**Attivo Networks** - With the BOTsink Solution, you can immediately uncover attacks brought into your network, typically unwittingly by users who often bypass existing security measures -- you quickly and accurately identify BOTs and APTs that may have been introduced by infected: Employee-owned devices – BYOD mobile workers accessing resources remotely, outside the firewall and 3rd party vendors and suppliers; Unlike traditional security solutions that are inline and rely on signatures (attack patterns) and known attacker command and control (C&C) addresses to try to identify suspicious attack activity, Attivo BOTsink Solutions focuses on the attackers that reached the network. It looks for BOTs and APTs probing your environment looking for your high value assets; it accelerates their detection, so you can stop them before they can reach their destination.

**Gigamon Systems** - Gigamon provides a data access switch for unobtrusive, simultaneous connectivity from any access point (span port or tap) to any monitoring, analyzing, or security tool. The GigaVUE-MP multiplexes, aggregates and filters traffic. Multiplexing solves the problem of too few span ports for too many tools, enabling multiple tools to share a single access point. Aggregation saves money by combining traffic from multiple access points to one or more tools reducing inefficient distributed tool expense and providing a unique total network view. Hardware bit-mask filters enable custom mapping of individual packets or session streams from multiple access points to multiple tools, enhancing tool performance and effectiveness.

**ThousandEyes** - Extend monitoring visibility beyond enterprise networks into the Internet. Troubleshoot DNS, BGP, IP, TCP, VOIP, MPLS and other network technologies. Quickly correlate network and application layer metrics to optimize performance. Customize alerting to be notified of performance or security issues. Easily deploy with lightweight agents and cloud-based software platform ThousandEyes monitors internal and external network performance to pinpoint where and why network issues occur, improving application delivery and reducing service interruptions. Your enterprise IT, online operations and network security teams will be able to instantly identify the source of problems, even if it’s outside your network.
Splunk - Splunk is a powerful search engine for logs and IT data. It indexes, manages and enables you to search logs and data from any application, server or network device in real time. Splunk is easy to download, install and use. Enterprises users are able to achieve higher availability, meet compliance requirements and cut IT costs. Splunk achieves the highest performance technology for IT data and provides optimal availability in applications and services. The product facilitates and automates alerting and reporting. It also reduces operations costs and the time needed to investigate and resolve performance issues directly contributing to increased internal and external SLA performance.

Gemini Data provides a situational awareness platform that removes complexity from big data, quickly applies context to fragmented data using AI, and securely shares investigations across your organization. Gemini was founded by big data and security experts from Splunk and ArcSight, with decades of experience developing and deploying large scale systems for enterprise customers.

Uila- Uila gives IT infrastructure teams x-ray vision for their data center operations and end user experience. Designed for Private, Public and Hybrid Cloud environments, Uila’s Application-Centric Data Center Infrastructure Monitoring and Analytics provide instant visibility into hotspots and bottlenecks in any data center. Uila provides service dependency mapping, full stack correlation with 1-click root cause analysis and patented deep packet inspection technology that understands over 4,000 application protocols for transactional meta data analysis. Businesses use Uila to align themselves with their IT Operations team and cut time to resolution from days to minutes, keep their application at peak performance at all time and ensure end-user satisfaction to the fullest.

Calligo is an innovative global cloud service provider offering companies the highest levels of data privacy and security. Key Services that Calligo provide include:

- Trusted Cloud platform with a strong emphasis on data privacy. Calligo can service your data within “Safe Harbor” jurisdictions as required.
- A GDPR enabled cloud platform.
- GDPR requirements and gap analysis consultancy.
- DPOaaS (Data Protection Officer as a Service). A requirement for meeting GDPR.
Calligo offers unparalleled application performance guarantees. Commercial flexibility and personalized support service from our globally located cloud platforms. Calligo can provide “high touch” services that organizations can trust to deliver desired levels of individualized support. And the protection they expect and that is lacking in many other cloud offerings.

**eGinnovations.** – eG is a global provider of performance monitoring, root cause analysis and triage solutions for both virtual and physical IT infrastructures. The company’s patented technologies provide proactive monitoring of every layer of every tier in the infrastructure, thereby enabling rapid diagnosis and recovery in enterprise and service provider networks. By ensuring high availability and optimum performance of mission-critical business services, eG Innovations’ solutions help enhance customers’ competitive positioning, lower operational costs and optimize the performance of their infrastructures. The product offers superior Virtual Desktop (VDI) and Citrix monitoring.

**Infoblox** - Infoblox is the leading developer of network identity appliances that connect applications to the network infrastructure. Infoblox’s appliances for IP Address Management, DNS/DHCP, RADIUS, and LDAP help companies build infrastructure that is more secure, easier to manage, and more reliable than traditional solutions—and Infoblox’s distributed platform simplifies management across the network. These appliances simplify and secure the network by hardening the delivery of each protocol and they work together to provide true integrated identity services and centralized data management. Infoblox’s products help businesses build networks that are more secure, cost less to operate, and easily scale as network infrastructures grow.

**InfoBlox (Trinzic Network Automation)** – Trinzic provides change monitoring and tracking which shows who changed what, where and when it occurred. Collection and archiving of current and all historical configurations with easy-to-view, side-by-side comparison is provided. Job creation, including dynamic template selection based on device, network attributes and location is simply achieved. Easy imports exist for Perl scripts as well as access by additional staff for automation of complex changes with dynamic templates or script variable population. User-based permission controls ensure individuals have access to only desired devices or locations. Job approval process is available for multiple authority level and peer review enforcement when needed. Single or multi-device change execution is standard. A rollback option can be invoked to return configuration settings to those of a previous template during a disaster recovery. Update real-time device configuration and attributes with CMDB can be utilized as necessary.
NIKSUN’s NetVCR is an advanced real-time network appliance for service and application performance monitoring. It intelligently integrates vital management functions into a single scalable architecture to facilitate proactive end-to-end SLA/QoS measurement, reporting and surveillance. NetVCR provides a large array of benefits including proactive alerting from link to application, point and click diagnostics and troubleshooting. Advanced functions include planning/trending, accounting/usage (including DiffServ), Application services monitoring includes e-commerce, email, VoIP, Multicast, FIX, custom applications, Performance analysis includes loss, delay, latency, jitter, service/application response time, good output, throughput and seamless integration with other management systems.

Netskope's cloud application visibility, control and analytics are very strong. The depth and flexibility of its product features are differentiators in the cloud security market. Netskope enables companies to Identify & encrypt (or block) specific data in transit as it’s being uploaded into the SaaS app. The product will also encrypt data already residing in those repositories (such as OneDrive - the storage drive for Office 365, or DropBox, Box, etc.) Netskope also provides blocking of sharing data residing in those sanctioned repositories to other storage apps. Lastly, the application enables for the protection of data being accessed outside of the firewall perimeter via mobile devices.

**SecureSphere Platform** - The SecureSphere platform provides database, file and web application security across physical and virtual systems in data centers, including those in traditional on-premises data centers as well as those in private, public and hybrid cloud environments. With flexible deployment options and administration capabilities, SecureSphere provides the scalability, adaptability, and management you need to achieve state-of-the-art data center security. Among the modules are Cloud Security, Incapsula DDoS Protection SecureSphere File Security, SecureSphere Web Application Security and SecureSphere Database Security.

**PacketViper** - a point and click Geo IP (country) network filtering appliance. In just a few clicks of a mouse, block entire countries' networks from accessing your critical network infrastructure. Or, specify which countries may access specific ports on your network, while blocking other countries completely. Other unique features include: Real-time display of traffic accessing your network. Includes country of origin of traffic. Clickable logs display detailed information about an IP address or host such as location, domain, “whois” information, number of times accessing your network, and administrator's tools such as ping, traceroute, RBL match, and the ability to instantly block the network. Triggered traffic events send administrators email and text notifications, rate-limit an IP, or permanently ban an IP. Many more important features are also included.
Sophos UTM helps you consolidate your security without compromising its effectiveness. By combining multiple security layers, it’s simple to protect your users everywhere while making security easier to deploy and manage. Modules include VM, Wi-Fi, Web gateway and email gateway. Also, there are products for AV, cloud and encryption. Finally, there are applications for Sharepoint, database and server security.

**Smart OOB™** out-of-band management with auto-response and remediation. Opengear delivers a new generation of remote management solutions to meet the growing necessities of always-on connectivity and resilience. By utilizing Opengear’s **Smart OOB™**, businesses are able to monitor, access, and manage virtually any electronic device on their network — remotely and securely — from anywhere, even when the network is down. The unique combination of remote access and monitoring capabilities include auto-response and remediation, plus OOB over cell/dial and Failover to Cellular™ backup. All features are easily managed from a centralized console.

**Tufin** - Delivers Best-In-Class Network Topology Intelligence and the first firewall management solution to enforce user and application level firewall policies. The product is the leading provider of security lifecycle management solutions that enable companies to cost-effectively manage their network security policy, comply with regulatory standards and minimize risks. Some of the areas which Tufin address include: firewall/network device auditing and monitoring of workflow. Additionally, optimization of rule base security on firewalls and network devices is one of Tufin’s many key strengths. PCI and other auditing reports on firewalls and infrastructure devices are core features and troubleshooting takes minutes on virtually any issue.

Bastille is the first company to enable enterprise security teams to assess and mitigate the risk associated with the growing Internet of Radios. Bastille’s patented software and security sensors bring visibility to devices emitting radio signals (Wi-Fi, cellular, wireless dongles and other IoT communications) in your organization’s airspace.

Bastille’s technology scans the entire radio spectrum, identifying devices on frequencies from 60MHz to 6 GHz. This data is then gathered and stored, and mapped so that you can understand what devices are transmitting data, and from where in your corporate airspace. This provides improved situational awareness of potential cyber threats and post-event forensic analysis.

**LiveAction Networks** - APN develops intelligent, action oriented software allowing IT professionals to master complex network operations with extreme ease and confidence. The company's LiveAction software leverages the existing technology and features inside network devices to maximize return on investment and provide intelligent on-the-fly router configuration, monitoring, and troubleshooting. Live topological flow and route visualizations enable instant comprehension and understanding of complex networks. LiveAction's extensible framework and built-in knowledgebase deliver cross-technology analysis for QoS, NetFlow, Routing, IP SLA, and more,
in a single easy to use tool. LiveAction enhances the speed and productivity of IT engineers tasked with performing end-to-end QoS for VOIP, IPT and UC deployments and troubleshooting.

**VMTurbo** is the world’s only software-driven control solution that automatically maintains virtualized datacenters and private, public, and hybrid cloud infrastructures in the most optimal state. VMTurbo is a sizing, placement, and configuration decision engine that assures application performance while dramatically reducing the cost to deliver compute services through ongoing efficiency gains. Continuously assure workload performance. VMTurbo’s algorithm dynamically allocates and realigns resources based on real time workload demand. Simulate adding workloads, VDI rollouts, DR failover, & more. VMTurbo is hypervisor agnostic, controlling VMware, Hyper-V,XenServer, RHEV, and KVM – heterogeneously or in isolation. VMTurbo also integrates with cloud tools vRealize Automation, SCVMM, CloudStack, and OpenStack to deliver multi-domain cloud control. A single instance controls up to 10,000 VMs and requires just 4 vCPU, 16GB Mem, and 20GB disk.

**Thycotic Secret Server** delivers a comprehensive Privileged Account Management solution set to protect your most valuable information assets from cyberattacks and insider threats. Thycotic Secret Server, Application Control, Local Security and Security Analytics solutions protect privileged accounts and enables organizations to enforce least privilege policies for business and administrative users, as well as control applications to reduce the attack surface without halting productivity.

The solution helps organizations revoke everyday local administrator privileges from business users while seamlessly elevating privileges when required by trusted applications.

Complementing these privilege controls, the solution also delivers application controls, which are designed to manage and control which applications are permitted to run on endpoints and server

**Morphisec** – blocks malware at the beginning of the kill chain by morphing the system resources. The malware cannot deliver the payload and is captured for further analysis. Antiviruses, IPS and firewalls use signatures and behavioral analytics, have many false positives and cannot stop zero-day, one-day, PowerShell and polymorphic malware attacks. Morphisec protects from in-memory attacks on 32 and 64-bit application, all web browsers and productivity applications running on 32 and 64 bit versions of Windows 7, 8, 8.1 and 10 on Windows 2008 and 2012 operating systems. These include for example: All web-borne attacks such as ransomware, all malicious files such as Adobe and Office documents, malicious sites containing Flash, Silverlight and Javascript attacks, attacks on Java that use shellcode to run payload (all recent attacks) and vulnerabilities exploited by file-less and non-persistent malware. Morphisec is paving the road with this new preventive technology saving companies on the average $3.2M a year in detection and remediation costs.

**CloudOptimize** – brings leading edge services and solutions to increase adoption and utilization of AWS, Google & Microsoft Cloud instances.
CloudOptimize offers powerful software that reports on billing information from the Cloud Service Providers (CSP’s). This data brings compelling assessment analyses and reports on capacity and utilization. Additionally CO provides suggested actions that dramatically increase ROI. Trending information and “what if” can be implemented and these projections offer actions that will add greater efficiency and effectiveness to the operation of Cloud applications.

**InnoSec** – provides a cyber risk management solution STORM that allows companies to measure *business asset risk* in terms of their cyber security controls. STORM provides a complete end-to-end solution for CISOs, CEOs, Compliance managers and every member of the cyber security ecosystem to focus and prioritize cyber risk mitigation. It allows business to tie strategic decision making with operational cyber activities and includes asset management, vulnerability management, remediation management, project and task management and compliance management. It integrates with SIEM and vulnerability scanners and provides real time data to the organization. STORM competes with EMC Archer and Metricstream and beats them on ease of implement, customization and cost. It is used by leading organizations like Amdocs.

**Kela**- Kela disrupts cyber-crime by leveraging dark web intelligence. The dark web is the google of the cyber-criminal world with relationships, offers, transactions, and illegal activities are bought and sold. Data on business executives, domains, vendors and other organization data is at risk from these dark forces. Kela’s RaDark exposes cyber criminals and their activities at the design and planning stages within The Dark Web and provides alerts for organizations to prioritize actionable intelligence.

- Demonstrates targeted threats against employees, corporate officers, facilities & resources
- Shows what type of attack is being planned – targeted phishing, data leak, etc.
- Where and when they will attack
- Who the attackers are and their motivations
- Which attack methods are being used

**Cybeready** - Provides phishing campaigns that are customized to each organization. Rated among the top three types of cyber-attacks since 2009, phishing is an email-based, social engineering attack. Messages disguised as legitimate communications lure a recipient’s response: clicking a link, opening an attached file, or transferring sensitive information. Security awareness is the first line of defense against malware. 90% of malware is accomplished using phishing attacks. 30% of users click on unsafe links and urls. When an employee opens a link within a fake email, he or she is then “marked” as a risk in the readiness report, and is led to a customized, white-label landing page. This page includes explanatory copy on the nature of the phishing “drill” and a short instructional video showing how to identify phishing emails.

Cybeready provides smart analytics each month to your organization with a CybeReady Report (an organizational readiness report) monitoring employee’s behavioral data in light of different phishing
attacks, the level of risk the organization is exposed to, and employees’ learning curves.

**Dyadic** – is the World Leader in Software Defined Cryptography and provides advanced authentication solutions and enterprise key management for the cloud. Dyadic has a unique software-based technology that features security guarantees previously only available on dedicated hardware. Based on Multi Party Computation (MPC), researched for the last 3 decades, Dyadic co-founders, Professors Smart and Lindell are world leaders in cryptography. Dyadic provides a novel one-of-a-kind software solution that enables EVERY mobile, laptop, desktop and server to have a Virtual HSM (vHSM). Key management use cases include code signing, SSL certificates, document signing, app-level encryption, database encryption, authentication, certificate authority, PKI infrastructure, and VPN gateways. Dyadic enables organizations to move securely to the cloud while gaining back control on protecting data and access. No need to share the data protection responsibility with the cloud provider.

**I am Real** - I am Real provides 3D verification using Social network verification and video face validation for on-line lenders, shared economy, peer-to-peer e-commerce, dating sites. I Am Real compares passport / driving license to the live video of the user and cross-correlates the name on the card to the user’s social presence. This provides high assurance that the photo and name appearing on the card are of a real living identity. I Am Real enables websites, applications and content providers to verify their users against their online profiles. This helps businesses satisfy their KYC/AML requirements, increase trust and loyalty and grow their user’s base and decrease risk and fraud, which results in increased revenue. I Am Real offers a complementary service for validating the true face of the user. A ten second video of the user is taken in real time, and our patented algorithms compare the claimed user photo to the taken video, in addition to voice matching the video and a random voice challenge. This feature provides further confidence in the identity of the user. Online lenders use I Am Real technology to validate their users, reducing risk and preventing abuse of credit cards.

It establishes mutual trust in shared economies between landlords and tenants, by ensuring each knows the real identity of the other. Peer-To-Peer platforms use I Am Real to enable a safer and more reliable commerce, by detecting fraudulent users on the one hand, and increasing reputation of verified users on the other. Multiply traffic and transactions by increasing your users’ feeling of trust. Dating Sites can increase their site’s user acquisition rate by enabling your users to trust and know that they are interacting with real people who were verified to be the person they claim to be. I Am Real authenticates the validity of payment gateways for their merchant identities, reducing the risk of having a fraudulent merchant trying to generate illegal revenue.
L7Defense – The L7 Defense Ammune™ technology (patent pending) is designed to protect organizations against the full spectrum of modern application-level DDoS attacks. By incorporating the most up-to-date immune system models enhanced with advanced machine learning technology, Ammune™ ensures continuous, real-time protection of the organization’s application systems. Ammune™ mitigates application-layer DDoS attacks in seconds! The Ammune™ DDoS protection system is a software solution implemented "locally", on-premises or on cloud-based servers. In the near future, the system will be available to customers in major public clouds (Amazon, MS…). The Ammune™ system includes the following major components: 1. The Reverse Proxy (RP) server mitigates attacking requests with "dynamic filters" enabling good traffic to pass. Optimized filters are also sent from the Algorithms server. 2. The IO server picks relevant traffic data and passes to the Algorithms server. 3. The Algorithms server processes the chosen traffic data, determines if an attack has been initiated, and defines new, optimized filters to mitigate it. 4.The Web services server securely passes the data between the UI system, DB & other modules and systems at RT. The basic system consists of all modules (except RP) gathered under the Back office (BO) system and placed on a single server instance. The Reverse Proxy is placed on a different server instance.

Intezer - provides Code Intelligence which takes all the files from an organization and dissects them to their most granular components identifying malware. Using advanced machine learning and its proprietary database, information regarding the file is provided in a report to the organization. As an example; this file is a maliciously tampered version of Photoshop. It uses code from ZeuS malware that gives full control on the victim computer. It also contains never-seen-before code that probably adds another capability. Organizations use this information to do file cleansing and malware eradication.

PlainId – PlainId is a business authorization drag and drop application that allows the business to manage authorizations. Defining Authorizations and Access are costly and the primary reason why IAM projects fail. PlainId empowers authorizations and Access in an automated, drag and drop application providing the high success rate needed in today’s connected enterprises.

Authorization Management is the key to IAM project success whether migrating to the cloud, consolidating ERPs or just providing the right access to the right people. PlainId addresses the authorization challenge that arises whenever businesses demand support of their rapid growth, expand their boundaries across devices and require multiple entities control. It is used across enterprises in conjunction with IAM solutions, for cloud migration and call centers. Most IAM, AIG, and IdaaS solutions are a decade or two old, usually acquired from companies that are long gone, are very difficult to implement and maintain and do not fit for cloud, multiple device, call center or mobile adoption. They typically do not provide any authorization solution. They require additional, manual operation from their
customers to manage accounts across all platforms and in the cloud. PlainID provides the following features: Immediate ROI for implementing new applications, Event driven authorization control, Multiple-entities authorizations management, Business oriented approach to authorization management, Dynamic and flexible rule engine, and Centralized management.

ReSec - ReSec's Content Disarm and Reconstruction (CDR) technology prevents malware from entering your organization and ensures that only threat-free, ready for work files are allowed in. There are no false alarms - just clean functioning files that your users can trust to get their work done. Current security solutions must detect malware in order to defeat it. They look at the past to identify and block files that have patterns (signatures) similar to known malware strains, or stimulate files in a sandbox environment to detect malicious behavior. Attackers constantly study these existing signature and behavior-based solutions and are developing new methods and strains to evade them.

A new breed of solution is needed to ensure that malware never gets a foothold inside your organization - without slowing down or disrupting your critical processes and day-to-day work through costly false positives and overly restrictive policies. Resec provides solutions for all attack vectors including email, cloud mail, FTP, Server, Endpoint, vault, file server and file portal.

SecDo - SecDo detects, blocks and remediates ransomware attacks. With cutting-edge deception technology, SECDO tricks ransomware into revealing itself, then freezes the ransomware before files are encrypted. Using the SECDO platform, you can then investigate and remediate the threat both on the affected endpoint, and across the entire organization. The frequency and sophistication of ransomware attacks are growing rapidly. Like other types of advanced malware, ransomware avoids conventional endpoint protection, and has already caused hundreds of millions of dollars in damage. To increase the stakes, hackers are now targeting hospitals, schools, banks and other organizations that cannot afford to shut down operations. Since ransomware is so destructive, it is essential to detect and stop it quickly, before files are encrypted. That is easier said than done, since ransomware uses evasion, reconnaissance and stealth tactics to detect and avoid or disable security solutions.

VNT Provides software that helps companies easily migrate their datacenters to the cloud. IlluminIT from VNT automatically generates a visual map of their application environment and a central repository of business services and the supporting infrastructure. In just a few hours, in the datacenter IlluminIT starts mapping critical business applications. IlluminIT uses a combination of active and passive mapping technologies to capture each business service and correlate it to the relevant servers and related infrastructure. IlluminIT’s unique active
mapping technology “crawls” the application, similar to an end-user, to activate and capture the business services and underlying servers. The passive technology “listens” to real user traffic in order to complete the map. To enable the passive mapping, Organizations are able to simulate the impact of environmental change on their business applications, to prevent downtime. And when incidents do arise, they are able to diagnose and resolve them faster. For the first time, the entire IT team has a complete, accurate picture of the application environment, to improve the efficiency of both the planning and implementation of services and infrastructure upgrades. As a company transitions to the cloud, IlluminIT is proving to be a vital tool for ensuring a smooth, on-schedule migration. From the beginning, IlluminIT uncovered discrepancies between the cloud and datacenter environment, preventing disruptions to critical services.

**Crossware Mail Signature** – Crossware creates professional and consistent email signatures to be appended to every corporate email which includes a company’s branding, advertisements and legal disclaimers. The product ensures all emails sent from mobile devices include your company’s email signature. It controls all of your email signatures from one configuration database. Install it on the server. No need to configure signatures on individual workstations. Crossware Mail Signature removes the need to configure signatures on individual workstations, and requires no design changes to your directory or mail template. You can centrally manage the design of your signature block, including logos, fonts and also include personalized information from your Corporate Directory.

**Palo Alto Networks** – a “next generation” firewall. Palo Alto firewalls enable unprecedented visibility and control of applications, users, and content – not just ports, IP addresses, and packets – using three unique identification technologies: App-ID, User-ID, and Content-ID. These identification technologies, found in every Palo Alto Networks’ enterprise firewall, enable enterprises to embrace Web 2.0 and maintain complete visibility and control. Content-ID uses a stream-based scanning engine and a uniform signature format to look for and block a wide range of attacks including vulnerability exploits, viruses, spyware, and worms. Stream-based scanning means that threat prevention begins as soon as the first packet is scanned while the uniform signature format eliminates redundant processes common to multiple scanning engine solutions (TCP reassembly, policy lookup, inspection, etc.). The result is a reduction in latency and improved performance.

**Plixer** – The Scrutinizer™ incident response system provides forensic insight into the users and applications that are raising suspicions or causing the most congestion problems. Using flow technologies such as NetFlow, IPFIX, sFlow, J-Flow and others, Scrutinizer is able to collect, archive and quickly retrieve the traffic details you need surrounding an incident. FlowPro™ is inserted into areas of the network where visibility is needed, but lacking. It uses deep packet inspection (DPI) to compile a flow cache and exports traffic and threat details reflecting 100% of all...
communications that pass it. FlowPro is a great complement to the Scrutinizer Incident Response System and ensures your security team has insight where they need it. The Flow Replicator™ allows numerous streams of log data to be transparently replicated to several destinations. It also acts as a syslog-to-IPFIX gateway by listening for sysslogs, extracting the details and forwarding them on inside IPFIX datagrams. This all-inclusive network appliance is equipped with a simple, web-based user interface for administration.

**Catchpoint** - a flexible, easy-to-use tool that allows you to monitor your system in real time, helping you quickly identify & resolve performance and availability issues before they affect your bottom line. A comprehensive set of monitors can be used to examine web-based services from the user perspective. Analyze communication speed, behavior and page structure for web applications, APIs and websites. Standard charting tools highlight common areas where problems arise and detect problems and identifies culprits. Monitor any server or service in your data center, private cloud or public cloud.

**IdentityFinder** – Offers classification and workflow with notifications, sophisticated search for personal information, toxic data, intellectual property management and comprehensive reporting. IdentityFinder provides for Breach Prevention, Data Discovery, Risk Management, Privacy Enablement, HIPAA Compliance, PCI Compliance, E-Discovery, Industries. Manage the entire sensitive information lifecycle: Discover, Classify, and Remediate nonpublic data anywhere it is stored within your enterprise. Centrally manage operations, track workflow, generate reports for compliance, and enforce remediation to reduce your risk.

**Tripwire** is rapidly growing, continuing to be the market leader for security configuration management, configuration compliance management, vulnerability management, and reliable log collection management. Auditing the configurations of IT systems and monitoring changes in those configurations is critical to reducing security risk and achieving compliance. Tripwire solutions are being aggressively implemented by large enterprises for overall integrity monitoring along with continuous monitoring of systems and network device changes. This has universally been determined as the most effective way to safeguard an enterprise network. We accomplish this in real-time, where other solutions cannot.

**mailWatch** offers enterprise email protection technologies and services in various flexible deployment options. We have a solution for you - whether you host your own mail server, host in the cloud, or are looking to move there. In addition to advanced email threat protection, the product offers productivity and security solutions that help organizations lower costs and ease administrative burdens while offering users increased flexibility. These services include communication, mobility and collaboration services based on Microsoft Exchange®. Also available are industry leading compliance and discovery solutions that include email archiving, file archiving and secure end to end encryption. All of the mailWatch additional services are cloud-based, can help your organization save money immediately and are backed by the company’s amazing and industry leading support organization.

**Entuity** – Entuity offers network management and service delivery solutions at price points to match a range of business models. The
Company’s line of Eye of the Storm (EYE) software automatically discovers and captures unrivalled network data and analytics. EYE’s powerful capabilities provide integrated fault, device and flow-based performance management. These capabilities enable businesses to reduce network downtime, lower operational and capital costs, achieve sustainability goals, commit to, deliver and prove service level commitments, and ensure network configuration compliance. Entuity supports contemporary IT initiatives including wireless, VoIP, virtualization, high availability, NetFlow, green IT and more.

**WildPackets** - the leading provider of network, application performance, and protocol analysis, VoIP monitoring, and troubleshooting solutions. WildPackets solutions are fully extensible and include training, professional service, custom engineering, and support offerings. WatchPoint provides enterprise-wide network monitoring and reporting. It brings aggregation and expert analysis of NetFlow, sFlow, and packet data to a new level by offering Web 2.0 dashboard-style reporting of network traffic and application performance trends across the entire enterprise. OmniPeek network analyzers perform deep packet inspection, network forensics, troubleshooting, and packet and protocol analysis of wired and wireless networks. TimeLine network recorders and OmniEngine software probes monitor and analyze NetFlow, sFlow, and packet data at remote locations and protocol analysis, VoIP monitoring, and troubleshooting solutions.

**Apposite** – Apposite Technologies makes WAN emulation easy by offering high-precision network emulation tools with unmatched ease-of-use at unbeatable prices. Apposite’s Linktropy and Netropy WAN/LAN emulation appliances simulate bandwidth, latency, loss, congestion, and other network impairments with fine-grained precision to provide accurate simulations of any type of wide-area network. Emulate networks from DSL to 10 Gig, Linktropy and Netropy install and configure in minutes. The products are reasonably priced Apposite’s network emulation products are used by leading enterprises, application and equipment vendors, government and military organization, test labs, and telecoms carriers around the world.

**Imation (IronKey)** - Imation has created the world's most secure hardware encrypted USB flash drive. IronKey products and services bring the power of authentication, encryption, identity management, and privacy to consumers and businesses around the world. IronKey integrates world-class security expertise with product design that emphasizes usability, simplicity, and accessibility. All IronKey products are FIPS 140-2 Level 2 certified. There is no need to install software or drivers, so the IronKey devices are truly mobile. All user data on an IronKey is encrypted with high-speed military-grade hardware encryption. Unlike software-based encryption, this “always-on” protection cannot be disabled and is protected against cold-boot and brute force attacks.

**Zscaler** - The Zscaler Security Cloud enables IT organizations to replace many different point security products with a single, cloud-delivered solution to deliver the industry’s most advanced suite: User Security - protect users accessing the Internet from any location, on any device. Application Control - effectively leverage the benefits of cloud applications and social media, while reducing security risks. Data Protection - perform full inspection of all Internet traffic leaving the organization, with near-zero latency. Bandwidth Control - allocate
bandwidth to business-critical applications and manage usage. Zscaler eliminates the need to reroute traffic to a central location or proliferate costly appliances in multiple locations, enabling businesses to instantly secure users on any device, anywhere in the world with no hardware or software required.

Packet Design— the leader in routing and traffic analysis solutions. The products offer unrivalled visibility into the logical operation of IP networks. Route Explorer and VPN Explorer are the industry’s leading route analytics solutions, deployed in the world’s largest OSPF, IS-IS, BGP, and MPLS VPN networks. Traffic Explorer and VPN Traffic Explorer provide network-wide, integrated routing and traffic monitoring. Powerful analysis and modeling on IP and IP/MPLS VPN networks with full historical replay are compelling offerings within the product suite.

Safend - Safend provides innovative end-point security solutions that are quick to deploy and easy to manage. The products provide in-depth visibility and control over the devices that users connect to their desktops and laptops. These solutions are managed through a streamlined user interface which enables end-point policies to be defined for any domain, group, computer, or user. Granular control is provided by device type, model or unique serial number. All local and wireless end-points plus removable storage devices can be secured by default, whether currently networked or not. Support for USB, Fastwire, PCMCIA, Wi-Fi, Bluetooth, IrDA, key disks and portable/removable devices.

SonicWALL is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high performance business network. The SonicWALL® E-Class NSA Series is the premier Unified Threat Management (UTM) solution for today’s enterprise network communications needs. Combining a multi-tiered proactive defense with a high-speed deep packet inspection and traffic classification engine, the E-Class NSA solution inspects real-time applications, files, and content-based traffic, irrespective of port and protocol without significantly impacting performance or limiting scalability. Globally deployable and manageable, E-Class NSA extends protection over both external and internal networks, delivering content inspection, application control and threat prevention throughout an enterprise network.

CyberOperations - Cyber ACL provides an enterprise level solution for management of complex network traffic policies by multiple IT personnel. Policies are stored on a centralized system with user access control and secure web access for management. Network device configurations can be synchronized automatically or manually to reflect changes in policy. Organizations with multiple locations and multiple network gateways are able to provide Automation, Compliance, Portability and Tracking. There are frequently updated links to useful online resources related to access-lists and network policy management. Tools to convert access-lists and firewall filters between
different formats such as from Cisco to Juniper or PIX to Cisco IOS, etc. are integrated within the product.

**CRYPTOCARD** The CRYPTOCard products offer Token Authentication / 2-Factor Authentication / One-Time Passwords (2FA/OTP) products which prevent unauthorized and undetectable remote access to privileged corporate data and private customer information. The technology positively identifies individuals to protect against compromised passwords and assists corporations to improve compliance with regulatory standards and privacy requirements. The solutions for two-factor authentication solutions have been deployed to thousands of companies around the world and are the most flexible solutions on the market for matching security policies, at a price all businesses can afford.

**Zyrion** – the leading provider of integrated Business Service Management (BSM) and IT Infrastructure Performance Monitoring Software. Zyrion’s innovative Business Service Container technology maps the virtual, cloud and physical IT infrastructure to supported business services. With everything from high-level CXT-friendly dashboards to intuitive performance correlation and drill-down to NetFlow capability, Traverse is an easy pick for replacing your “Big4” NMS platform.

**JAMF** – the Casper Suite offers features and functions that provide IT administrators with best practice strategies to meet the challenges of supporting Mac OS X and iOS in the enterprise, allowing your organization to build and sustain a stable, cost-effective, and user-friendly computing environment. The Casper Suite is a powerful framework around which your IT ecosystem can be unified and extended to manage both Mac OS X and iOS devices from a single console. Normalize your IT administration with the only client management solution developed exclusively for the Apple platform. the Casper Suite allows administrators to easily achieve the four major tenets of iOS mobile device management: Inventory, Configuration, Security Management, and App Distribution. Casper Suite allows administrators to manage the eight major tenets of Mac OS X client management: Inventory, Imaging, Patch Management, Software Distribution, Remote Control, Settings and Security Management, License Management, and Usage Management.

**NetiquetteIQ®** – Provides email content scanning for basic and advanced email composition. The product offers compelling capabilities to find, recommend and correct common mistakes in email. Areas which are addressed include basic features, addressing, appearance and errors. Netiquette adds significant power and distinction to virtually any outgoing original or email reply… from the simplest personal communication to the most critical business message.

Our president, Paul Babicki, has recently published books on Netiquette entitled *Netiquette IQ - A Comprehensive Guide to Improve, Enhance and Add Power to Your Email*” and “*You’re Hired! Supercharge Your Email Skills In 60 Minutes (And Get That Job!).*"
Additionally Netiquette presentations, classes and process design service are available.

There is also an email "IQ" test on our sister website: www.netiquetteiq.com
There is also currently a blog: http://netiquetteiq.blogspot.com
There is also a radio show: www.blogtalkradio.com/netiquetteiq

For further information on any of the products or services listed, contact Tabula Rosa Systems at 609 818-1802 or sales@tabularosa.net