



User Case Study: UDR, Inc.

About UDR, Inc.:

UDR, Inc. (NYSE:UDR) is a leading multi-family real estate investment trust (REIT) with a demonstrated performance history of delivering superior and dependable returns by successfully managing, buying, selling, developing and redeveloping attractive real estate properties in targeted U.S. markets. As of June 30, 2007, UDR owned 71,290 apartment homes and had 5,917 homes under development and another 1,108 homes under contract for development in its pre-sale program. For over 30 years, UDR has delivered long-term value to shareholders, the best standard of service to residents, and the highest quality experience for associates. An S&P 400 company, UDR is the fourth largest apartment REIT in the nation. With sales reaching \$68.7 million for the quarter ended September 30, 2007, UDR, Inc. continues on its path of steady growth.

Many new and exciting changes occurred in 2007 for UDR, Inc. including an entirely new identity. With a strong focus on innovation, UDR, Inc. (formerly known as United Dominion Realty Trust) re-launched in January 2007 with a new name and fresh strategy, which included a new interactive web site that reflected the company's updated look and feel.

With the arrival of the New Year, came a worm that was reported to UDR in error – the software they had in place detected it as a known worm which could be resolved, but in reality it was unknown with no available fix. As a result, malicious behavior proliferated as the worm had a party of its own and propagated itself throughout the company's network – infecting every machine.

Instead of champagne toasts at the stroke of midnight, the UDR network team consisting of seven administrators frantically tried to put an end to this worm that so quickly took down the network which supports approximately 2500 employees. It is a small IT team, when compared to companies of equal size, that supports both network and security functions from a central location but they work extremely efficiently and effectively. At the time of this crisis, the team realized the existing antivirus was outdated and a new, updated version would take 36 hours to arrive and remedy the situation.

Q1 Labs Delivered:

- ◆ Improved threat detection
- ◆ Significant ROI
- ◆ Excellent customer service



The Nexus of Security and Networking

“It was a nightmare. Our Symantec server blew up and this unknown worm proceeded to propagate itself filling up all of our routers with sessions. Our routers can handle 150,000 sessions at one time and it was blowing them out of the water,” said Josh Erosky, director of network services for UDR, Inc. “This attack opened up everyone’s eyes and made us realize that we needed additional help.”

With this attack behind them, Erosky and his team set out to assess the situation to determine what went wrong and what changes were required to avoid any future attacks. Assuming they had all the right technologies in place – firewall, Symantec anti-virus, and an IDS intrusion detection system – this attack demonstrated inadequacies in their network security capabilities including alerts, and especially centralized reporting. Thus began the exploration for a data collector that could pull together all the data and present it within one central console.

Erosky notes, “For the size that we are, the only way we can survive is to use technology to our full advantage. We don’t have two separate teams to manage both network and security – we have one team that does it all as there is just no other way to do it.”

Functionality, Customer Service and Support Key to Purchase Decision

During their search, Erosky and his team looked at many different vendor solutions and ultimately decided on comparing solutions from RSA, a division of EMC, and Q1 Labs. After an extensive 2 month evaluation process and feature comparison, UDR chose to purchase QRadar for its ability to:

- ◆ Identify and locate the source of any insider threat, infection, and BOT and immediately remedy the situation. What once would take UDR’s team hours to track down and resolve (if they knew about it at all), now took minutes, and in some cases seconds.
- ◆ Provide strong, satisfied customer references. Hearing customers’ experiences working with Q1 Labs versus other products gave UDR insight into Q1 Lab’s commitment to customer service and technical support, and definitely helped solidify the deal.
- ◆ Follow through with unparalleled customer service and support. According to Erosky, “Working with the Q1 Labs support team has been a great experience. They came in and let us test the product to see just what it could do for us: we realized it offered much more than just a data collection product would have offered.”

“We almost chose EMC since they were going to give us a great deal, but once we saw QRadar in action and got a taste for what it could do and realized its potential, we had to go with Q1 Labs, said Erosky. “QRadar’s drill down features were unbelievable, especially for the price. By choosing QRadar, we were able to get 10 times more features than what EMC was offering at half the price.”

QRadar – More than just data collection

In just a matter of hours, UDR had QRadars up and running, and according to Erosky “it did everything they promised and then some.”

With QRadars in place, Erosky and his team are confident that they are now prepared to see any potential security incident that comes their way. In fact, UDR has already managed to save Erosky’s team countless hours trying to locate network problems that would have gone either undetected or misdiagnosed with their previous architecture.

In fact, recently UDR noticed that an unknown source was using about 50 percent of the bandwidth. Knowing that many people in the company listen to AOL Radio during work hours, the network team automatically believed that was the cause of the problem. They shut down everything – AOL Radio, YouTube, and anything else that could drain bandwidth. UDR lacked the ability to identify positively the root of the bandwidth crunch but at the suggestion of Q1 Labs, they brought in a QFlow Collector, which could provide visibility into the different applications running across their pipes. With QFlow installed and running, UDR found out that the problem was not with AOL Radio, but was actually a configuration issue with one of its routers. Without QFlow in place, UDR would have continued to blame AOL radio as the cause of its bandwidth issues.

Another thwarted incident with the help of QRadars occurred when a UDR security engineer noticed huge spikes in network activity while watching real time traffic profiles. With QRadars, he immediately identified the source of the spikes –one machine that was draining bandwidth. The machine’s user was unaware of any issues with their computer. A simple shut down and restart of the offending computer resolved the problem.

For UDR, the decision to invest in Q1 Labs was the best choice. While it is difficult to attach a dollar figure that accurately reflects the costs savings realized by UDR from using QRadars, Erosky did express that the political benefits of being able to quickly identify the locale of security and network problems is unparalleled and that time savings alone are incredibly significant.

According to Erosky, “when my CEO or CIO approach me and ask about network issues, I can quickly describe the problem and provide accurate traffic updates. I look smart, my team looks smart, and everyone benefits. Our investment was well worth the money spent. It was actually a bargain when compared to all other solutions evaluated. Moreover, we have only just scratched the surface of what it can do. I am confident that it will easily pay for itself in a year’s time.”

About QRadar

QRadar goes beyond traditional security information/event management (SIEM) products or network behavior analysis (NBA) products to create a command-and-control center that can monitor, analyze, and remediate threats. QRadar combines, analyzes and manages an unequalled set of surveillance data—network behavior, security events, vulnerability profiles and threat information—to empower enterprises to manage business operations on their networks efficiently from a single console. More information about QRadar is available at: <http://www.q1labs.com/products/>.

About Q1 Labs

Commanding a unique position at the nexus of security and networking, Q1 Labs is redefining network security management. Q1 Labs' flagship product, QRadar, integrates previously disparate network and security functions into one solution. This convergence ties the impact of security threats directly to specific business assets and services, reduces acquisition and operation costs, and increases accuracy. Q1 Labs' installed customer base ranges from government agencies and financial institutions to universities and healthcare providers. Please visit <http://www.q1labs.com/company/> or call (781) 250-5800 for more information.



The Nexus of Security and Networking

Copyright © 2007 Q1 Labs Inc. All rights reserved. Q1 LABS, the Q1 Logo, QRADAR and the QRADAR Logo are trademarks or registered trademarks of Q1 Labs Inc. All other trademarks and service marks are the property of their respective owners. Specifications are subject to change without notice.

Corporate Headquarters

Q1 Labs Inc.
890 Winter Street
Suite 230
Waltham, MA
02451 USA

Telephone 781.250.5800
Fax 781.250.5880