Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Improving Security Management with Real-Time Queries

Copyright SANS Institute
Author Retains Full Rights
A SANS Analyst Product Review

Written by Dave Shackleford

March 2014

Sponsored by
McAfee
One of the biggest challenges facing organizations today is the lack of knowledge about system state at any given time. SANS has long espoused a strategy of continuous monitoring for all systems (or at least critical ones), but most have struggled to actually implement this. As threats become more stealthy and persistent, understanding organizational security posture at all times and reacting quickly to any potential attacks become paramount.

McAfee's Real Time products address such next-generation threats and consist of two products:

- **McAfee Real Time for McAfee ePolicy Orchestrator.** This ties into McAfee's flagship security management tool, ePolicy Orchestrator (ePO), facilitating access to ePO's policy-based deployment, automated workflows, permissions and security models, as well as other McAfee tools.

- **McAfee Real Time Command.** This provides agent-based monitoring and control of systems, but with a twist: The dashboard has a flexible query syntax that facilitates the use of natural English language to a greater degree than many similar products and provides results that can be correlated and drilled into for further analysis.

We recently had the opportunity to review McAfee Real Time Command and explore several use cases that it fits into, with a focus on features and ease of use. We examined its security-related features and found the product to be surprisingly intuitive. Security and operations teams will surely find a wealth of useful information at their fingertips when using Real Time Command.
Overview

We began the review with a brief look at the basic functions of Real Time Command. The review environment consisted of approximately 500 virtual machines set up ahead of time by McAfee, with a dashboard already installed and ready to go. The main dashboard is simple to understand, with flexible configuration, and is shown in Figure 1.

Administrators can create new dashboard elements quickly, and the drag-and-drop configuration interface is intuitive. On the Actions tab at the top of the dashboard, users can configure and review a number of scheduled actions on monitored assets, as shown in Figure 2.
Users can create Action Groups—collections of actions—with as many actions included as are appropriate. This task and script aggregation reduces time to response and guides investigators to logical workflows. Having all desired actions take place automatically, on a schedule, can potentially detect issues much faster and save time during a real incident, which may, in turn, prevent the problem from worsening.

The next tab in the main console, the Authoring tab, is where most of Real Time Command’s interesting features are configured, using its various tabs: Dashboards, Saved Questions, Sensors and Packages. The Dashboards tab enables users to change the dashboard layout. The drag-and-drop functionality makes it simple to create or modify available queries and the groups into which queries are organized on the main screen. We modified several dashboard elements and created a new one as well. Figure 3 illustrates this feature.
The left column shows the data we thought would be most helpful in gauging an individual system’s security posture. Information about the McAfee agent, critical applications and services, and the operating system are all in one place, making this a very valuable dashboard for operations teams.

The Saved Questions tab allows the archiving of frequently used queries that Real Time Command will offer during relevant searches (as shown later under “Rapid Incident Response”). Figure 4 illustrates this tab.

Editing questions was simple. Clicking the pencil icon next to a question enabled us to see what options were set and made it possible to “drill down” into a query, to levels where much more granular information was available. The editing pane is shown in Figure 5.
The Sensors tab is where an administrator can choose the types of monitoring that Real Time Command will perform and the data that will be returned to the console. Within the tab, users can preconfigure many sensors, as shown in Figure 6.

Sensors can assess many configuration aspects of systems on the fly, thanks to Real Time Command’s live polling of agents, which examines status in areas ranging from network details to patches and applications, as well as processes and users (and many more areas). Figure 7 shows a simple test sensor we created during our review that returned the results of several simple Linux commands.
Numerous query types are available for many operating systems, as shown in Figure 8.

Finally, Figure 9 shows an example of an existing query that scans Windows systems for Java information (certainly a relevant query for security professionals).
The last tab under Authoring is the Packages tab, where users can bundle a command or set of commands together for use later to take specific actions on systems. In Figure 10, we show the results from querying all the existing packages that perform Java-related actions.

![Figure 10. The Packages Tab](image)

The final main tab, the Administration tab, enabled us to configure additional options, such as the user accounts for access and logging.
The first major category of functionality we reviewed within Real Time Command was the product’s applicability to IT operations teams in the form of systems management. In some organizations, the same team is responsible for both platform administration and security functions, while better-staffed outfits will separate those duties. In either case, getting rapid and up-to-date system information related to patches and configuration is critical. Even a single system that is missing patches or lacks sound configuration can easily lead to a compromise scenario or data exposure, so Real Time Command takes advantage of McAfee's long experience in agent-based monitoring to provide the latest endpoint status.

The Real Time Command dashboard allows administrators to easily see if there are known systems with the McAfee Agent, shown in Figure 11; issues that are easily fixed are to the left, while the right-hand pane shows errors that may require deeper intervention.

Another simple check provides the version of the McAfee Agent installed to ensure the endpoint is up-to-date, as shown in Figure 12.

Other important information, such as the level of logging configured at the endpoint, is included on the Administration tab.
Some clients can take remediation actions based on specific triggers and administrator actions, which allows for more rapid and automated systems control and administration. This may not be suitable in the case of some sensitive systems, so these actions should be locked or disabled to prevent any changes without explicit testing and approval. This is another simple check that administrators can perform within the Real Time Command dashboard, as shown in Figure 13; locked systems appear to the right.

![Figure 13. Client Action Locks](image)

A final dashboard view that was useful showed us systems that were unable to execute VBScript, which would prevent some packages and sensors from functioning properly (see Figure 14).

![Figure 14. Machines Unable to Execute VBScript](image)

To start exploring the types of queries that operations teams will find compelling, we first investigated the dashboard’s Computer Health category. Here, admins can look at any attribute of system state, such as disk capacity, memory consumption or CPU performance. An example of a dashboard item for systems with a slow CPU performance is shown in Figure 15.

![Figure 15. Computer Health—Slow CPU](image)
Within any of the categories of dashboard, administrators can drill down into more granular data and results to explore a vast range of system attributes. Organizations can use the numerous prebuilt queries and the ability to create and save their own queries to explore their systems. This capability is one of the more powerful features of the product. Some of the queries available in our test environment appear in Figure 16.

![Figure 16. Drill-Down Queries](image-url)
We explored several of these, finding queries like “Local User Information” and “Last Logged In User” to be useful for “spot” audits and the “Machines Requiring a Reboot” query valuable for planning change control actions. As an example of a more granular result, Figure 17 displays detailed CPU information for system “IP-0A3C2364.”

![Figure 17. CPU Details](image1)

But we could dig even further. A very valuable drill-down query was “Highest Memory Usage by Process,” shown in Figure 18.

![Figure 18. Highest Memory Usage by Process](image2)

Investigating which processes are currently hogging memory can aid in troubleshooting, as well as incident investigation for in-memory compromise and malware potentially. Many sophisticated threats are memory-resident (instead of dropping code and files onto systems), and having simple remote visibility into processes using excessive memory can help ferret out potentially compromised services.
Administrators can leverage Real Time Command to quickly get an accurate depiction of patch status across systems in the environment. If an administrator needs to get a fast snapshot of the number of systems missing five or more patches, he or she can easily access such information in the dashboard view “Patch Management: Windows OS Patch Overview,” shown in Figure 19.

Admins can then drill down into this data to see which individual systems meet this criterion, as shown in Figure 20.

Given the proliferation of attacks against client-side software, such as Adobe Reader and Java, operations teams need general visibility into software installed on endpoints, as well. A dashboard for application information (including versions) on endpoints is shown in Figure 21.

Real Time Command offers a detailed window into system conditions, patches and overall inventory of platforms and applications across the environment. Specialized servers and services, such as Microsoft SQL Server, can also be easily monitored.
Given the deep level of visibility Real Time Command provides into systems across the IT infrastructure, it makes sense that security analysts and incident responders will find it a powerful window into suspicious behavior on systems whenever needed. In SANS Institute classes on incident response, one of the core topics we stress with our students is working with operations teams ahead of time to ensure access to systems during emergency situations such as security incidents. This has always proven to be challenging, as administrators do not want to share access credentials to production systems unless absolutely necessary, which is understandable. With Real Time Command, security teams can access enough data about systems to enable a more accurate determination of whether deeper access is warranted, which helps everyone involved make faster decisions.

To evaluate how Real Time Command could aid in incident response, we took a different approach to searching for data and explored one of the most powerful features of the product’s console. The Ask a Question query field allows any text input and tries to match up potential results based on what you’re looking for. Following on our memory utilization example from the previous section, we performed a simple query for “high memory” as shown in Figure 22.

![Figure 22. Real Time Command's Query Field](image-url)
The results, a list of predefined and stored queries, led us to run the query “High Memory Processes from all machines” to see what were the most memory-consuming processes across the environment. That returned a list similar to the one shown previously in Figure 18, but it also featured a Count column showing the number of systems on which each process was found (these results can be drilled into for further analysis). We then chose to perform queries looking for a unique keyword, in our case, IP-0A200BD9, the name of a Windows computer in our testbed that was thought to be behaving suspiciously. The search returned the results shown in Figure 23.

![Figure 23. Searching For a Unique String Value](image1)

We then clicked the link for Get IP Connections from all machines to place the query string in the Ask a Question field and then replaced the words “all machines” with “IP-0A200BD9” (the name of the system we wanted to investigate). This query is shown in Figure 24.

![Figure 24. Intelligent Query](image2)
From our limited input, Real Time Command was able to properly form the query we wished to create, and we clicked the link to see IP connections originating from this machine, as shown in Figure 25.

In this result set, we could see the source and destination address and port, processes and applications in use, and the current connection state. Correlating this information with the list of applications and processes using a high percentage of memory may indicate malware or other compromise symptoms that security staff should investigate further. To verify the memory consumption for processes on this system, a similar query was formed and executed, as shown in Figure 26.
Finally, as another simple example of a step in a potential investigation, responders or analysts may need to determine how many systems are running a vulnerable version of software involved in an incident on another system. For example, an incident may occur on one system, with the root cause being exploitation of a certain version of Adobe Reader. Analysts could then search quickly for all other systems running this version, as shown in Figure 27.

Overall, Real Time Command has several flexible search options that allow analysts and responders to drill down into system details, which can help quickly pinpoint suspicious services, files or applications, or other issues. In conjunction with operations teams, responders can use Real Time Command to verify events and coordinate further analysis before actually requesting access to specific systems. Using sophisticated sensors to look for indicators of compromise and customized packages to, say, gather hash values for files or even update system variables, investigators could remotely manage a compromise scenario in a much more expedited fashion than without such tools.

Figure 27. Adobe Reader Versions
Although Real Time Command is not a security awareness platform as such, it offers security teams ample fodder for building better awareness-focused business cases and educating employees about security issues within the environment.

To demonstrate this, we examined a dashboard called Proactive Security that shows a number of system state attributes, many of which affect or reveal security posture. In Figure 28, you can see systems using DHCP to the left and those with local firewall profiles disabled on the right.

In this case, the systems with a disabled firewall may pose a risk to the organization, because malicious traffic won’t be blocked. Administrators can leverage their awareness of such systems to improve security by making profile changes or talking to users about why disabling the firewall can pose a security risk.

Another interesting view within this dashboard is local user information, which includes the last date of local administrator logins. This could be very valuable in getting visibility into illicit use of local credentials, or the use of potentially compromised accounts on endpoints. Figure 29 displays such logins.
A series of screenshots is shown in Figure 30, where administrators can quickly see endpoint hardware captured in a dashboard called System Inventory; details include (clockwise from upper left) network adapters, BIOS, memory and disks.

These views can help administrators identify users who may be using nonstandard hardware or systems within the environment.

On a similar note, many organizations are struggling with employees who install applications that aren’t standard or approved. Many of these could potentially expose vulnerabilities or lead to data being stored in cloud environments without the organization knowing it. Our final example focused on systems that may have Dropbox installed, which could lead to data being stored in the cloud without approval. First, we built a query using the Ask a Question menu, leveraging existing sensors that can assess and report on installed applications on any managed system, as shown in Figure 31.
This was incredibly simple, and it used nothing more than a keyword to scan systems for a pattern that matched “Dropbox” in the application list. The results—44 systems out of 482 that were active at the time—came back almost immediately, as shown in Figure 32.

As you can see, this kind of information could easily be used to not only monitor and control policy violations, but also build awareness training programs and tailored security policy announcements that can help end users as well as management understand why certain applications can be a devastating risk if not managed properly. In information security, more insight into what’s running in the environment is powerful and can help maintain a secure environment through both controls and education.

Figure 32. Systems Running Dropbox
This product was impressive. It was intuitive, easy to learn and usable immediately. There are a myriad of use cases for McAfee Real Time Command, limited only by imagination and time needed to configure sensors and packages to monitor and control systems. The intelligent query system was fast and helpful, providing full queries based on simple keywords and information we entered—even when we weren’t sure what we were looking for. This product could easily facilitate the collaboration of operations and security teams, allowing for faster monitoring and incident response. Operations teams can use this product as well, keeping up with patches and configuration states simply and quickly.
Dave Shackleford is the founder and principal consultant with Voodoo Security, a SANS analyst, instructor and course author, and a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft and CTO for the Center for Internet Security. Dave is the author of the Sybex book Virtualization Security. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>