



# FinTech Innovator Lumin Digital Deploys Uptycs as Premium Visibility Layer on Its macOS Workforce Endpoints

## Company

Lumin Digital

## Champion

Sean McElroy, CSO

Lumin Digital

## Workforce Endpoint Environment

macOS

*“Uptycs simplifies investigations and saves time—about 30% time savings per investigation. The additional context Uptycs delivers gives our security operations team a high degree of confidence that we’re doing all we can to safeguard our workstations and our business.”*

Sean McElroy

Chief Security Officer, Lumin Digital

## Lumin Digital Redefines Digital Banking

Fintech innovator Lumin Digital's cloud-native platform redefines digital banking for financial institutions. The platform provides a comprehensive and contemporary integrated suite of capabilities built on the industry's most sophisticated technologies and best practices. Banks and credit unions can now offer exceptional user experiences across platforms; these create more personalized journeys and connected relationships through highly targeted, actionable, and unique digital interactions.

Financial institutions can now innovate at lightning speed and with minimal risk. Lumin Digital's platform permits new features to be rolled out without any interruption of services, thereby assuring high performance with safety and security.

## The Security Focus Is On Workforce Endpoints

Chief Security Officer Sean McElroy joined Lumin Digital in its early years, bringing the perfect mix of experience in digital banking and cybersecurity with him. He understands how to provide managed banking services in a highly regulated industry. Today he oversees the company's Enterprise Risk Management Group.

## Security Challenges

- Get more context around alerts raised by SentinelOne to facilitate incident response
- Provide user device CIS compliance benchmarks in a regulated fintech environment
- Discover what's installed on devices beyond just applications

McElroy's team is primarily focused on securing the company's fleet of some 200 macOS endpoints. The cloud-based server environment is not a concern for a rather unique reason: "Our server infrastructure is 100% containerized," says McElroy. "Our situation is unique in that the average lifespan of one of our servers is two and a half days. Our engineering team has gone all in on the concept of immutable infrastructure. If we want to make a state change, we just build another server to replace the old one. We do all this through automation. It's very secure because it's really a read-only immutable environment."

The workforce endpoints are more vulnerable to compromise. Here, the company has built an effective security stack around them; it involves a set of tools that includes the Uptycs sensor.

*"Our tech stack is a little unusual because there's an extremely low degree of variability in our servers, but potentially a high degree of variability for our workforce endpoints. That's why we've deployed Uptycs for those devices."*

**Sean McElroy**  
CSO, Lumin Digital

## Building The Security Tech Stack Piece By Piece


The team initially used Jamf for its fleet management. This was useful for deploying policy and configuration profiles, but it didn't help with knowing the state of the devices.

Later, they added the SentinelOne EDR solution to help detect threats. "It's good at doing certain things to increase our workstation security," says McElroy. "SentinelOne looks for bad stuff and figures out how it got on a device. But outside of that use case, it's not a generalized tool. Also, it's not designed to show you how a machine looks from a compliance perspective because there aren't any compliance templates to deploy with SentinelOne."

Lumin Digital first considered Kolide, but at that time that product wasn't robust enough to justify its cost. The security team also needed more context around alerts. It turned to Uptycs, specifically for its osquery-based approach to delivering rich, purposeful security telemetry.

### Uptycs Results

- Uptycs provides an enriched, premium visibility layer on top of SentinelOne EDR
- Uptycs' CIS benchmarks enable Lumin Digital to replace old and hard-to-maintain scripts written for Jamf
- Uptycs easily visualizes everything on macOS devices to provide a complete inventory of plugins and third-party packages



*“SentinelOne gives us an alert. Is it normal? Maybe we’re seeing this one for the first time. If the historical background isn’t part of a finding, we don’t get much for baselining. So we were looking for something that SentinelOne and Jamf couldn’t provide. Uptycs is the software that really ticks the boxes for us.”*

**Sean McElroy**  
CSO, Lumin Digital

## Uptycs Data Provides Enrichment To Investigations

“We went with Uptycs for our workstations because it pulls a wide variety of metrics and stores them in our own security data lake in the cloud. We can review whatever metric we’re interested in over time. We can go back to see what’s normal and when something suspicious is going on,” says McElroy. “We can build compliance baselines using CIS benchmarks out of the box. Or if we just want to internally define something, we can do that, too. Maybe we just want to know what’s going on regarding a policy. Uptycs is extensible enough to do that, whereas SentinelOne isn’t suited for that, and it’s not intrinsic to Jamf. Uptycs ticks the boxes to complete our endpoint security stack.”

While Uptycs also offers preventative capabilities, Lumin Digital didn’t want to uproot SentinelOne. “We treat Uptycs as an enriched, premium visibility layer on top of SentinelOne as opposed to a replacement. Uptycs tells the story of how something got on a user system, which SentinelOne doesn’t do.”

He gives an example of SentinelOne giving an alert. “We look at the finding and have no idea if it’s true or false. SentinelOne helps us do some first-level analysis, like ‘What’s the path?’ Is it in a known file hash database? If everything comes up OK, we want to mark it as a false positive, but that shouldn’t be the end of the story. With Uptycs, we can build a bigger picture to learn ‘How did this get here? What other kinds of browser extensions or package managers does this developer have on their machine that might be installing things?’”

McElroy says the osquery dataset lets them assemble both a timeline and assess how the workforce might be circumventing rules—though not necessarily in a malicious way—to do what they need to get done. The security team doesn’t have visibility in SentinelOne to know whether something is good or bad, which is how Uptycs completes the backstory.

## Simplified Investigations Yield 30% Time Savings Per Investigation

One big benefit of having Uptycs on macOS is that it's now easier for a level one analyst to do deeper investigations. McElroy says, "I want to give the easy stuff to the people who are developing their skill set."

*"We can help junior-level people add value to the team by giving them a tool that provides much more visual context and lets them drill down deeper. Uptycs simplifies investigations and saves time—about 30% time savings per investigation."*

Sean McElroy  
CSO, Lumin Digital

## Deeper Security Visibility Into Developer Plugins, Package Repositories, And More

Uptycs provides visibility that none of Lumin Digital's other tools can. It visualizes things other than applications installed on an endpoint—Visual Studio plugins, browser plugins, brew, and other package managers like Python—things that are actually running on developers' machines. "As you probably know, those package repositories get compromised and could be a vector for the next update to incorporate malware. But they don't show up in a list of installed applications" says McElroy. "Uptycs is the only tool that gives us that important insight."

McElroy says Uptycs is one of the best tools for macOS environment visibility. "We understand our risk profile better from the latent posture coming from Uptycs that we can from SentinelOne that's looking for the bad thing that's just happened. The additional context Uptycs delivers gives our security operations team a high degree of confidence that we're doing all we can to safeguard our workstations and our business."

*"What stands out the most about Uptycs are its people. They have a high level of engagement and take a strong interest in helping to solve our problems."*

Sean McElroy  
CSO, Lumin Digital

## About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive, enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

**Shift your cybersecurity up with Uptycs.**

