

Introducing netForensics Cinxi Appliances

A flexible, affordable, high-performance SIEM platform that delivers complete log management and actionable intelligence for secure, compliant operations.

netForensics new Cinxi SIEM (Security Information and Event Management) appliances offer a low cost, easy-to-use solution for managing the deluge of security-related data that inundates your organization every day. Cinxi combines log management, real-time event correlation and alerting, remediation, and reporting in a single high performance solution that simplifies the time-consuming task of monitoring and managing the compliance and security risks that can affect your business operations.

The Cinxi line of appliances are the most cost-effective, yet advanced SIEM solutions available on the market today. Cinxi offers the fastest events per second (EPS) performance, greatest flexibility, most available live data storage, and the lowest total cost of ownership thanks to netForensics simple pricing models and the low overhead required to install and maintain the platform.

And with unparalleled speed and performance, Cinxi provides better situational awareness, rapid in-depth analysis of threats and flexible deployment options to accommodate complex networking environments. Powerful log management and reporting features help ensure you are prepared to prove and document compliance audits.

In addition to being the most powerful SIEM solutions available, Cinxi appliances are also the easiest to deploy and operate. Cinxi can be deployed in as little as one hour and all systems operation and management is made simple through an array of features and an intuitive graphical user interface.



CINXI PROFILE

- :: **Powerful yet affordable log management and security compliance for all environments**
- :: **Lightening fast setup and configuration, very easy to manage and use**
- :: **Automatic correlation and identification of security incidents**
- :: **Rapid access to centralized log data for incident response, forensics, and discovery**
- :: **Service-oriented architecture provides maximum scalability and flexibility**
- :: **Built in Support for over 1,000 devices and applications plus easy device integration tool**
- :: **Includes reporting packs for all major regulatory compliance standards**

A HOLISTIC APPROACH TO SECURITY AND COMPLIANCE

Compliance regulations require perimeter defenses, asset control, event logging, and data security – and so do common security standards. In short, compliance is security and security is compliance. That’s why Cinxi delivers a holistic approach to compliance with real-time collection and alerting of security-related network data, as well as a full range of compliance monitoring and reporting features right out of the box. Whether it’s PCI, SOX, HIPAA, GLBA, FISMA, ISO 27001 or any of hundreds of other global regulations, Cinxi places the information you need right at your fingertips.

INTELLIGENT EVENT CORRELATION AND ANALYSIS

Security threats aren’t getting any less complex, which is why signatures and low-level event rules are no longer effective for identifying network attacks. Cinxi counters those increasingly sophisticated threats with an intelligent event correlation engine and proprietary MetaRules™.

MetaRules™ go well beyond simple rules and signatures by incorporating an advanced logic system that performs real-time attack detection through identification of threat pattern sequences and behaviors across disparate network devices. This means Cinxi can deliver faster, more accurate security event correlation and alerting while virtually eliminating false positives.

Used in conjunction with the built-in case management and remediation tools, Cinxi’s Intelligent Correlation and Alerting suite gives IT managers and security specialists everything they need to detect, respond and resolve even the most sophisticated security events when and where they happen.

UNMATCHED SECURITY VISIBILITY

Cinxi provides a complete view of enterprise security posture and rapidly identifies suspicious patterns of activity that would otherwise go unnoticed. Multiple views of actionable security information are tightly integrated with reporting and analytics to rapidly and intuitively pinpoint the true threats.

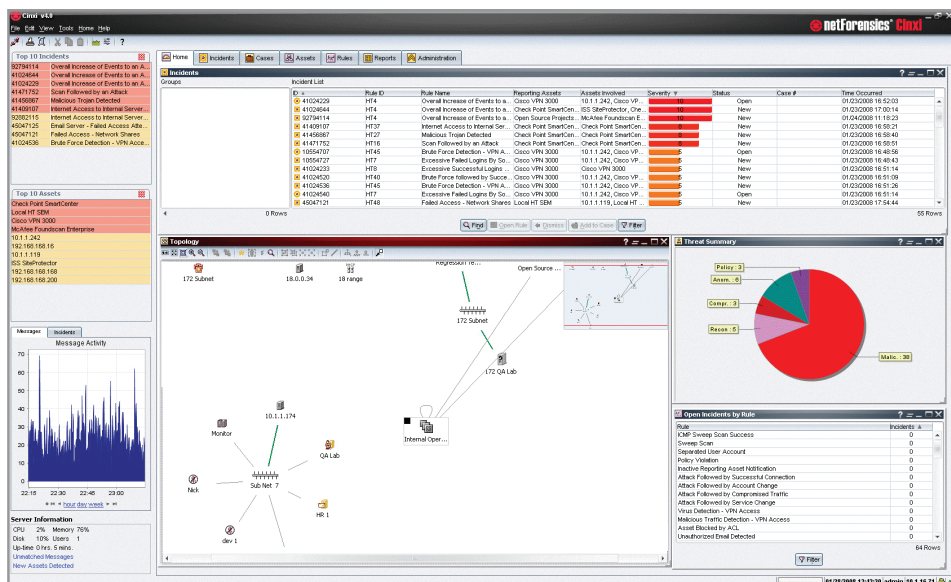
POWERFUL, CENTRALIZED LOG MANAGEMENT

Even modestly sized networks can have hundreds or thousands of systems and devices generating huge volumes of security-related data that make log collection, management and archival a nightmare for IT and security professionals. With Cinxi’s powerful log aggregation and management capabilities, centralized log collection is a snap. Fast and flexible, Cinxi supports more than a thousand different types of network devices, hosts, and applications right out of the box. And through Cinxi’s unique Device Class technology, new reporting devices are easily added to the system ensuring comprehensive, ongoing support for your environment. All Cinxi SIEM appliances feature software-based encryption encryption of all data at rest.

FLEXIBLE, SCALABLE AND LOW TCO

Experienced IT professionals know that there’s no such thing as “one size fits all.” That’s why Cinxi offers multiple hardware platforms and a flexible Service Oriented Architecture (SOA) that integrates with virtually any network environment of any size or configuration. Whether your network is highly centralized or fully distributed; low bandwidth, regional, national, or global, Cinxi has the horsepower and flexibility to integrate with your network on your terms.

Best of all, there is no additional hardware or software to purchase. From one location to thousands, Cinxi’s Master Console coupled with flexible analytics and reporting modules allow you to easily fine tune your Cinxi deployment to best meet the unique event management and compliance requirements of your organization.



Cinxi Delivers a Powerful Suite of Capabilities for Log Management and Security Compliance

- **Event Logging and Storage:** Cinxi enables rapid incident investigation and convenient access to all audit and incident data by storing raw logs and correlated records on the same device. And with up to 8 TB of onboard storage and the ability to add an additional 45 TB of near-line storage, Cinxi appliances enable long-term, fully-accessible data retention.
- **MetaRules™ Correlation:** Cinxi intelligently analyzes all event messages to identify patterns of attack, filters out false positives and prioritizes critical events. All data related to incidents are tagged in 'threads' so users can easily identify any effected assets and systems. Incident names such as "Credit Card in the Clear," "Policy Violation," and "Malware," make it easy for even non-technical team members to understand the nature of a threat.
- **Rapid Drill-downs and Incident Summaries:** Incident information is accessible from nearly all screens within the Cinxi GUI, and details on incidents are immediately available with an absolute minimum of clicks. Users can quickly investigate all incident-related information and see who was involved in an incident, what systems were affected and how the attack occurred.
- **Real-time Incident Identification:** Cinxi's blazing fast engine normalizes, parses and correlates incoming messages in near real-time. Administrators can see threats and attacks the second they are reported, have time to secure systems and prevent the attack from negatively impacting the network and connected assets.
- **Vulnerability Scan Integration:** By incorporating vulnerability data into its correlation technology, Cinxi can alert administrators to the true threats, the incidents that have the potential to exploit your systems.
- **Zero-day Attack Identification:** Using powerful behavior-based analysis, Cinxi identifies new attacks that follow similar patterns to past attacks, but use different types of connections to bypass signature-based countermeasures.
- **Built-in Incident Remediation:** Comprehensive workflow management provides best-practice recommendations for remediation, mitigation, centralized case tracking, and automated notification, so incident response personnel know what to do and administrators have clear insight into the actions of their team.
- **Security and Compliance Reporting:** Cinxi delivers detailed reports to aid in investigating incidents and compare new threats against historical data. Users can gain a better understanding of how an incident occurred, if there has been previous related activity, and what systems might have been affected. Cinxi's reporting system enables fast, easy searches of raw logs based on a wide-range of criteria. Pre-configured reports specific to a variety of compliance regulations include PCI, SOX, HIPAA, GLBA, FISMA and ISO.
- **Extensive Device Support:** Cinxi includes out-of-the-box integration support for over 1,000 devices, systems and applications. An integrated device builder tool lets you quickly and easily add support for other data sources and proprietary systems.

Cinxi | Express™



Cinxi Express is a 1U rack-mountable appliance that delivers full log aggregation and event correlation capabilities. Designed for installations with modest network traffic volumes and incident frequencies, the system offers full-featured log retention, access to threat data, and security and compliance reporting. Logs and/or security alert information collected by Cinxi Express can be rolled-up to any other Cinxi appliance for regional or global overview of activities.

Cinxi | Ranger™



Cinxi Ranger is a 1U rack-mountable appliance offering full scale, high performance Security Information and Event Management capabilities. Ranger appliances can be used as standalone SIEM solutions in small and medium-sized environments, or incorporated into a larger distributed architecture for enterprise-class deployments.

Cinxi | Midway™



Cinxi Midway is a 2U rack-mountable appliance designed for medium to large environments with higher volume data collection, correlation, and storage requirements. Midway appliances can be used as stand-alone solutions, as the centralized log storage and management component in a distributed architecture, or as regional solutions that roll-up to Cinxi Enterprise appliances.

Cinxi | Enterprise™



Cinxi Enterprise is designed to meet the most demanding enterprise-class log management, compliance, and security threat analysis requirements. Deployed as a stand-alone solution or as the central component(s) in large-scale global deployments, Enterprise is the ideal solution for organizations that require log collection and analysis from a multitude of locations with centralized management.



Cinxi Vault is an optional add-on storage cabinet to accommodate high volume long-term data retention. It is the ideal solution for organizations that wish to centralize log storage for security or regulatory compliance requirements. Data stored on Cinxi Vaults is online “live” data accessible in real-time, so all SIEM reports and analysis are available on-demand without having to restore archived data from offline resources.

KEY CAPABILITIES

- 15 TB near-line storage
- Deploy up to 3 Vaults in sequence for a total of up to 45 TB
- Fiber Channel
- SATA Array
- Hot-swappable high availability drives
- Hot-swappable redundant power supplies

SUPPORTED DEVICES

Cinxi Vaults are compatible with the following Cinxi Appliances:

- Cinxi Enterprise
- Cinxi Midway

TECHNICAL SPECIFICATIONS

	EXPRESS	RANGER	MIDWAY	ENTERPRISE	VAULT
Description	SIEM Appliance	SIEM Appliance	SIEM Appliance	SIEM Appliance	Near-line Log Storage
Events per second	14,826 EPS	34,656 EPS	69,312 EPS	115,520 EPS	-
Processor	1 Xeon Dual Core	1 Xeon Quad Core	1 Xeon Quad Core	2 Xeon Quad Core	-
Form Factor	1U	1U	2U	5U	3U
RAM	4GB	8 GB	32 GB	48 GB	-
Storage	2 750GB SATA discs	2 1TB SATA discs	6 1TB SATA discs	8 1TB SATA discs	15 1TB SATA discs
RAID	1	0, available with 1	5	5	5
PERC 6 RAID Controller	No	No	Yes	Yes	Yes
NIC Cards	2	2	2	2	2

SUPPORTED DEVICES FOR CINXI EXPRESS, MIDWAY, RANGER AND ENTERPRISE

- AAA
- Antivirus Software
- Content Monitoring
- COTS Applications
- Custom Applications
- Database Servers
- DHCP Servers
- Email Servers
- File Management and Integrity
- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Load Balancing Software
- Operating Systems
- Routers
- VPN/SSL VPN
- Switches
- Vulnerability Assessment Scanners
- Web Servers
- Windows Host Agents *and more*



June 30, 2008

- “The strength of Cinxi SIEM lies in its simplicity. Cinxi was up and collecting data in literally minutes.”



May 25, 2006

- “This is the first time we’ve used Cinxi and we’re impressed!”
- “...it was our go-to product for many investigative efforts”
- “Cinxi will be hard to beat!”



PRODUCT RATING	
Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★☆
Overall Rating	★★★★★

- “We found Cinxi to be quite simple to use due to the intuitive user interface”
- “This SEM appliance has many excellent features”
- “...a good value for the money ...a good investment”

