

Putting Intelligent Workloads on the Path to Wisdom

by Richard Whitehead

**Caine: I will prepare myself, Master.
Master Po: That is wise, Grasshopper. That is wise.**

Long before Yoda imparted his wisdom on Luke, Master Po was teaching Caine some of life's most important lessons. It seems we've all found ourselves under someone's mentorship at one time or another. Someone who tried to teach us right from wrong. Someone who showed us a different way of thinking. Someone to show us the path to wisdom. Why should intelligent workloads be any different?

The next evolution in intelligent workload management (IWM) is going to be what I'm terming "wise workloads." Now there's no hard and fast definition for these sage bits of software. IWM itself is still evolving. Wise workloads are simply where I see IWM ultimately headed.

Like intelligent workload management, wise workloads will be identity-enabled, secure and compliant. They will also traverse all physical, virtual and cloud computing environments—while remaining unscathed. IT staff are able to monitor and track them wherever they may be running—but they don't really need to. That's because wise workloads will be capable of monitoring themselves and their environments. In fact, and this is the "wise" part of the equation, the workloads have moved beyond simple intelligence and are able to learn from their experiences.

> The Evolution of Man—and Workloads

Consider this: As humans, we have an innate desire to learn, but it's not until we put our knowledge into practice that we can truly become wise. For example, say you're walking to the neighborhood grocery store late one night. You're about to take your favorite shortcut when you hear gunshots down that particular alleyway. You decide it might be more prudent to take the slightly longer way around.

I submit that future workloads will be capable of something similar to this behavior. Based on their initial programming and what they learn from their experiences, they will be able to better predict outcomes to scenarios encountered in any given environment and make wise choices. Hence, they will be more capable of completing their functions, protecting their data and staying within compliance.

> Novell Operations Center: Turning Knowledge into Wisdom

The ultimate solution for making workloads wise is [Novell Operations Center](#). This customizable console plays a critical role in reducing costs and gaining control over complex physical, virtual and cloud infrastructures. Novell Operations Center simplifies and automates this process of monitoring and measuring business service levels (including the customer experience) of virtually all business service you define.

> Sentinel 7

While Novell Operations Center may be the majordomo of wise workloads, [Novell Sentinel 7](#), its able-bodied counterpart, has its back. This newest version of Novell Sentinel offers improved data baseline and trending, enhanced corporate interaction, advanced reporting tools and numerous productivity-enhancing features.

> Improved Data Baseline and Trending

Essentially, there are two primary methods used to detect threats: The first involves knowing exactly what the threat is and what it looks like. The second requires a good understanding of your operating environment and the ability to identify when something out of the norm is occurring. To protect your organization against both known and emerging threats, you need to be able to establish rule sets that can detect threats in both ways.

However, this second detection method has been historically difficult to enable. Other vendors have tried and failed, as they haven't been able to solve the problem of false positives. That's because their systems haven't included enough intelligence to be able to tune them such that you know the anomalies you are seeing are actual anomalies.

With Novell Sentinel 7, Novell has raised the bar on detecting emerging threats. Through real-time analytics, IT environments can proactively trend the data it sees against set baselines and alert IT staff when they detect an anomaly. Now organizations are able to protect against unknown threats before they occur.

For example, say IT staff have established a baseline for the typical number of unsuccessful login attempts encountered after hours. Novell Sentinel 7 notices an unusually high number of unsuccessful logins late one night—a pretty good indication of a hack attempt—and alerts a security analyst by text message, so they can look into it.

> Enhanced Corporate Interaction

Another area where Novell has made improvements to Novell Sentinel is in bridging communications between corporate security analysts and the administrators who actually configure the security policies. Through shared interfaces, security analysts and system administrators can work together to create correlation rules that target current and future anomalies that may threaten the organization.

> Advanced Reporting Tools

It's no secret that a reporting war is raging among security vendors. Vendor A says they offer 500 out-of-the-box reports. So guess what. Vendor B's next product release features 520 reports. How many of those generic reports do you think are actually usable by the average organization? Likely only a small fraction. Organizations want to be able to search through data and turn it into reports that are meaningful to them.

With Novell Sentinel 7, Novell has changed the game in the reporting wars. Our base reports focus on specific security analytics, based on a unified compliance framework. This puts the right information in the hands of the right people.

> **Productivity-Enhancing Features**

Perhaps the best aspect of Novell Sentinel 7 is that it's designed to enhance productivity. After all, who has the resources to have humans monitoring their systems 24x7? Systems need to learn how to monitor themselves and make the appropriate decisions based on what they learn. Or, as Norman Cousins put it, "Wisdom consists of the anticipation of consequences." In my book, therein lies wisdom.

> **Novell Sentinel 7's Place in the Cloud**

When designing the newest release of Novell Sentinel, Novell surveyed its customer base as well as the market to understand the perceived security vulnerabilities and associated threats. The resulting Novell Sentinel 7 fits perfectly into the company's WorkloadIQ paradigm, as it is at once intelligent, secure and cloud-ready.

While other security vendors continue to focus on the network, Novell has moved beyond the firewall to the cloud, where an increasing amount of application activity is taking place. Novell Sentinel 7 is fully capable of monitoring applications running in the cloud and correlating that activity with what's happening inside the firewall—to give companies a truly complete picture of their security.

> **Putting Wisdom to Work**

One company that's seen the wisdom of putting Novell Sentinel to work for it is Sony Italia. To meet new Italian government regulations for protecting personal data privacy, Sony Italia worked with Novell and H4T to implement Novell Sentinel Log Manager. In little more than a week, Novell Sentinel Log Manager was up and running, monitoring multiple servers and pulling all relevant data into a single database for easy reporting. Today, Sony Italia is able to comply with the new privacy legislation with minimal effort.

You can learn more about Sony Italia's story at www.novell.com/recording/videos/review/sony_italia.html

> **"When You Can Take the Pebble from My Hand..."**

While we talk about intelligent identity, smarter security and craftier compliance, the ultimate goal is wise workloads. Workloads that are able to care for themselves and stay out of harm's way. It's an achievable goal. And we're already on the path. Who knows, someday soon, we may be able to say that the student has become the master.

–Richard

Learn More

- [Novell Operations Center](#)
- [Novell Sentinel 7](#)