MICRO FOCUS

Data Sheet
Security

ArcSight Reputation Security Monitor

Detect and Analyze Threats Using Reputation Intelligence

Product Highlights

Micro Focus® ArcSight Reputation Security Monitor (RepSM) solution brings reputation-based intelligence to security information and event management to deliver even greater protection and to further reduce business risk. By correlating security events with vetted security intelligence, threats can be detected earlier. And, by detecting and blocking communication between malicious hosts and infected infrastructure, even the most sophisticated attacks can be detected.

Key Features

Insight Using Vetted, Reputation-Based Threat Intelligence

The volume of security intelligence data has exploded in recent years. Security information and event management systems can collect and correlate massive volumes of data. But without the proper tools, it is challenging to find what is most important, most relevant to the business, and most real; and timeliness is key to consider the most current conditions. Tools that can go a step further to actually detect the threat are best able to help manage business risk. The RepSM solution actively manages "reputation based" security policies to detect and prevent communication with known bad actors representing vetted security threats.

The most important consideration for any reputation-based service is the reliability and accuracy of the information that is provided. DVLabs, the security intelligence and research organization continues to lead the way in vulnerability discovery. The company disclosed 274 verified vulnerabilities, more than the eight closest competitors combined, according to a Frost & Sullivan report.[1]

In addition to DVLabs, where researchers worldwide find vulnerabilities and threats, data is collected and consolidated from real-world attack sensors, feedback from customers of TippingPoint Next Generation Intrusion Prevention System (NGIPS) worldwide installations, and leading open-source community resources. Your own criteria can be added to this vetted reputation data to provide a comprehensive view of suspicious sites and actors.

For each malicious host, the insight specifically includes:

- Reputation scores—between 1 and 100, with a score of 100 identifying IP addresses or hostnames with the most malicious history

1 *Source: "Analysis of the Global Public Vulnerability Research Market in C Y 2011," Frost & Sullivan, April 2012.*

What's new in version 1.5

- Detect additional threats including peer-to-peer network use and potential spear phishing
- Accumulate and analyze suspicious connections, including internal, over time further surfacing attack reconnaissance and abnormal activity levels
- Integration with TippingPoint IPS to automatically block attacks and exfiltration
- Integration with ThreatDetector to detect and verify zero-day attack and APT spread patterns

- Host reputation types—that identify whether the identified host or IP address is a botnet, malware, spam, phishing, and more
- Geolocation—from where the specific threat is originating

Together these insights can help further prioritize vulnerabilities and threats within the context of business risk. By correlating reputation with security information and events, RepSM can help focus on those threats with most risk and can identify and prevent exfiltration of intellectual property to sites known to have bad reputations.

Packaged Expertise

To bring immediate value, several use cases are included that correlate common events with insight on the reputation of security threats. RepSM includes scenarios to aid in detection and prevention at every stage of security.

- Before a breach occurs, RepSM can detect dangerous browsing of ill-reputed sites, potentially preventing a compromise.
- After a breach occurs, RepSM can identify infected assets or infrastructure trying to communicate with ill-reputed command and control centers, potentially before intellectual property is leaked out of the company.
- Given that most breach victims are notified by a third party, RepSM can proactively check your enterprise's customer-facing assets and websites to verify none have been corrupted and placed on the threat list, potentially blocking access by your customers and business partners.

Established Capabilities

RepSM enhances the market-leading security information and event management solution, ArcSight Enterprise Security Manager (ESM). In fact, ArcSight ESM has been a leader in Gartner's "Magic Quadrant for Security Information and Event Management," this year and every year the product has been reviewed.[2] This foundational element provides visibility across information assets and users with comprehensive logging and efficient monitoring along with a powerful correlation to assess relative business impact. RepSM integrates the power of ArcSight ESM with timely, vetted reputation data from DVLabs to provide even greater insight to detect and prevent security threats.

Key Benefits

By correlating vetted reputation intelligence with security information and events, RepSM can:

- Detect threats early using frequently scheduled updates of reputation data, vetted from a cadre of experts globally
- Prioritize remediation efforts more effectively using reliable threat intelligence
- Factor in your own unique threat experiences
- Prevent exfiltration of intellectual property from infected internal machines to sites with bad reputations
- Monitor and protect the reputation of your own enterprise so that company websites, assets, and those of partners are not found in the bad reputation list

Why Micro Focus?

- Quality of the reputation data—research provided by DVLabs, one of the industry's most accurate and reliable security research firms that continues to lead the market in vulnerability identification.[3]
  - The comprehensive reputation database provides in-depth reputation context with reputation score, threat type, and origin of threat for greatest insight and prioritization.
- Comprehensive capability of one of the market-leading security intelligent system to correlate threat data to security information and events
  - Real-time event correlation with frequently updated reputation data
  - ArcSight ESM dashboards, drill-down, and integration commands to investigate and mitigate attacks
- Micro Focus Security Services to assist with security and risk strategy implementation and ongoing management

Supported Platforms

- ArcSight ESM 5.2 and higher
- ArcSight Express 4.0 and higher

About Micro Focus Enterprise Security

Micro Focus is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in its hybrid environment and defend against advanced threats. Based on market-leading products from ArcSight, Fortify, and Micro Focus Data Security, the Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

2 *Source: "Critical Capabilities and Magic Quadrant for Security Information and Event Management," Gartner, May 2012.* hpenterprisesecurity.com/register/2012-gartner-critical-capabilities-and-magicquadrant-for-security-informat

3 *Source: "Analysis of the Global Public Vulnerability Research Market in C Y 2011," Frost & Sullivan, April 2012.*

Micro Focus Services

Micro Focus Services takes a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results, and demonstrate ROI. Our proven, use case-driven solutions combine market-leading technology with sustainable business and technical processes executed by trained and organized people.

Learn More At

www.microfocus.com/securitysolutions

Contact us at:
www.microfocus.com