Solution Flyer

Insert Market Space Designation String Here

Protection Starts with Security Management Solutions

Enterprises are under constant attack from internal and external threats. Repelling today's advanced threats requires an approach to security that emphasizes centralized log management, real-time event management and user-activity monitoring. Micro Focus® makes getting on the path to better security simple with our Security Management solutions. These solutions help you detect and defend against attacks before they cause irreparable damage to your business.

"Since implementing Sentinel, we have better insight into potential security issues. If an unauthorized person tries to access a server, I can see the entire event within seconds. It's mind blowing how well that works."

RANDY HARDIN

Lead Systems Engineer
University of Dayton IT

The Changing Landscape of Security

Information security has undergone a fundamental change over the past several years. The old security model emphasized protecting the internal network from external intruders. The goal was to build a barrier around the enterprise using a collection of firewalls, endpoint security software, vulnerability scanners and intrusion detection system (IDS) and intrusion prevention system (IPS) devices.

In today's world, with technology such as cloud computing moving users and applications outside the walls of the enterprise, organizations must now take a fundamentally new approach to security. They must focus on monitoring individuals and access to resources inside and outside the enterprise.

Security for Today's Threats

Security Management solutions from Micro Focus have proven efficient and effective for organizations that need to collect security information to protect against targeted security threats, decrease risk and ensure regulatory compliance. These solutions enable organizations to integrate security management directly into their business processes and decision making, providing an insight into enterprise risk, and supplying a significant competitive advantage. Security Management solutions are the central nervous system of security, tying together security information from all corners of an organization to provide a clear view of past events, current status and future risk. Trusted and proven in organizations such as the U.S. Navy Cyber Defense Operations Command, Telecom Argentina and Sony Italia, these solutions deliver innovative and powerful log management and include the most robust, scalable and mature security information and event management (SIEM) capabilities available today.

Security management solutions from Micro Focus deliver on the immediate need for centralized log management capabilities and the long-term goal of effective, real-time security monitoring and remediation.

Industry-Leading User Activity Monitoring

One of the shortcomings of traditional security techniques is the inability to cope with the rise of insiders causing data breaches. Disgruntled former employees with backdoor access, current employees with malicious intent and unintended user access miscues are all insider challenges that enterprises must protect their data against. Security Management solutions from Micro Focus also achieve industry-leading user activity monitoring, which enriches security events with additional information in real time, including such information as user identities and asset information. Enriched data provides a clear picture of what activities are actually taking place, improving the likelihood that a security anomaly will be detected. It reduces the time needed to detect a breach

and enables organizations to monitor user activity. The result is fewer and less costly data breaches and a more productive security workforce that spends more time on real problems and tracks down and fixes those problems faster.

Address the Rising Tide of Regulation

In addition to all the challenges associated with securing data, organizations are faced with the added burden of proving that information is secure and in compliance with government regulations and industry mandates. Even for the most advanced security programs, efficiently and cost-effectively proving compliance is still a challenge. Security Management solutions provide many of the controls, tools and reports that enterprises need to comply with the Payment Card Industry Data Security Standard (PCIDSS), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), North American Electrical Reliability Council Critical Infrastructure Protections (NERC CIP), Basel II Accord and many other regulations. In addition, these solutions are flexible enough to adapt to new regulations as they are added.

Solution Capabilities

Security Management solutions comprise two products: NetIQ® Sentinel™ Enterprise and NetIQ Sentinel Log Manager, which deliver all the capabilities you expect in a powerful, enterprise-class security information and event management (SIEM) and log management.

Security management solutions from Micro Focus deliver on the immediate need for centralized log management capabilities and the long-term goal of effective, real-time security monitoring and remediation.

Log Management

Security Management from Micro Focus provides the best solution for organizations that want to reduce the cost and complexity of collecting, searching, reporting and retaining event log data. It solves the dual challenges of security and compliance. It provides fast return on investment (ROI) with a software appliance deployment option, automatic detection and configuration of syslog sources, and simplified reporting using built-in reports. It makes extracting value from log data easy with simple, yet powerful, search capabilities that work seamlessly over local and external storage. This solution also allows organizations to leverage their investment in log management and take advantage of real-time correlation and automated remediation of security events.

Real-time Security and User-Activity Monitoring

Sentinel Enterprise is a high-performance SIEM tool that allows organizations to meet today's security challenges head-on. The advanced correlation engine in Sentinel Enterprise monitors an organization's entire infrastructure and detects security anomalies that would otherwise go unnoticed. Powerful and intuitive graphical displays and security intelligence dashboards provide real-time insight into the current state of security within the enterprise. Sentinel Enterprise also includes a flexible workflow engine for automated or manual remediation and ships with the controls you need for a wide variety of regulations.

Benefits of Security Management

Log Management for Improved Security, Forensic Analysis and Regulatory Compliance

Enterprises are deluged with information from their ever expanding IT infrastructure, and managing this data is a serious challenge for even the most talented administrator. Security Management solutions from Micro Focus deliver enterprise-class log management, which automates the process of collecting, organizing, storing and reporting on log data across the entire organization. Not only does this reduce the cost of complying with various information security regulations such as PCI-DSS, SOX and NERC CIP, but it also allows organizations to detect weak points in the security infrastructure and speeds up the process of forensic analysis if a security breach does happen.

Sentinel Log Manager is built to perform all of these tasks and more. Searching through data to conduct a forensic analysis is made easy with a powerful search engine, advanced filtering controls and the ability to seamlessly search across local or networked storage. Creating dynamic reports takes just a single click. Sentinel Log Manager supports data retention policies so data is not stored longer than it's needed, and it compresses data 10:1 automatically, maximizing storage efficiency without sacrificing usability.

Enterprise Protection Against Security Threats

Data breaches are extremely costly, and recent trends indicate the number of breaches, as well as the cost per breach, are increasing. The average cost of a breach is US$6.6million,* which includes the cost to notify individuals, legal expenses and fines. Breaches are not only costly, but the damage to a company's brand can be long lasting and extremely negative. The advanced correlation engine in Sentinel can spot weak points before hackers do or even detect a breach as it's happening, which makes accessing an organization's sensitive data much harder for insiders and outsiders.

** Ponemon Institute: 2008 Annual Study, The Cost of a Data Breach*

When you deploy Micro Focus solutions, you have access to Micro Focus Services, world-class support, training and professional services offerings to help you make the most of your investment.

Contact us at:
www.microfocus.com

Like what you read? Share it.

Staged Approach Maximizes Investment

Now organizations can take a tactical, focused approach to security with Security Management solutions from Micro Focus. Enterprises can start by deploying Sentinel Log Manager without overinvesting in hardware capacity or software before they are ready to use it. Taking this right-size approach to security allows an organization to maximize the dollars it spends on security and extracts the most value out of the software it deploys. Other vendors require customers to run both their log management and real-time correlation engines on the same hardware. In practice, this means organizations must buy additional hardware that will sit idle until the organization is ready to start using real-time correlation. The software for these other solutions is also more costly overall because all of the capabilities are included in the initial purchase, even though the organization will need months to start using the more advanced features.

Achieve Rapid ROI with Micro Focus Services

When you deploy Micro Focus solutions, you have access to Micro Focus Services, our world-class support, training and professional services offerings to help you make the most of your investment. For example, our Fast Track professional services engagements can help you deploy tailored solutions quickly and efficiently at a fixed cost. Our flexible and convenient training options ensure that your people can get the expertise they need, which leads to faster ROI and reduced downtime and support costs.

Partner Opportunities

Micro Focus continues to build strong partnerships with System Integrators and Global Solution Providers. These providers have the expertise not just to deploy a Micro Focus solution set but also to advise organizations on security best practices and technologies.

Defeat Tomorrow's Threats with Security Management Solutions

Whether you have a short-term tactical need for log management, or you need a complete real-time SIEM solution, Security Management solutions from Micro Focus have you covered. We have the best products with the best capabilities to ensure you have a solution for centralized management of security data. We provide the clarity your enterprise needs not only to stop today's threats to your business, but also to defend against the attacks of tomorrow.

To learn more about Sentinel Log Manager, go here.

MICRO FOCUS