Success Story

Redner's Markets Leverages Rapid7 Nexpose® and InsightUBA for Compliance, Vulnerability Management, and Incident Detection

Industry: Retail
Website: www.rednersmarkets.com

With breaches making regular headlines, security teams are under more scrutiny than ever before. This is especially true in retail, where strong security practices are paramount to protecting customer and organizational data.

Challenge: Maintain PCI compliance, and gain visibility into suspicious or anomalous user behavior on the network, from the endpoint to the cloud.

Solution: Nexpose and InsightUBA simplified compliance and incident detection and investigation.

Nexpose for PCI Compliance, Vulnerability Management

PCI compliance is a key component of any retail organization's security program, and Redner's Markets is no exception. The supermarket chain is a level 2 merchant that must conduct regular vulnerability scans in order to maintain compliance.

"Compliance was what began our relationship with Rapid7," explains Nick Hidalgo, Director of IT at Redner's Markets. "We purchased Nexpose for PCI compliance, and afterwards we brought on InsightUBA." He and his team are tasked with securing a business environment that includes more than 700 point of sale machines across 45 traditional supermarkets, 18 gas stations, and three corporate facilities. "InsightUBA watches over everything," he laughs.

Not surprisingly, Nick counts the PCI features within Nexpose as his go-to for showing the efficacy of compliance practices and controls, as well as generating PCI security audit reports and remediation plans. But he also views Nexpose within the broader context of a vulnerability management program, not just PCI, and is constantly pushing to measurably reduce risk over time.

Nexpose enables Nick to focus on being efficient with the remediation strategies and risk reduction practices that will lower the organization's overall risk score: "Sometimes one Java patch will address 50 vulnerabilities on a single machine; knowing what actions are high impact makes a big difference."

InsightUBA for Incident Detection and Investigation

Another PCI requirement calls for collecting logs and reviewing them daily. To satisfy this mandate, Redner's uses a security information

"If someone breaks into your network, and they know that your policy locks out a user who makes three unsuccessful login attempts, then they can circumvent that by trying to log in twice across 200 machines. You need to ask yourself, would I catch that? Without InsightUBA, the answer is no."

—**Nick Hidalgo**, Director of IT, Redner's Markets

and event management (SIEM) solution that Nick says is "quite flexible when it comes to configuring a multitude of security log sources." However, he adds that InsightUBA enhances the SIEM by providing useful information without all the effort. "Here's an example scenario: If someone breaks into your network, and they know that your policy locks out a user who makes three unsuccessful login attempts, then they can circumvent that by trying to log in twice across 200 machines. You need to ask yourself, would I catch that? Without InsightUBA, the answer is no. Our SIEM would only have caught it if the attacker was using domain credentials; local machines are a blind spot."

InsightUBA's intruder analytics provide Nick and his team with security alerts that matter and also help with incident detection and investigation. "Because of PCI, we keep archives of potentially relevant security events. To get the same degree of visibility without InsightUBA would take a heck of a lot more work. It's elegantly simple in how it functions. Having an agentless endpoint monitor delivers tremendous value, as well. Monitoring all of our POS machines was really easy to set up. Getting this done with our SIEM would have taken months, so this feature alone made the investment worthwhile."

Nick has taken full advantage of InsightUBA's various technology integrations. "I have connected as much as possible to it," he says, "including our antivirus solution for endpoint protection. The endpoint monitoring features in InsightUBA are what I personally find to be the most valuable, because it encapsulates so many machines and scales to cover every endpoint, not just ones in the 'PCI zone.'"

While endpoint monitoring ranks as InsightUBA's biggest selling point for Nick, there are other features he appreciates:

- **Detection without having to write rules:** "Rule programming in our SIEM was a huge time sink. With InsightUBA, we don't have to worry about the rules – Rapid7 constantly develops and maintains detection rules for us."
- **Highlighting privileged accounts:** "It opened our eyes to how many domain admin accounts there were. Did we really need them all? No. The same thing goes for services accounts: certain people had passwords that never expired. I was able to makes changes to all that."
- **Quicker incident investigation:** "Due to the current state of the marketplace, I need to be confident that I can detect an incident in a small amount of time. With InsightUBA, I can do that with just a few clicks."
- **Noise reduction:** "We've had to turn down the notification level of some of our other security products because we were getting too many garbage alerts. InsightUBA provides just the right amount of information with roughly 5 to 10 alerts per day, all of which provide value."
- **Reducing the impact of phishing attacks:** "It's handy to know if someone within the organization has received an email with a bad link in it."
- **Tracking activity from third party vendors:** "I've set up 'flags' for certain vendor accounts, in order to get an alert when they log in remotely. One time a vendor logged in at 2 o'clock in the morning and I was able to confirm whether it was legitimate activity. Knowing about remote logins is big for my sanity."
- **Flagging credential compromise from third-party breaches:** "If millions of accounts are compromised, InsightUBA will do the legwork. Using the Adobe breach as an example, I'd get an alert that shows me which user accounts that are part of my environment were involved in that breach."

- **Exposing shadow IT:** "InsightUBA shows me when certain people are using unsanctioned cloud services, like Dropbox."
- **Honey pots:** "The honeypots are a great idea for detecting illegitimate network scans."

With so many useful features within the product, how did Nick decide on making the business case for InsightUBA to upper management? "I just say, 'This software will allow us to detect if someone has broken in.' Plus, it's very simple to deploy and use and provides huge value – it was a no-brainer for us."

Redner's Markets, Inc., an employee owned company, currently operates 45 Warehouse Markets and 20 Quick Shoppes throughout Eastern Pennsylvania, Maryland and Delaware. Redner's is committed to supporting the community in which each Warehouse Market and Quick Shoppe is located through a variety of supportive partnerships and enrichment programs. Redner's continually strives to provide the lowest prices, freshest product and the outstanding service our customers have come to expect for 44 years.