CASE STUDY

Case Study

Developing a business-specific risk reduction plan through visualized security

About the Business

This organization is a market-leading property and casualty, accident, health, and specialty insurance solutions with a nearly 200-year history of helping their customers manage risk.

The Challenge

The insurance company's cybersecurity team sought to develop incremental methods to mature their vulnerability management programs. The cybersecurity team is led by Chris, who sought to increase the efficiency of his team and develop more targeted risk reduction processes that would reduce the greatest amount of risk unique to the business. However, disparate data sources created a challenge that resulted in manual analysis and challenges in reviewing all risks.

CASE STUDY

Vulnerability Management

"Vulnerability management is a thorn in the side for every company. The volume of vulnerabilities we had surpassed our ability to effectively remediate all of them just like every other large complex organization," reflected Chris. "We did what any other security team does, and looked at the severity of vulnerabilities based on CVSS scores. We then tried to prioritize those based on disclosure dates -- the longer the vulnerability had been disclosed for, the more likely it could be an issue identified by attackers. But the approach and our team's capacity to manually analyze these vulnerabilities didn't have a large risk reduction, and we wanted to improve our business-specific risk analysis processes for vulnerabilities."

"The hazard when working with unintegrated solutions is we need to accommodate each one's limitations in data. We'd need to log into Rapid7 to identify the vulnerability and assets with it, and then separately correlate that manually with other tools' data," commented Chris. "The hazard is each tool has its own method for data - for some, it's an IP, others it's a domain, and even when we did correlate after two days we still needed to understand the impact to the business. To accomplish this, it would take a lot of time from each analyst which we needed to reduce to achieve efficiency."

To develop a business-specific model for vulnerability prioritization, Chris and his team sought to develop a single source of truth to converge their network and business information with their Rapid7 scanning output.

"The reality is that what one organization considers a risk won't be the same to another."

- Chris, CISO

Achieving Visibility

To achieve a more effective and efficient vulnerability management program, Chris and his team implemented appNovi to contextualize their Rapid7 vulnerability data with their netflow data.
The result is visibility beyond assets and systems. The team not only gains better insight on directly exposed vulnerabilities to the internet, but they understand which assets are indirectly exposed to drive effective mitigation and remediation to reduce the most amount of risk to the business.

CASE STUDY

Reducing Risk

"Historically speaking, there hasn't been an effective method for automatically understanding how vulnerable systems were communicating, so it's something we hadn't pursued," noted Chris. "Once we were able to consolidate our netflow data with assets and vulnerabilities, we could map out our complex network, understand the assets with vulnerabilities, and what other assets would be impacted if that vulnerability was exploited. We continue to mature our risk management processes, and appNovi is the latest iterative step to enable us to understand where the greatest risks are unique to our business."

Reducing Risk

Having obtained a greater level of visibility over the network and vulnerabilities, Chris's team continues to mature the effectiveness of their risk reduction efforts while achieving greater efficiency in doing so.

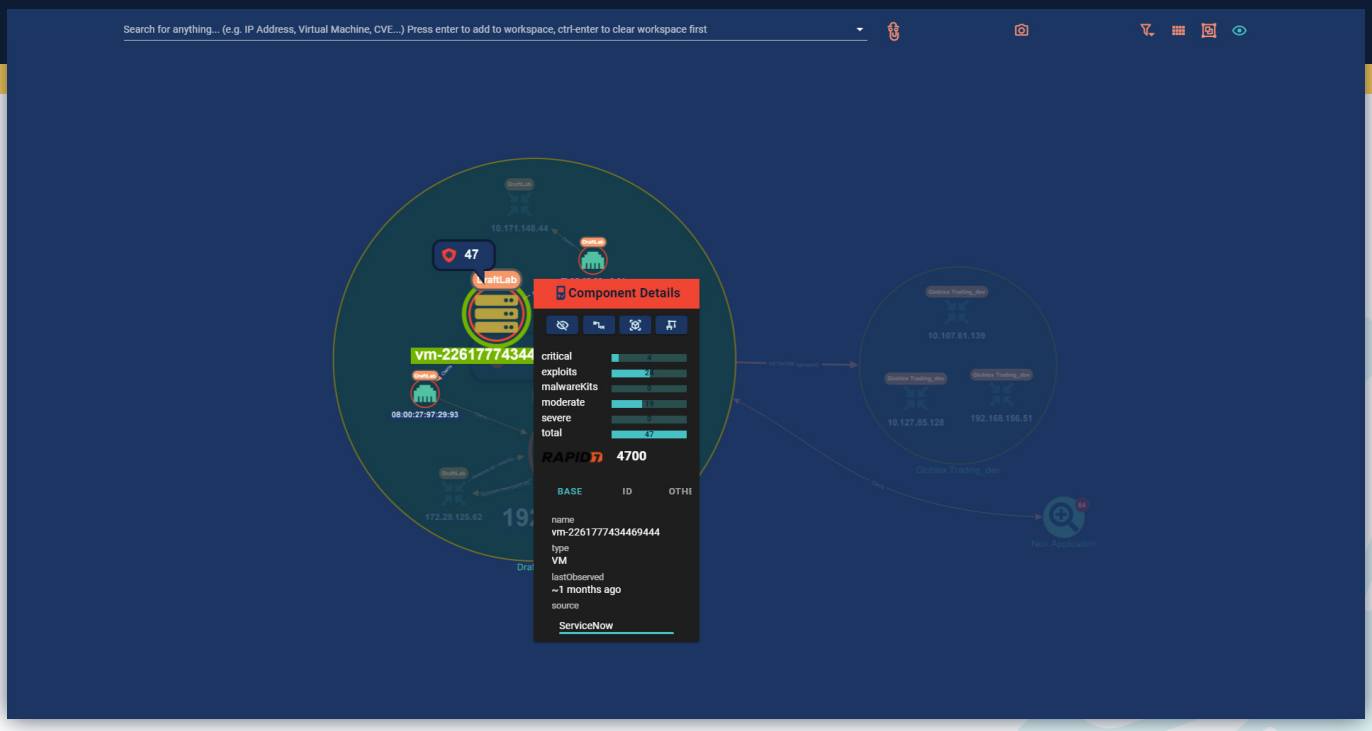
"appNovi enables us to identify the risks with the greatest impacts to the business, which leads to our patching being more efficient, which brings down our time and resources on analysis and enables us to remediate risks that truly match business risk," asserted Chris. "The reality is that what one organization considers a risk won't be the same to another, and we're confident in our business-specific risk management process in which appNovi is a critical piece in maintaining and growing."

Once we were able to consolidate our netflow data with assets and vulnerabilities, we could map out our complex network, understand the assets with vulnerabilities, and what other assets would be impacted if that vulnerability was exploited.

- Chris, CISO

SOLUTION BRIEF

appNovi for Vulnerability Management



Vulnerability management is the identification of risks in your environment, prioritization of risk reduction, reduction of risks through remediation or mitigation, and tracking the outcomes of risk reduction efforts.

appNovi is the only security analytics and visualization solution that enables vulnerability management teams to identify the assets, teams, and businesses impacted by vulnerabilities to effectively prioritize vulnerabilities across their hybrid network. By correlating your CMDB data with your vulnerability scanning output, network assets and their importance to applications and business operations is understood.

appNovi enriches vulnerable infrastructure datasets with network logs to provide the ability to understand contextual exposure of assets for exploitation, connected assets actively communicated with, and the impact of a vulnerable exposed asset to other accessible and vulnerable assets, and mitigation and remediation options available.