Success Story

# BlackLine Cuts Incident Investigation Time by 85% with UserInsight

**Industry:** Finance
**Website:** www.blackline.com

BlackLine provides a leading, enterprise-class solution that delivers powerful real-time automation to accounting and finance teams.

Russ Swift is the Information Security Manager at BlackLine. "My job involves securing a very diverse environment," he explains. "There are some employees working remotely, several primary data centers, a corporate headquarters and satellite offices around the world."

As a modern financial organization, BlackLine puts security high on the business agenda. "A lot of my time goes towards ensuring that BlackLine's user base is secure, and for a while we had a specific blind spot in that area," says Russ. "We didn't have a good way to profile a regular user, or a way to understand what 'normal' activity would look like."

BlackLine uses Rapid7 UserInsight to gain visibility into threats and risk in their environment. When asked what the primary benefits of UserInsight are, Russ names two. The first is time savings. "It's made the security team able to investigate an incident much more quickly. When you compare it to our previous method of manually going through logs, it's reduced investigation time by roughly 85 percent."

> "UserInsight has made us aware of anomalous events that we wouldn't otherwise know about. Even if we had the data, without UserInsight we would have no way to correlate the separate pieces of information to give us an accurate picture of the event."

The second benefit, according to Russ, is visibility. "UserInsight has made us aware of anomalous events that we wouldn't otherwise know about," he says. "Even if we had the data, without UserInsight we would have no way to correlate the separate pieces of information to give us an accurate picture of the event. For instance, if someone successfully logs onto a server in your network, you won't know whether that log-on is anomalous. Even if you're collecting logs of successful log-on events, you'll just know that a user successfully authenticated to a server to which they seem to have legitimate access. But what if the user in question doesn't typically access that server? UserInsight will correlate additional data points, such as antivirus infections or other IDS alerts, to alert on that type of activity."

> "[UserInsight has] made the security team able to investigate an incident much more quickly. When you compare it to our previous method of manually going through logs, it's reduced investigation time by roughly 85 percent."
>
> **— Russ Swift,** Information Security Manager at BlackLine

## Setup

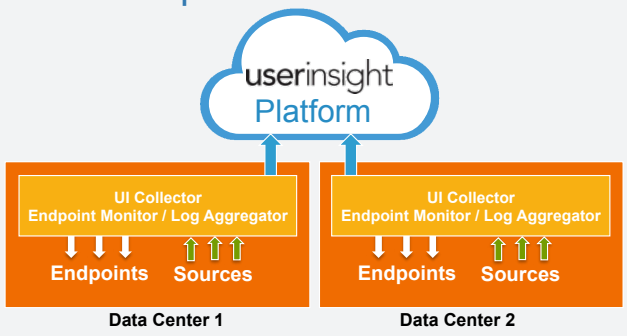
BlackLine has taken UserInsight to the next level by integrating it into the fabric of their business environment to get even better analytics. "There's a saying, a thing is what you use it for. That's especially true in this case," says Russ. "We've taken what was a great product to begin with and tailored it to meet the requirements of the organization."

"We've added a few log sources to UserInsight. LDAP is the primary log source, but the list includes DNS, VPN, DHCP, Radius, Firewall, IDS, Rapid7 Nexpose, Antivirus, endpoint scanners, and syslog relays that get forwarded. All edge relays go to the central syslog server. Basically, I took the recommended UserInsight setup and adapted the suggested architecture to meet the needs of the business, because for us flexibility was quite important."

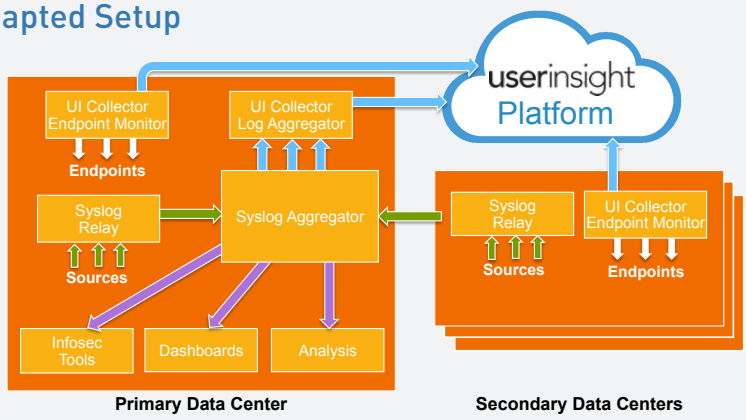
## Standout Features

UserInsight can detect malicious processes on endpoints without having to deploy any software on those endpoints. "I love that functionality," says Russ. "And it's great at monitoring endpoints. Once I encountered a situation where someone had installed a piece of spyware that didn't connect out of the network. It snuck by the antivirus scanners, but UserInsight caught it."

### Recommended Setup




### Adapted Setup




UserInsight also offers a feature that many incident investigation and detection products lack: the ability to set intruder traps. These include honeypots, which are decoy machines that detect network scans, and honey user accounts, which help spot intruders stealing user lists from a directory service.

"At BlackLine we're running multiple honeypots in UserInsight, which will be triggered if anyone tries to scan our network. Recently, we received an alert from a honeypot that made us aware of a rogue scanner in our environment – that was really good to know. We've even set our own unique traps."

"Honeypots and honey users are a valuable source of data for my team. Using these features, we've found malicious insiders trying to get into stuff and enumerating systems. Once I even found my boss poking around, which led to a few laughs in the office. But we've also discovered people using tools that we didn't know about. Once it hits the honeypot, we get an alert and can ask IT what's going on."

## Accelerating Incident Investigation by 85%

During the investigation of a security incident, time is of the essence. Attackers can be fast, so swift detection and investigation is key. Prior to UserInsight, BlackLine had only a limited ability to detect an intruder moving laterally throughout the network. The tools they were relying on were not scalable and not automated. This, Russ points out, was a weakness they needed to correct.

"It took just one week for us to deploy UserInsight and start to see its value," says Russ. "For starters, it's cost-effective to license and maintain, and as I mentioned earlier, with UserInsight up and running I completed one investigation in a single day, which is an 85 percent reduction in time."

In many cases, incident investigations require manually pulling together disparate data from their SIEM into a report that identifies the assets and users which could potentially be compromised. Before deploying UserInsight, BlackLine was no different. "The right information can be hard to get," explains Russ. "UserInsight provides intelligent correlation as a result of all the log sources we have feeding into it. It correlates antivirus alerts, IDS engines, firewall alerts, and the like, and links all the data together to reduce the complexity and present actionable information. It saves me from having to wade through a sea of log data. UserInsight provides an intelligent, actionable alert in real-time. That's fantastic. Often, as a security practitioner, you can find yourself drowning in data from many different locations."

> "At BlackLine we're running multiple honeypots in UserInsight, which will be triggered if anyone tries to scan our network."

## Alerts and Anomalies

Russ has many UserInsight anecdotes: "A few months ago UserInsight flagged that a generic Active Directory account had been given privileged access to HR systems containing sensitive data. Two employees were suspected to have the credentials; they were put on leave while my team investigated. Another time, someone from HR asked IT to disable an employee account. Then, once they had done so, IT was asked to reenable it. UserInsight immediately alerted me about anomalous usage for that account. Luckily, in this case it wasn't nefarious, but it's crucial that we have that visibility in case a terminated employee ever does try something malicious or simply wants to take information that they aren't entitled to."

UserInsight is designed to produce intelligent, low-noise, high-value alerts that call immediate attention to sophisticated intruder behavior patterns. Russ appreciates that the product has never overwhelmed his team with information or caused alert fatigue. "A lot of the alerts we receive from UserInsight have to do with flagging anomalous user behavior, or the occasional infected system, so we can determine whether it's an incident which needs to be investigated further. For example, I just received an alert revealing malware that was not detected by our primary Antivirus deployment. Another time, someone cleared their event logs which, by itself, is only mildly suspicious – but in conjunction with other activity became an actionable event."

BlackLine continues to innovate and leverage UserInsight's existing capabilities. Russ says, "We are currently using UserInsight to monitor cloud platforms which will become increasingly useful as we roll out new services to our customers and employees.