Despite its undeniable importance for most companies' security initiatives, the current approach to governance, risk, and compliance (GRC) is still an essentially manual process. Although a necessity ensuing from the ever-evolving rules regarding privacy, environment, and cybercrime, traditional GRC approaches often miss the mark. It rings truer when risks increase, and the inability to mitigate them comes with terrible consequences. GRC are necessary functions within businesses, but companies’ structure these and employ them differently. For example, in some companies, the GRC works as three separate and decreed functions. While some companies feel “I am compliant,” they must be secure.
Even when GRC works as a combined organization, cybersecurity – another risk function – tends to operate separately. One of the reasons is that the functions of the GRC are considered business or operational functions, while cybersecurity is perceived as an IT function. However, as any cybersecurity episode demonstrates, the scope of risk fallout tends to impact more than one function simultaneously.

"Platformization is a quintessential entity that all businesses should consider right now. Otherwise, they can't own it up to their existing interfaces that deal with GRC if they're using disparate systems. Today's systems need to be fully agnostic of technology framework," says John Ayers, VP MXDR, Optiv. "Our MXDR solution's secret sauce derives from that pedigree: tested processes, proven IP, best-of-breed technology, leveraged automation, and providing top-shelf talent."

The MXDR Magic
MXDR is XDR delivered as a managed service. Designed as an open/hybrid platform (Managed Extended Detection and Response), it integrates and works by Optiv meeting its clients where they are and adapting to their tech stack, offering real-time threat detection, containment, isolation, and incident validation. The provision of supplemental technology and security skills makes MXDR simpler than DIY XDR. MXDR is also always-on and lightning-fast due to automated response and remediation across endpoints. "One can rely on MXDR, especially when we're exposed to so many endpoints around us," John comments.

He reasons, "endpoint detection is as tricky as it gets. Think of us going to a coffee shop, using their internet, and coming back to the home where we leverage the SSL using TLS from a basic modem or router." To compound this, today's devices, such as smart TVs and refrigerators, thrive on immense connectivity and pose as attack vectors for actors. "But with MXDR, now endpoints are spotted out quickly, and the vulnerable ones are isolated for faster resolution." MXDR is a powerful enabler that unites log + data capture that's either not seen by EDR and NDR services (such as Active Directory or VPN logins), as well as allowing correlation and validation from other rich data sources to validate threats.

He exemplifies an automated response – whenever any tickets are logged for any suspected threat or weakness, "we curate the data and glean insights to further bolster the power of our threat intelligence." As the next steps, the MXDR system draws upon its intelligence pool and enrich plus assesses the type of incident. All this involves solutions for our clients to build out a dynamic policy or build out various things to terminate in what we call short-form containment, update a particular session between an effective endpoint. "We go beyond just symptoms treatment; we delve into the root cause. Our customers like to consider our solution as a 'security-first' lifecycle management approach."

What happens behind the scenes
Optiv MXDR ingests data across various layers of technologies to correlate, normalize, enrich and enable automated responses to malicious activity in real-time. By automating incident investigations with actionable insights, organizations can detect threats faster and prioritize which threats to mitigate first, significantly reducing the attack surface.

The product is integrated into an organization's current security technology to gather events, enrich the event data and escalate potential threats. From there, Optiv MXDR can identify the threats that "matter most" to ensure rapid investigation as well as determine the severity, impact, affected assets, and root cause of the attack, properly assessing business risk.

Optiv MXDR leverages Security Orchestration, Automation, and Response (SOAR) to respond quickly, eliminate threats and administer containment actions with runbook development. Security incidents are managed to completion by Optiv MXDR with corresponding after-action reviews, the company says.
No. 1 pain remediator for clients
Cloud services help health insurance providers reduce costs by centralizing patient records and leveraging big data to make more informed decisions. Cloud technology allows employees to access data from anywhere, but it opens the door to malicious actors, and well-meaning employees can also gain unnecessary permissions. Optiv helps insurance providers identify proper security controls and best practices for configuration and implementation of cloud platforms so you can safely migrate to, and utilize, cloud-based resources.

The future shines brighter
Looking ahead, Optiv wants to expand aggressively and remarkably reduce technical complexity that often demotivates businesses from deploying futuristic security solutions. Their next area of focus is user behaviour analysis. John foresees, "there is a bigger challenge coming, and it can be only won at the endpoint. Our learnings of today will help us build a reliable bastion for our clients." Lastly, he emphasizes maintaining the scalability of the solution as the world keeps buzzing with more endpoints.
As cybersecurity and regulatory compliance become the top concerns of corporate boards, some are adding cybersecurity experts specifically to scrutinize security and risk issues. Driven by recent events such as security breaches and the ongoing COVID-19 pandemic, cyber threats are also significantly affecting the regular operation of businesses.

Meanwhile, the cybersecurity mesh is becoming a buzzword among security experts. The cybersecurity mesh is a modern conceptual approach to a security architecture that enables the distributed enterprise to deploy and extend security where it's most needed.

Alongside, the modern hybrid work and the migration to cloud applications have solidified the trend of identity as the perimeter. This way, identity-first security has also become the prime target.

As misused credentials are growing part of the top technique used in breaches, security teams have to consider this change and tackle these changing threats deeply. Though multifactor authentication usage is growing, there are still loose ends.

Amidst the changing threat landscape, cybersecurity teams are being asked to secure countless forms of digital transformation and other new technologies. This requires security options that are strong, agile, and flexible, with the power to help businesses rise above the threats.

To help make your security posture stronger and sharper, GRC Outlook Magazine's team has selected a list of some of the innovators in the threat management landscape. Here is the 'Top 10 Threat Management Solution Providers 2021.'

Optiv is an information security company and security solutions integrator that delivers end-to-end cybersecurity services globally. The company help clients plan, build and run successful cyber security programs across the globe.