CASE STUDY

Harmony Purple: Solving Vulnerability Management Challenges at Lowell Five Bank

THE COMPANY

Lowell Five Bank is a regional savings bank with 16 banking centers located in Massachusetts and New Hampshire. With over $1B in assets, Lowell Five takes its responsibility to protect client assets and personal information very seriously. At the same time, it must operate efficiently – it needs to maintain security without business interruption and within the budget limitations of a community bank.

THE CHALLENGE

The IT team at Lowell Five Bank faced ongoing difficulties managing vulnerabilities. They had replaced an agent-based system with an agentless solution from a leading vendor but frequent, random gaps in discovery created a lot of extra work for the IT team – tracking down the IPs that the system was failing to report on and manually adding them in for analysis. We spoke with Thomas D'Entremont, VP of Network Systems at Lowell Five Bank, about how Harmony Purple helped his team solve these issues and improved their process for managing vulnerabilities and meeting audit requirements.

CHOOSING A NEW SOLUTION

Tom and the IT team decided on using an agentless approach due to ease of use and to avoid having to manage, maintain and troubleshoot software agents on the over 1000 IP end points needing protection. However, it was critical that the agentless system be fully reliable in discovering and scanning IPs distributed across many locations, subnets and VLANs. After evaluating several solutions, they chose Harmony Purple because it met their needs for reliability, efficiency, the clarity of its reports and cost.

THE INSTALLATION

> *Setting up the system was fast and easy. In two or three days it was up and running and scanning everything it should*

Thomas D'Entremont, VP Network Systems
Lowell Five Bank

THE RESULTS
EFFICIENT AND EFFECTIVE VULNERABILITY MANAGEMENT

Traditional vulnerability management systems prioritize patching based on severity level of CVE, with little consideration to the context of the system that has the vulnerability. Harmony Purple's unique attack path scenario analysis provides that needed context. It identifies which systems are exposed to which vulnerabilities and identifies the level of risk those vulnerabilities pose to the organization.

The attack path scenario analysis benefits the bank in several ways. It allows the IT and security team to meet the mandates for secure operations without excessive maintenance downtime. In addition, the clear, concise reporting enables them to effectively communicate status to senior management and the audit committee. As Tom said, "When we communicate to the audit committee and to executives, we need clear reports in language that they understand. The executive reports from Harmony Purple are great for that."

> *We really like the attack path scenario approach in Harmony Purple. It is very valuable for identifying which systems need patching, and it helps us communicate clearly to the audit committee.*
>
> Thomas D'Entremont, VP Network Systems
>
> Lowell Five Bank

AN ONGOING PARTNERSHIP

Timely and responsive support is critical when dealing with IT security. The bank needs a vendor partner that responds quickly, knowledgeably and transparently when issues arise. Tom let us know his high satisfaction with the support he has received from Orchestra, "Whenever we have had to deal with support, they have been fantastic. Very quick to respond. They let us know what their thoughts are and how they are going to resolve the issue."

SUMMARY OF BENEFITS

Reliability	More consistent and accurate end point discovery and scanning.
Efficiency	Reduced emergency patching and system downtime.
Clarity	Improved communication to executives and the audit committee.