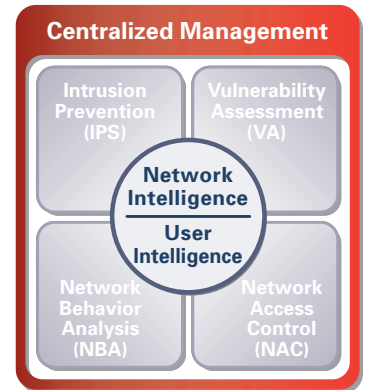


Sourcefire RUA™ (Real-Time User Awareness)

USER INTELLIGENCE FOR ENTERPRISE THREAT MANAGEMENT (ETM)

By integrating Intrusion Prevention System (IPS), Network Behavior Analysis (NBA), Network Access Control (NAC), and Vulnerability Assessment with actionable intelligence – all under one management console – ETM is drawing the praises of risk, compliance, and security professionals who are finding it to be a far more effective and efficient approach than their current security solution. Within Sourcefire's ETM approach, the user intelligence of Sourcefire RUA™ is the perfect complement to the network intelligence found in the solution.



MATCH USERS ID TO IP ADDRESSES IMMEDIATELY

Who wouldn't love to be able to list – in seconds – the actual identities of those people who continually download those enormous files or run unauthorized applications? With potentially tens of thousands of IP addresses in an organization, right now tracking a single user of an IP address can be like finding a needle in a haystack. Sure, you can do it but you've probably lost a half hour in the process. With RUA's user tracking, you can identify actual users immediately and rapidly respond to a potential network threat or attack – speed resolution to network events, more tightly control the environment, and improve your network security decision-making. RUA uses LDAP and Active Directory domains as its sources of data to build user intelligence.

Much more than a stand-alone user identity product, RUA enhances the Sourcefire 3D™ System with powerful user identification capabilities to directly correlate individual user logins with specific network behavior, traffic, and events. In addition to providing network administrators with actionable intelligence that identifies the source of policy breaches, attacks, or network vulnerabilities, RUA also enables user-based policy and response rules for greater control.

GAIN GREATER VISIBILITY WITH INTEGRATED USER AWARENESS

As a complement to your existing Sourcefire solutions, RUA gives you integrated user awareness never before available, including:

- ▶ **24x7 passive identity discovery with comprehensive user identity information capture including e-mail and IP addresses**
- ▶ **User connection with all the IP addresses it's currently using and a time stamp to support long-time horizon analysis and forensics**
- ▶ **Automated correlation of identity with security events – threat, NBA, NAC, or policy events**

When added to the Sourcefire 3D System, RUA provides real-time user identities of IP addresses in Sourcefire IPST™ and Sourcefire RNA™ event data, hosted system data, and reports. User identities can also be included in table views and workflows as well as flow data information and graphs. Now Sourcefire customers can correlate user intelligence with network intelligence for a more informed understanding of how the network is being used.

Sourcefire RUA at a glance:

- Matches user IDs to IP addresses
- Complements and enhances the Sourcefire 3D System
- Correlates threat, endpoint, and network intelligence with user identity
- Speeds resolution of issues
- Eliminates manual efforts to track users
- Has no network impact
- Uses the same data collection sensors as Sourcefire IPST™ and Sourcefire RNA™
- Identifies employees hacking into internal systems
- Identifies employees misusing network bandwidth
- Provides visibility on users running non-standard or unauthorized applications
- Allows an administrator to set up remediation policies for specific user IDs



Table View of Users

▼ Query Constraints (Edit Query Save Query) Disabled Columns

Intrusion Events | RNA Events | Hosts | Host Attributes | Services | Client Apps | Flows | Vulnerabilities | Compliance Events | White List Events | **Users** | Remediations

User X	Current IP X	First Name X	Last Name X	E-Mail X	Department X	Phone X
⌵ Abe Lincoln (abel)		Abe	Lincoln	abe.lincoln@presidents.gov	historic figures	
⌵ Benjamin Franklin (benf)	10.4.15.11	Benjamin	Franklin		historic figures	
⌵ Christopher Columbus (chrisc)	10.4.15.25	Christopher	Colombus		historic figures	(410) 803-1492
⌵ Dorothy Dandridge (dbld)	10.4.15.29	Dorothy	Dandridge		historic figures	
⌵ Edgar Poe (edgarp)	10.4.15.27	Edgar	Poe	ed.poe@poets.tv	historic figures	
⌵ Francis Xavier (francisx)	10.4.15.28	Francis	Xavier		historic figures	
⌵ Genghis Khan (qenghisk)	10.4.15.12	Genghis	Khan		historic figures	

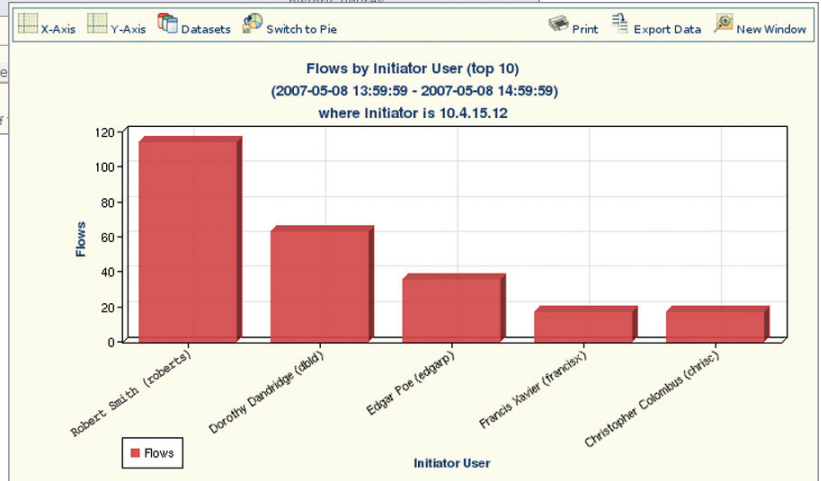
Delete De

1
(Showing 1 - 7 of

Security administrators can view user identities within event data without having to perform an external lookup.

GAIN GREATER CONTROL AND COMPLIANCE

RUA significantly improves audit controls and assures regulatory compliance by linking events directly to individual users. For greater control, you can set policies and rules once based on user IDs and apply these across your Sourcefire Intrusion Prevention, NBA, NAC, and Vulnerability Assessment ETM components.



WORK SMARTER WITH SOURCEFIRE RUA

Whether your organization is using all or part of the Sourcefire 3D System, adding the powerful user intelligence capabilities of RUA speeds incident containment, enhances control, eliminates manual efforts and associated costs, and improves decision-making.

For more information about the Sourcefire 3D System, including RUA, contact your Sourcefire sales representative or call 1.800.501.6008.

www.sourcefire.com

SOURCEFIRE®, SNORT®, the Sourcefire logo, the Snort and Pig logo, SECURITY FOR THE REAL WORLD™, SOURCEFIRE 3D™, SOURCEFIRE DEFENSE CENTER™, SOURCEFIRE IPS™, SOURCEFIRE MASTER DEFENSE CENTER™, ESTREAMER™, SOURCEFIRE RNA™, SOURCEFIRE RUA™, DAEMONLOGGER™, OFFICECAT™, NETWORK USAGE CONTROL™ (NUC) and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. Nessus is a trademark of Tenable Network Security, Inc.