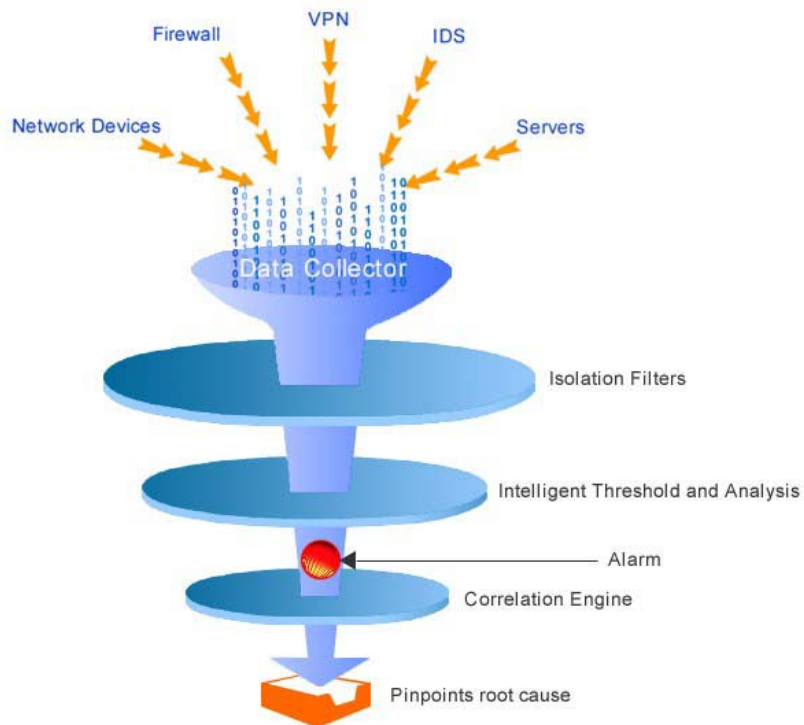


Figure 1: ViewTrust ThreatVision™ architecture

ThreatVision™: description

Unified Security Threat Management

ThreatVision™ offers real time protection against rapidly changing information security threats by unifying the threat information from multiple devices across multiple platforms. ViewTrust SEMS products provide an integrated solution that detects, analyzes and responds to malicious attacks. ThreatVision is capable of correlating security events across a variety of security devices and their alert formats, including Checkpoint, Cisco, ISS, Nokia, SNORT and Sonic Wall.

Security Solutions for Enterprise

ThreatVision™ performs advance intrusion detection, real-time threat analysis and response that protects corporate network against intrusion and denial service attacks. ThreatVision enables a highly coordinated approach to managing security issues by identifying threats and gathering information to respond quickly to emerging threats.

Real Time Event Correlation and Analysis

ThreatVision™ provides a state-of-the-art correlation and analysis engine that filters out data and refines only the relevant information, providing threat alerts without data overload. The real-time event aggregation, correlation and analysis enables administrator to gather intelligence across multiple devices to quickly spot abnormal behavior. This reduces the effort required by security analyst to identify threats, giving them time for more sophisticated intrusion investigation and policy management.

Unique Abnormal Behavior based Intrusion Detection

Abnormal behavior detection is a new frontier in the threat management space. ThreatVision profiling engines build a security 'baseline' for each environment and detects any behavior that does not confirm to the 'good' behavior. The traffic deviation from the good behavior 'baseline' is continually tracked by ThreatVision and is used to indicate an attack. Examples include detection of excessive use on port 80 or detection of use at unusual hours. The benefit of this approach is that it can detect the anomalies without having to understand the underlying cause behind the anomalies. It also provides detection when a signature based IDS system misses on a new type of an attack.

Real time Console View

ThreatVision™ provides a unique web-based view of the security events detected. Since this is a secure web-based view administrators can view security events from anywhere in the world.



Increased Accuracy

ThreatVision™ attack threshold categories were developed over live customer environments across of hundreds of Security devices. This provides for rapid tuning of the ThreatVision, thus reducing false positives that are common in most other “out of the box” IDS solutions.

Clean Incident Response Team (CIRT)

ThreatVision™ product and service offering is backed by ViewTrust Incident Response Team (CIRT). The CIRT Team works closely with customers to define the scope of a security breach, recommended actions to minimize damage and rectify vulnerabilities that contributed to the event. Throughout the process, security analysts carefully preserve evidence that may be required for criminal proceedings.

	The Clean Incident Response Team provides...
Monitoring	<ul style="list-style-type: none"> <input type="checkbox"/> Monitoring event logs 24x7 using centralized security management console <input type="checkbox"/> Sophisticated diagnostic tools <input type="checkbox"/> Extensive security knowledge database
Alert	<ul style="list-style-type: none"> <input type="checkbox"/> Alerts via pager, email and voice
Detect	<ul style="list-style-type: none"> <input type="checkbox"/> Known Offender Database <input type="checkbox"/> Abnormal Behavior Pattern
Analyze	<ul style="list-style-type: none"> <input type="checkbox"/> Probability Analysis <input type="checkbox"/> Correlation across Origination / Destination, type of attack, service, multiple devices or customers <input type="checkbox"/> Measure Threat and prioritize
Respond	<ul style="list-style-type: none"> <input type="checkbox"/> Battle Tested CIRT Process <input type="checkbox"/> Experienced CIRT Team <input type="checkbox"/> Immediately terminate the connection <input type="checkbox"/> Reconfigure the firewall to block such attacks <input type="checkbox"/> Send an administrative alert by telephone, console, e-mail or pager
Reporting	<ul style="list-style-type: none"> <input type="checkbox"/> Incident Reporting

Rapid Deployment

ThreatVision™ deployment does not require deployment of special hardware sensors or software to load on customer systems. Implementation requires a simple configuration change on the security devices.



ThreatVision™ Specifications

Features	Benefits
Correlation across multiple related devices	Identify abnormal behavior that would be missed due to lower thresholds as traffic is spread across multiple devices.
Correlation across unrelated devices	Identify new vulnerabilities and measure impact across larger sample
Security Traffic Classes of Service	Reduced time to install and tune new installation Reduce false positives Improved Accuracy
Pre-defined thresholds	Reduced time to install and tune new installation Reduce false positives Improved Accuracy
Log based IDS	Open, Multi-vendor / Multi-platform approach. Building upon previous work, new devices can easily added as required
No Dedicated hardware sensors	Reduced complexity and cost compared to Network based IDS
No Software on Servers or Devices	Reduced complexity and rapid deployment No additional software licenses, reduced cost Reduced ongoing maintenance Improved service reliability
Behavior based attack signatures	View malicious activity prior to a signature based IDS is aware of a vulnerability.
Defined Service Specific Attack Signatures	Detects service specific (e.g., FTP, Telnet, HTTP, etc.) abnormal behavior.
Defined General Protocol Attack Signatures	Predefined threat signatures that detect general protocol (TCP, UDP, ICMP) abnormal behavior.

ViewTrust ThreatVision™ delivers value by unifying the view of multiple threats across multiple security devices recorded in multiple formats.

Corporate HQ:

6311 Cardinal Hill Place
Springfield, Virginia 22152
Tel: 703.627.7539
Fax: 703.913.0301
info@viewtrust.com

