



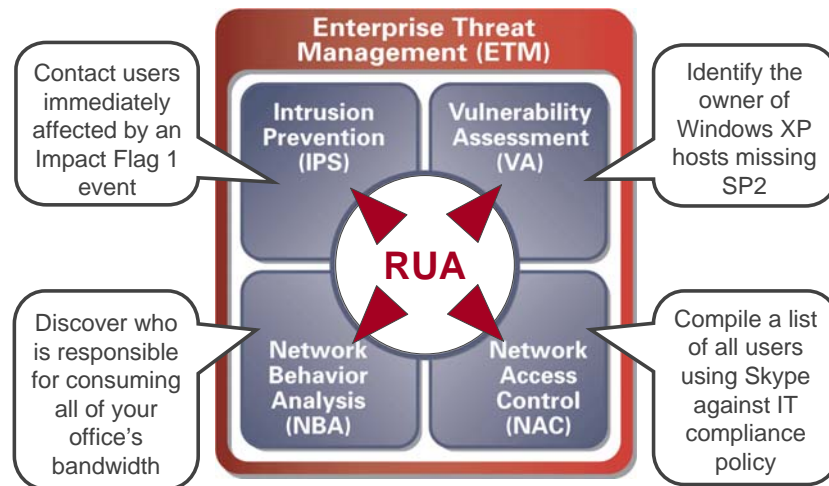
Frequently Asked Questions

Sourcefire RUA™

Overview

What is Sourcefire RUA?

Sourcefire RUA™ (Real-time User Awareness) is the newest addition to the Sourcefire 3D™ System product family and benefits all four Sourcefire Enterprise Threat Management (ETM) solutions, including IPS, NBA, NAC and VA. (See diagram below.) Sourcefire RUA streamlines the process of associating a host IP address related to security and compliance events with Active Directory and LDAP usernames. Other user attributes, including first name, last name, department, phone number and email address, are also available within Defense Center, right at your fingertips.



Sourcefire RUA benefits all Sourcefire ETM solutions

How can Sourcefire RUA benefit Sourcefire customers?

Sourcefire RUA can tell you the “who” behind the “what”. In other words, RUA can tell you:

- **Who** owns the host targeted by a given Impact Flag 1 event
- **Who** just initiated an internal attack
- **Who** just launched an internal port scan
- **Who** just attempted to access the payroll server
- **Who** is consuming the most bandwidth in our office
- **Who** is missing Service Pack 2 for Windows XP
- **Who** is using Skype in violation of company IT policy

How did Sourcefire customers determine user identity prior to RUA?

Prior to RUA, customers either didn't associate users with events, or they typically sifted through Active Directory or LDAP log files, or in some instances attempted to correlate usernames with IP addresses within the context of a SIEM. By implementing RUA, the process of resolving user identity to a host IP address associated with security and compliance events is completely streamlined, saving customers both time and money.



Frequently Asked Questions

Sourcefire RUA™



Does the value that RUA brings differ for servers rather than user desktops and laptops?

Yes. RUA provides insight into the “who” behind the “what”. Servers are generally under IT control and often use static IP addresses. RUA enables customers to resolve intrusion and compliance events more quickly by determining the owner of a given host. When it comes to servers, the owner of the host is typically IT. But when it comes to desktops, laptops and other user devices, DHCP is commonly used, making it far more difficult to ascertain the owner of any end-user device. Thus, RUA is far more valuable for end-user hosts than servers managed by IT, although RUA can tell IT which users were connected to a given server (for a rolling 24-hour period) at the point of an attack.

How It Works

How does RUA work?

The options for implementing RUA differ slightly based on the user directory technology an organization employs. But regardless of whether the organization uses Active Directory (AD) or LDAP, the first part of the solution is effectively the same. One of the organization’s directory servers is designated as “primary” and is used as the source of information to generate a user database within a designated Sourcefire Defense Center appliance. (See step “A” in RUA diagram.) New user accounts and revised user account data are replicated to Defense Center via a synchronization process that occurs every 60 minutes. The purpose of the user database is to establish and maintain a record of known usernames and a few additional pieces of helpful information, including the user’s actual name, email address, phone number, and department.

For Active Directory shops, the second part of the solution entails running Sourcefire RUA Active Directory Agents on each of the organization’s AD servers. (See step “B” in RUA diagram.) These agents monitor users as they log into the network or when they are authenticated against the AD credential store for any other reason (e.g., to obtain access to a given service or application that relies on AD for centralized authentication). As a user logs on, the RUA Agent captures the username being submitted and the corresponding IP address associated with that user’s host. Then, the username-IP address pair is forwarded in near-real-time to Defense Center for incorporation within the user database. Then when a security or a compliance event occurs, the Sourcefire administrator has the user’s identity right at his/her fingertips.

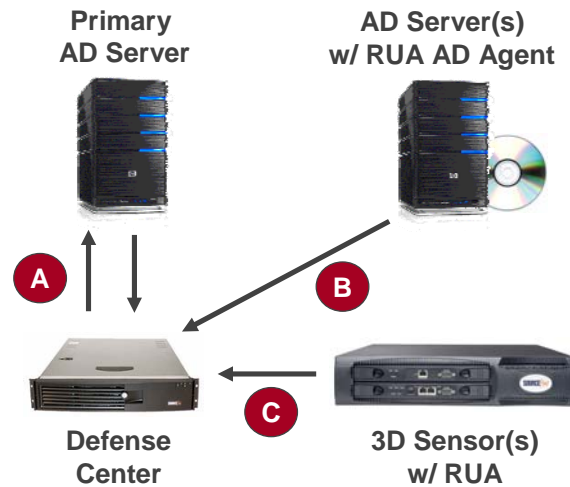
Alternatively, administrators can run RUA software on Sourcefire 3D Sensors that are deployed in the network. (See step “C” in RUA diagram.) This configuration enables the 3D Sensors to passively detect (Kerberos) logon activity in the traffic they observe and to forward username-IP address pairs for incorporation in the Defense Center User Database. This configuration is intended primarily for LDAP shops not running Active Directory, but is also an option for Active Directory shops that have an objection to running agents on their AD servers. LDAP / Active Directory usernames and corresponding IP addresses are passively detected by RUA running on 3D Sensors. This user intelligence is forwarded to Defense Center in near-real-time for storage and analysis.



Frequently Asked Questions

Sourcefire RUA™

SOURCEfire®
Security for the real world.



How Sourcefire RUA Works

What are the advantages and disadvantages of using the RUA Active Directory Agent?

There are three advantages that the RUA Active Directory Agent brings to AD customers:

- If installed on all AD servers, RUA AD Agents provide comprehensive coverage across an entire organization, not having to rely on 3D Sensors with RUA to cover all network segments.
- By using RUA AD Agents instead of 3D Sensors, the hardware resources of the 3D Sensors can be dedicated to running Sourcefire IPS™ and Sourcefire RNA™ applications.
- RUA AD Agents are more cost-effective, as no additional expense is incurred by purchasing additional 3D Sensors to support RUA.

The only “disadvantage” of the RUA AD Agent is one of customer misperception. Customers may perceive RUA AD Agents as being a “risk” to AD Servers by either consuming too many resources and/or causing AD servers to crash. Neither assertion should be a concern, backed by extensive Sourcefire internal testing and customer beta testing.

I’m concerned about installing agents on my Active Directory servers. How much server resources will the RUA Active Directory Agents consume?

The RUA Active Directory Agent is less than 1MB in file size and runs as a background Microsoft .NET Framework service on Active Directory servers. Typical CPU utilization consumed by the RUA Active Directory Agent is less than 5%, depending on the processing power of the server and the frequency and quantity of on-going Active Directory authentications. Typical memory usage is approximately 15MB of RAM.

Are there any RUA limitations in an Active Directory environment?

No, providing that the Active Directory customer has not removed Kerberos as the default authentication mechanism. Kerberos is required for passively detecting usernames and associated IP addresses in an Active Directory (and LDAP) environment.



Frequently Asked Questions

Sourcefire RUA™



Does Sourcefire offer an RUA Agent for LDAP servers?

No. Sourcefire does not offer an RUA Agent for LDAP servers at this time.

Does RUA work with all LDAP systems?

RUA is designed to work with LDAP systems that incorporate Kerberos authentication. Secure LDAP is also supported.

Are there other methods for detecting usernames besides Active Directory and LDAP?

Yes. RUA installed on 3D Sensors can passively detect username / IP pairs through POP, IMAP and SMTP email access and AIM instant messaging. This enables RUA customers to detect username / IP pairs for “guests” on the network or users without usernames in the organization’s user directory (i.e., university students).

Does RUA work with Novell eDirectory?

RUA does not support Novell eDirectory at this time. Novell eDirectory customers can use RUA to detect usernames associated with e-mail authentication for POP, IMAP and SMTP e-mail platforms. However, additional user attributes, such as first name, last name and telephone number, cannot be imported into the RUA User Database (stored on Sourcefire Defense Center™) via a Novell eDirectory server.

Can RUA pair usernames with host IP addresses if SSL encryption is used during the authentication process?

No, Sourcefire RUA cannot passively detect AD or LDAP authentications on the wire when SSL is used. However, for AD customers, the RUA AD Agent can detect AD authentication requests on the AD Servers regardless of whether SSL was used on the wire.

Can RUA be used on a stand-alone 3D Sensor without the use of a Defense Center appliance?

No. Defense Center is required to host the RUA user database and to correlate username / IP pairs with security and compliance events.

Does RUA detect both logons and logoffs?

No. RUA detects logons only.

Does RUA support double-byte characters, such as Japanese and Chinese?

No. RUA does not detect usernames with double-byte characters at this time.

Pricing & Availability

How is RUA licensed?

RUA is licensed on a per-username basis. This is different than RNA, for example, which is licensed on a per-host basis.



Frequently Asked Questions

Sourcefire RUA™



Is RNA a prerequisite for RUA?

No. However, RNA extends the value of RUA considerably, if present, by making RUA useful not only for the IPS solution, but also NBA, NAC and VA solutions as well.

At what point are RUA licenses consumed?

RUA licenses are consumed the first time a given username is processed by Defense Center. This could occur at the time an AD or LDAP user database is replicated to Defense Center, or it could occur when a username is detected by RUA, paired with an IP address, and fed into Defense Center.

What happens when you run out of RUA licenses?

Once all RUA licenses have been used, no additional usernames can be fed into Defense Center. Additional RUA licenses will be required to store additional usernames and associated user attributes.

How much does Sourcefire RUA cost?

Please contact a member of your Sourcefire Account Team for RUA pricing information.

Are customers with active 3D System maintenance agreements eligible to receive RUA at no additional charge?

No. Customers will not receive RUA licenses as part of an existing maintenance agreement. RUA is a new Sourcefire product and is licensed separately.

When will Sourcefire RUA be available?

Sourcefire RUA software is available now via the Sourcefire Customer Support web site. RUA will come pre-installed on Sourcefire appliances beginning in mid-October, with the exception of the new 10Gbps 3D9800 Sensor, which is anticipated to support RUA in the first half of 2008.

For More Information

The following materials are available now on the Sourcefire Customer Support web site. They provide additional information about what's new in the Sourcefire 3D System 4.7 release, including Sourcefire RUA:

- What's New in Sourcefire 3D System 4.7 Brochure
- What's New in Sourcefire 3D System 4.7 Webinar
- Sourcefire 3D System 4.7 User Guide
- Sourcefire 3D System 4.7 Installation Guide

To learn more about Sourcefire RUA, or to get answers to related technical questions, please select from the following options:

- Visit the Sourcefire Support Site at <https://support.sourcefire.com>
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 1-800-917-4134 or +1-410-423-1901



Frequently Asked Questions

Sourcefire RUA™



For information on Sourcefire's training and certification programs, please select from the following options:

- Visit the Sourcefire Education Site at <http://www.sourcefire.com/services/education>
- E-mail Sourcefire Education Services at training@sourcefire.com
- Call Sourcefire Education Services at 1-866-505-9113 or +1-734-743-6550

Copyright © 2007, Sourcefire, Inc. All rights reserved. Sourcefire®, Snort®, Sourcefire 3D™, Sourcefire IPS™, Sourcefire RNA™, Sourcefire RUA™, and Sourcefire Defense Center™ are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.