THE FUTURE OF ERP

Always watching: 24/7 security monitoring and the shared responsibility model

Richard: Welcome to the Future of ERP, a podcast where we discuss hot topics, latest trends, and innovations across global business. I'm Richard Howell, and I'm joined by my wonderful cohost, Oyku.

Oyku: Hello, everyone. I'm Oyku Ilgar, a marketer, blogger, and podcaster in the supply chain and ERP area at SAP. Today, we'll be talking to Michelle De Liberty from EY about the importance of security when it comes to cloud ERP, and specifically, 24/7 security monitoring and the shared responsibility model. Michelle, lovely to have you on the series. Could you please introduce yourself and your current role at EY?

Michelle: Hi. Yeah, thanks for having me. I am in our EY cybersecurity practice and technology consulting, and I have been focused primarily on our cyber for SAP capability and competency. I've been in the technology and cyber consulting industry for well over 20 years. So I have a lot of interesting experiences along the way with SAP and then more broadly outside of SAP with cyber and technology transformation, mergers, and acquisitions.

Richard: I bet you've also seen a lot of change over those 20 years as technology has evolved and we've moved to the cloud and so on. I want to get straight into the topic at hand. When we talk about 24/7 security monitoring, what exactly are we referring to in a modern cloud ERP environment?

Michelle: It's definitely changed over the years, right? Security used to just be infrastructure and firewalls and keeping an eye on that. But with the world of the internet and everything moving to the cloud, everything has changed. The biggest thing that I like to say about security and monitoring in general is that it's really about ensuring the business and the business value are protected operationally.

We want to make sure that the business is enabled to go out and make product, ship product, and make money ultimately, right? And bring products and services to customers. So when we talk about 24/7 monitoring, that's a huge part of it. Making sure that you have visibility to all of your critical assets. You understand your critical business processes within your organization and understand the broader ecosystem.

When you have visibility into those things, you can then implement the correct monitoring tools, alerts, and capabilities. The idea is really to be proactive about anything that doesn't look normal in the system. When we talk about 24/7 monitoring, all of that comes into play. There are many tools out there, but really at the heart of it, it's protecting the business.

Oyku: As cloud adoption continues to rise, understanding who's responsible for what becomes increasingly important and a little confusing for some of us. Maybe you can explain this shared

responsibility model to someone who is totally new to cloud security. And if you can, give us your perspective and explain a little bit about what falls on the provider and what remains the customer's responsibility.

Michelle: Everyone used to have their own data center. Back in the day, over my 20-plus years, people had their own data centers. They would rack-mount their own servers. They knew where everything was.

Today, primarily everything is hosted by a cloud provider or a software- or platform-as-a-service provider. Things that the business and organization had control over, specifically in security with monitoring and even the ability to patch and receive notifications or certain administrative privileges, all change.

The biggest thing is that if you can touch it, if you can configure it, then you are accountable for it. But at the end of the day, the business that owns the data is also really the end-all, be-all that's accountable. So it's up to the business to make sure they're comfortable with the security model that's in place and that they understand who has the accountability and responsibility.

When things move into the cloud—and this is a big one for SAP because it's always been in maybe a private cloud or within its own data center—it changes quite a bit. Customers are responsible for user access, data, authorizations, approving access, custom code, and business monitoring.

The platform could be the database and the infrastructure layer. All of that becomes more the accountability of the provider who's hosting. Whether it's SAP or one of the big cloud providers, control over the physical infrastructure layer is more handled by the provider.

It's important to understand, especially when you get into patching and who's responsible for patching at which level. Much of it is shared. The accountability is shared. Then when you get into incident response, it's important to update the playbooks and make sure that your role is understood.

Should you have an incident, your playbooks should be updated appropriately with who you need to call and when, and the correct prioritization of incidents that reflects your organization's priorities. That's a big one we see organizations working through as things change.

Richard: And my goodness, things change on a daily basis at the moment, it appears. So we've talked about that shared responsibility with cloud providers, software providers, and the company that runs and owns the business. Then we add technology and automation on top of that.

There's so much emphasis on automation, embedded intelligence, and AI-driven tools everywhere across the business—and also when it comes to security. What role does human analysis still play in an always-on monitoring environment?

Michelle: Absolutely important and critical. Breaking news, right? This week we see major advancements and announcements happening across AI.

Richard: And next week there'll be more announcements, and the week after.

Michelle: Of course. Every day, right? You can't go a day without a new announcement.

But AI should be a great accelerator. Humans are in the center. AI can accelerate so much of what a security analyst is doing. And not just security analysts, but many parts of the business where organizations are looking for automation to accelerate outcomes.

When it comes to security, we talk about this huge talent gap. There are so many things happening and not enough skilled security people.

Richard: And more and more threats as well.

Michelle: Exactly. We talk about AI as an accelerator, and it is an accelerator on both sides. It's an accelerator for the good guys trying to protect and defend, and for threat actors using it to maliciously gain access and exploit vulnerabilities in systems.

We're seeing that happen much faster. Humans still need to be at the center. They need to be the people in charge who can take the data that has been accelerated, correlated, and deeply analyzed much faster with AI, and then use that information to make decisions.

It should accelerate informed decisions, but it's definitely going to remain critical. Especially as AI takes what would have been considered lower-priority vulnerabilities and quickly combines them into more toxic combinations that can be exploited much faster.

Just as we're seeing AI driving automation, we're seeing it on the other side as well. That means we need it just as much, if not more, so we can stay ahead of the threat actors.

Oyku: Exactly. Not only the good guys but the bad guys are stepping up their game with AI too. Security teams sometimes face a flood of alerts that can drown out real dangers. How can security teams avoid being overwhelmed by these constant alerts, and how can they distinguish between routine signals and truly dangerous anomalies?

Michelle: It goes a little bit back to the first opening comment that I made around really understanding the business and business resilience. So all your crown jewels, your high-value assets, what you have and where it is, and what you really need to protect—that becomes the prioritization for how you should be tuning, as well as the level of risk and the risk of the vulnerability as you're made aware of it.

So definitely, more is not better. The goal is really around more meaningful insights. When we think about tuning and the tools that need to be in place to make sure that we get rich content, not just a lot of content, we need to reduce the noise. Using tools and using AI to help roll that up and accelerate the contextualization of that data so we can prioritize it.

It always goes back to knowing what you have, making sure that you are appropriately monitoring those systems, and taking that risk-based approach to how you get your notifications and alerts and then how they're triaged on the back end.

Richard: Michelle, I want to quickly go back to the shared responsibility model because I want some advice based on the experience that you've had. What are some of the most common misconceptions organizations have about what the cloud provider is responsible for versus what they must secure themselves? And I know you've touched on this already, but maybe you can elaborate.

Michelle: Yeah, I think one of the biggest misconceptions is, "Oh, we're moving to the cloud," or "We're moving to SaaS," or RISE, or whatever platform you're moving to. The biggest misconception is that security is covered end to end and I don't really need to do anything anymore because it's all covered.

Richard: That's the most dangerous thought possible, I would think.

Michelle: Right? Some of the burden might be reduced from an infrastructure standpoint. It doesn't go away. You have to understand the RACI of who's accountable, who owns what, and then how you're going to get notified when there is an issue or an alert that you need to remediate.

That is one of the biggest misconceptions. We do a lot of workshops and discussions educating our clients on this. This is the shared responsibility, this is what you're accountable for, and this is what your hosting provider is going to do for you.

Then there's a lot of gray space in the middle. The gray space around that shared piece is where our clients sometimes say, "Oh, I was not made aware of that."

Firewalls, identity and access management, the connectedness and integration of tools and platforms, getting the logs, and understanding who's patching what are all questions that come up. Patching at the application level definitely falls within the client's responsibility.

Richard: I would imagine there's prep work in advance once you move to a new platform or cloud environment. It's really down to trust in the process and trust in the partners that you're working with. That takes time as well.

Michelle: It does. And we always recommend— you've probably heard this a lot—but when you're updating your playbooks, make sure you're practicing as well.

When you have an incident, speed is really critical. If you're calling someone who's not accountable and you're wasting critical minutes escalating to the wrong team or following the wrong workflow, that could really be impactful.

I don't want to say practice makes perfect, but practice certainly brings about critical learnings that can help improve your response time overall and streamline decision-making.

Oyku: We plan in a perfect world, but we execute in the real one, right? I can imagine this also often happens in the ERP world. Maybe you can share an example of what happens when there's a breakdown in the shared responsibility model, perhaps a real-world breach or near-miss scenario.

Michelle: Yeah, sure. Most organizations learn through practice and maybe some coordinated pen testing, tabletop exercises, and other operational checks rather than breaches or near misses, because near misses are very disruptive.

There have been times when you won't know what's happening, but what shows up is the user community. The business feels it first. Something's wrong. Maybe some laptops or devices are down, or we can't ship, or orders are stuck. People say, "Hey, something's going on," but they're not thinking we have a security incident.

Again, this could be someone who had privileged access that wasn't revoked in a timely manner or was left unnecessarily open. It could be a phishing incident where a threat actor got in, was able to compromise credentials, and then move throughout the landscape laterally to higher-value assets and wreak havoc.

Getting in and changing delivery or payment terms could be a situation that has happened. What starts out as something that seems simple or just like a blip could really end up being missed revenue or impact production, operations, and uptime.

We've also seen situations where, back to the shared responsibility model, not knowing what you have, where everything is, or the blast radius can cause issues. Knowing what you can shut down and what should shut down is important.

We've seen decisions made in a vacuum where things were unnecessarily shut down and actually caused more problems than if they had stayed up and been properly contained while dealing with threat actors.

Richard: I'm looking ahead to the future now. Things have evolved so much in the last five to ten years. I can only imagine it's going to evolve that much again, or more, over the next five to ten years. How do you see security monitoring evolving over the next five years, with technologies like AI in particular driving the future?

Michelle: Everything is much faster because of AI, but trust will become more measurable.

Security monitoring will be shifting from the back office to continuous verification and assurance. Trust, again, will become measurable because we're going to be reporting more, and we'll have to, because it will be embedded in everything we do.

Advancements in better signal correlation between disparate tools and platforms, tighter integration between identity and access management, incident management, and threat intelligence—and correlating that data—will all happen much faster. That's already happening now.

As threats get faster, responses also need to get faster. The convergence of AI will become more integrated into the end-to-end ecosystem, and governance will also be critical.

Oyku: For organizations that want to strengthen their approach to monitoring and better understand their side of the shared responsibility model, what's the first step you'd recommend?

Michelle: We'll always start with aligning the risk posture to the business strategy. There has to be a give and take. There has to be a balance.

The business is there to create products and generate revenue. It's there for shareholders. So there's a lot that needs to be considered. It's not just security for security's sake. I always say that in the beginning because there can be organizations out there that have shiny-object syndrome and think, "I just need to buy this one tool and it's going to solve all my problems."

But there's more to it. I always say, be brilliant at the basics.

You need to make sure that before you're adding complexity and tools, you know where your critical assets are. Where is the critical data? What do you need to protect? What's the minimum viable business and all of the systems that need to be up and running to support those business processes?

Make sure everyone understands that. Be brilliant at the basics. Make sure you have your core tools for monitoring and alerting so you know what you have to protect. Then make sure you have visibility into it. You can set the right alerts and integrate as much as you can where possible.

When you're really strong on the foundation, some of this can happen in parallel because not everything is perfectly sequential. Then you can start to automate more and use AI.

There's also a lot to consider regarding the human in the middle. We have to have transparency, traceability, and understand what is being presented to us. That's why you have to be brilliant at the basics, so you have that traceability and can trust the decisions being made based on the data you have.

Oyku: And how can EY help?

Michelle: We do everything from strategy, transformation, and operations all the way through. We help in all of these areas, especially with AI and the rise of responsible AI, as well as the tools you're using to accelerate and support business enablement through security.

I say this, and many of my colleagues say it: security isn't back office. It's an enabler.

When we move away from viewing security as a cost-center line item and move toward seeing security as a business enabler, it allows you to move faster. You understand your risks, know things are secured, risks are mitigated, and you can use new tools and technologies with confidence because you've done the work on the back end.

Some organizations get out ahead of themselves. They'll start using all of the tools without having the governance, compliance, and controls in place. We help with that end-to-end.

Richard: Michelle, we're coming to the end of the podcast, and we always ask our guests the same question at the end. I think it's the most difficult question because I'm going to ask you to

summarize the conversation we've had in a few sentences. From a cybersecurity perspective, what's the future of ERP?

Michelle: The future of ERP is really going to be more integrated with the broader security ecosystem and enterprise.

With the rise of AI, the rise of risks, and ERP and SAP continuing to sit at the center of running a business, things will shift and change. Data will also become more dispersed.

I see the future of ERP not being off to the side in an air-gapped facility where only SAP security practitioners are looking at SAP. Instead, it becomes much more integrated with the broader cybersecurity ecosystem of tools, capabilities, and platforms.

That's because it is so critical to running a business. It is one of the high-value assets. Keeping it resilient and secure is going to be absolutely critical.

Richard: Great summary. Thanks very much, Michelle, for a great conversation. I've certainly learned a lot.

Michelle: Thank you. It's great to be here with you both.

Richard: You are welcome. I'm sure you'll be back as well, and thanks everyone for listening. Please mark us as a favorite so you can get regular updates and information about future episodes. Until next time, from Michelle, Oyku, and me, thanks for discussing the future of ERP.