Driven by compliance, data leaks, risk mitigation, and the need for better security, CISOs, CIOs and their security teams are discovering a new way to protect information. nexTier Networks is leading this new era in security with the invention of a semantic intelligence and analysis technology that gives enterprises insight into what confidential data is stored across their enterprise -- on laptops, on desktops on servers and other devices throughout the network -- and protects that data based on its content. nexTier's technology brings a whole new approach to information security that introduces greater accuracy and speed to data leak detection over traditional data leak prevention solutions (DLP).

nexTier's Semantic Firewall for Greater Security

nexTier is innovative. Unlike other solutions that are deployed at the edge of the network, nexTier is deployed deep inside the enterprise network between corporate employees and information repositories. nexTier's patent-pending algorithms are capable of analyzing, in real-time, all data or information transmissions through email, ftp, telnet, instant messaging or unauthorized copying/saving of data on desktops, disks or CDs.

nexTier Networks' Semantic Firewall technology evaluates the security level of data and then automatically invokes a corresponding security policy to automatically prevent data leaks or extrusion. Once identified, a breach is then flagged to IT and security operations for further action.

To protect content identified as security critical, nexTier developed advanced algorithms that extract, or 'sequence' just enough information – the equivalent of a human's DNA in concept but smaller than 1000 Bytes – to accurately identify the information should it appear in other forms. Called the 'Semantic DNA Sequence™,' this nexTier innovation identifies where information originated, even if the information is extensively modified or repurposed by someone either inadvertently or maliciously.

Further, nexTier's Security-Semantic CORelation and indEXxing (S^2 COREX™) algorithms discover, classify, and index information in real-time based on the security value of the data's content. These technologies from nexTier represent a significant breakthrough that can scale accuracy and speed limitations that have significantly limited previous generations of DLP, traditional Latent Semantic Indexing (LSI) and other similar algorithms.

nexTier's DLP Agent Technology automatically applies security and other DLP policies prior to any system activity occurring on the end-user's machine. It then analyzes data in real-time to determine the significance of the data/information and accordingly invoke the corresponding security policy to prevent possible data leak (or extrusion) in real-time, while simultaneously prompting the security admin and logging the incident.

nexTier's next generation data leak prevention software enables total protection against malicious or inadvertent theft and misuse of unstructured, semi-structured and structured mission critical information across the enterprise. Available as software or in an appliance form factor, nexTier's technology is a highly-accurate, highly-performing data leak prevention system that protects all information assets in global, distributed enterprises. Deployed transparently into existing network and security infrastructures quickly, easily and automatically. nexTier's DLP does not require extensive policy setting or prior knowledge of what needs to be protected.

The World's Most Intelligent Data Leak Prevention

nexTier Networks, Inc. | 2953 Bunker Hill Lane, Suite 400 | Santa Clara, CA 95054

408.282.3561 | fax 408.282.3501 | www.nextiernetworks.com

nexTier's Scalability and Performance

The nexTier Semantic Firewall was built from the ground-up for massive scalability. Depending upon the individual needs of enterprises from data traffic volume, data traffic type, protocol types and applications specific requirements, multiple Semantic Firewalls from nexTier can be stacked to meet data traffic throughput and latency requirements.

nexTier's technology is designed to be easy to deploy, easy to configure and easy to use with no end-user behavior changes required for it to work. Enterprises are able to reduce deployment, administrative and set-up tasks from months to just days. The system also automates security processes including reporting compliance activities enterprise-wide.

A one-time initial installation and configuration process includes set-up to connect:

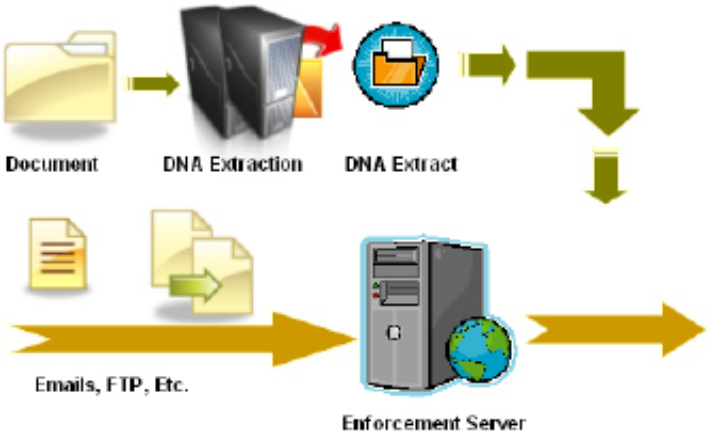
- ***Active Directory, LDAP and RADIUS:*** *The Semantic Firewall has built-in interfaces to enterprise information servers such as Active Directory, LDAP and RADIUS.*
- ***Enterprise Organizational Databases:*** *The Semantic Firewall has built-in interfaces to connect to Human Resources and other databases that contain pertinent information about the enterprise organizational structure such as Departments, Groups, Reporting Structures, etc.*
- ***Application Servers:*** *The Semantic Firewall has the ability to connect to Application Servers through its built-in Protocol Engine that supports multiple protocols (such as http, ftp, smtp, IM, etc.) Connections are established via configuration of {IP Address : Port Numbers} for individual Application Servers.*

How It Works

nexTier Networks' innovations introduce a new generation of security technology that when appliced to DLP is able to analyze, classify, recognize, and secure unstructured information in a way that is fundamentally different from existing technologies and methods.

The Semantic Firewall is comprised of a crawler for automated data discovery, a multi-protocol engine, the Semantic-DNA Vector Engine, the Semantic-Security Correlation Engine, a Policy Engine, and a Real-time Workflow and Monitoring Engine.

Key technological inventions at the heart of nexTier's solution are the high performance algorithms; a Semantic-DNA Vector Encoding Algorithm, a Semantic-Security Correlation and Indexing (S^2-COREX) Algorithm, the 3-Dimensional Contextual-Conceptual Reasoning Algorithm, and Automated Security Policy Synthesis and Enforcement Algorithm), which significantly improves the performance and accuracy of any existing DLP.



.

The nexTier Semantic Firewall has a highly scaleable and distributed architecture that is quickly deployed across an enterprise to deliver superior results in terms of both accuracy and with a path to security maintainability. The ability to automatically discover content, automatically classify it, generate security policies in real-time without requiring constant tedious manual intervention, and provide real-time protection against purposeful evasion makes it truly unique and the most effective way to protect enterprise data available today.

Redefining the way enterprises secure data, nexTier Networks combines the most advanced data leak prevention technology with semantic analysis, automating data security with unparalleled insight to discover, classify, assess, and protect data anywhere.

HIGHLY ACCURATE

- Intelligent information discovery with Semantic Vector Encoding and Indexing
- Superior content analysis of unstructured, semi-structured & structured data
- Advanced semantic analysis, classification and correlation

EVASION RESILIENT

- Deep Security~Semantic Correlation
- 3-D Contextual-Conceptual Analysis
- Highly granular security policy control and analysis

HIGH PERFORMANCE & SCALABILITY

- Appliance form factor
- High throughput, real-time information discovery for virgin and/or pre-processed data
- Efficient semantic index storage that is independent of information size
- Processing speeds from 4 Gb/sec (or >100 files/ sec)
- Real-time operation for 'virgin' and/or pre-processed data
- Storage Scalability is upper-bounded to 1000 bytes irrespective of info size versus current DLP solutions that are unbounded

REAL TIME, AUTOMATED

- No pre-marking of policies required
- Intelligent policy engines require minimal to no human intervention
- Requires no change in user behavior
- Real-time automated policy setting & enforcement
- Real-time data monitoring & workflow on enterprise LAN, storage and endpoints
- Comprehensive protocol interfaces & crawlers
- Automated reporting of information extrusion & compliance violations

REAL-TIME INFORMATION DISCOVERY

High performance Semantic Vector encoding & indexing	Smart conceptual search and patent-pending indexing algorithms High throughput - up to 0.5 GB/s (>100 files/second) Real-time processing for "virgin" or pre-processed data Efficient index database storage with upper bounds of 1K, regardless of data size
Comprehensive Network and Application monitoring	Microsoft Exchange email, SMTP, IM, HTTP, FTP, Telnet, SMS, IMS, Mail, SIP, RPC, RMI, Citrix protocols supported
Broad Range of Devices Supported	Crawler examines NAS, database, file systems, and desktops with over 48+ content format decoders
Highly Accurate	Low false positives and Low false negatives

SUPERIOR CONTENT ANALYSIS

Structured Data	Full keyword & phrase matching capabilities identify known data types Expressions can be combined with wildcards and defined constructs
Pattern Matching & Analysis	Full support of Logical and Pattern-based occurrence analysis methodologies Goes beyond traditional Statistical or Bayesian methods
Semi-structured Data (Regular Expressions)	High performance and real-time regular expression (reg-ex) matching algorithms for data such as Credit Cards, Social Security Numbers, Bar Codes, etc.
Unstructured Data	Identify and protect Unstructured Data in real-time

ADVANCED SEMANTIC ANALYSIS

Intelligent Data Classification	Built-in intelligent classification system works with domain ontology to perform categorization & classification that goes beyond transactional data identification
'Security~Semantic' Correlation	Provides superior security-based analysis of unstructured data with minimal or no human intervention required by using a domain ontology database engine
3-Dimensional Conceptual Analysis	Correlates / 'Actors~Operations~Information' in real-time to identify and discriminate between "real" data leak incidents vs. legitimate communications to significantly reduces false-positives & false-negatives. Performs sophisticated correlation by utilizing pre-existing information in AAA, RADIUS, LDAP and Active Directory to automatically create the enterprise's organizational structure and assign clearance levels to Actors

POWERFUL POLICY ENGINE PROTECTS DATA IN REAL-TIME

Automated Security Policy Enforcement & Real-time Reactivity	No pre-marking of security policies required Automatically calculates the 'significance" of information and applies the appropriate policies in real-time with minimal to no human intervention Policies can be set "one-time" at initial configuration Identifies and resolves any internal policy conflicts
Highly Granular Policy Settings	The policy definition interface sets access control policies at varying levels of granularity, as coarse as entire file or document or as granular as a paragraph, sentence, field or words within a file.
User-friendly Security Administration	Central interface for the creation, monitoring and management of system configurations, multiple security administrator's accounts, end-user privilege settings

REAL-TIME MONITORING & REPORTING CONSOLE

Real-time Incident Monitoring Dashboard	Instantaneous reporting of any violation, drill down into DLP incidents, analysis of preventative measures taken, detailed forensic analysis tools
Extensive Incident Reporting and Logging	Reports are generated in a variety of pre-defined and user-defined formats for export into other reporting systems. Multiple reporting criteria is specified through easy-to-use interfaces.
Automated Real-time Compliance Monitoring & Enforcement	Pre-defined templates for compliance including SOX, GLB, SB-1386, HIPAA. Compliance violations are reported real-time so security administrators can take corrective measures.
Health Statistics and Network Traffic Monitoring	Provides health statistics of different modules and network traffic statistics such as traffic throughput rate, monitored protocols and other real-time performance statistics

For more information about nexTier Networks' DLP products, contact info@nextiernetworks.com.

FEATURES

- **Semantic Intelligence for advanced data security**
- **Rapid forensics investigations & troubleshooting**
- **Deploys easily in distributed or stand-alone enterprise architectures**
- **Automatically discovers new data & assigns security values & policies**
- **Enables data to be secured in real-time**
- **Automated fail-over, fail-back and back-up capabilities**
- **Full Services Oriented Architecture (SOA) and Web Services compliant**
- **Creates dashboards for compliance, risk and forensics in addition to managing & automating compliance, business processes.**
- **Breakthrough, patent-pending S^2 COREX™ algorithms discover, classify, and index information in real-time based on the security value of the data's context.**