accenture Google Cloud

Accenture Managed Extended Detection and Response, powered by Google

In today's world of vulnerable security perimeters, increasing data exchange and fast-paced technology changes, the traditional "prevent and detect" approach is no longer effective. To keep pace, businesses must pivot to faster, more adaptive responses. This includes continuously monitoring and remediating threats to alter behaviors and stop attacks before they happen. This will require deep integration of security into the organizational infrastructure and the ability to be flexible so that security services can be dialed up and down on demand.

Integrated "adaptive" solution

Fortunately, Accenture has enhanced its managed extended detection and response (MxDR) capabilities by creating a new adaptive detection and response offering by teaming up with Google to create a modular solution that continually adapts, accelerates and innovates. This approach drives the prevention, detection, response and remediation of IT and OT threats on an ongoing basis. Businesses can improve cyber resilience, security posture and return on investment, while reducing the total cost of ownership up to 30 percent and gaining predictable costs.

Backed by our breadth of security services, global footprint and industry knowledge, Accenture has built its innovative MxDR service on top of the Google Chronicle Security Operations, integrating the Google stack with Accenture-owned technology accelerators. This includes industry-specific detection and response capabilities and an innovative web portal providing an intuitive user experience. Running on a standardized framework, this flexible model allowsbusinesses to integrate with multiple technology stacks such as Security Incident and Event Management (SIEM), Security Orchestration and Automated Response (SOAR) and EDR/XDR/NDR solutions. Accenture's integration layer enables clients to customize modules, avoiding costly rip-and-replace business models, helping them realize value faster.

Accenture's MxDR services provides a vendor-agnostic approach that allows businesses to control the technologies, tools and cloud providers they prefer. By capitalizing on these existing investments, companies can select the best options for their strategies and environments.

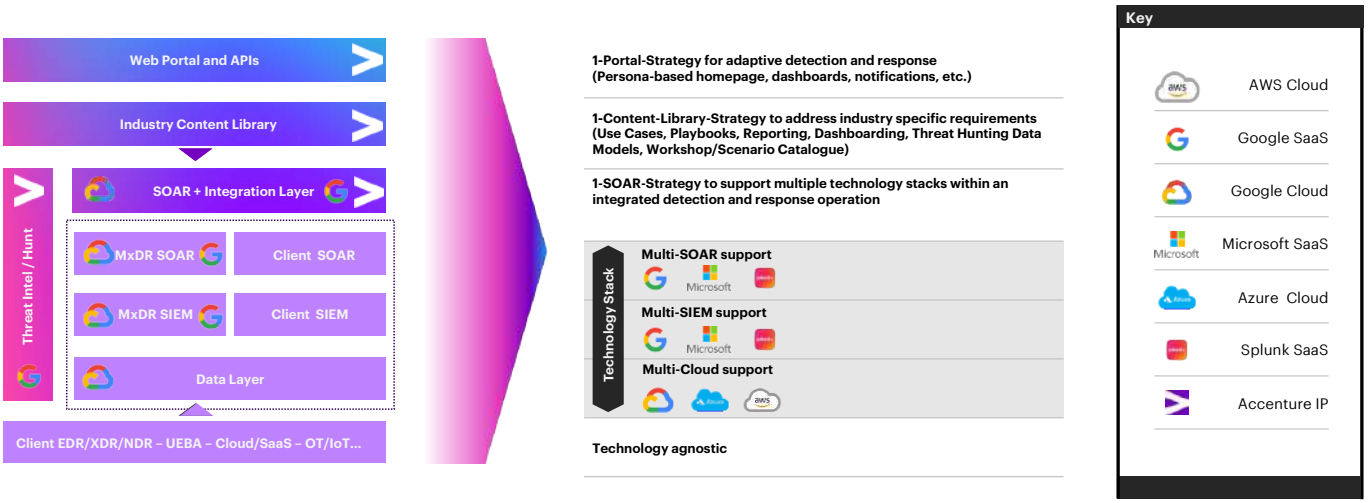
Accenture's MxDR uses two approaches:

Full-stack: An end-to-end offering that combines Accenture's market-leading cybersecurity services and IP with Google Chronicle's multi-tenant, high-speed analytical and response platform. This full stack comes pre-populated with use case detections, playbooks and threat intelligence from Accenture and Mandiant expert analysts, as well as access to a user portal and API suite.

Hybrid: Because of the modular nature of our new adaptive MxDR solution, businesses can select the options that best align with their requirements. For example, a company might decide to maintain its existing SIEM, while using Accenture's detection use case library, threat intelligence and SOAR integration layer, as well as our expert analysts.

Adaptive detection and response

Open to clients' changing needs



A new era for detection and response

Now is the time for businesses to proactively mitigate cyberattacks with Accenture's MxDR services powered by Google. Accenture is the first company to utilize the Google Cloud Security AI Workbench, a new security-specific large language model (LLM) that leverages Google's visibility into the threat landscape and Mandiant's frontline intelligence on vulnerabilities, malware, threat indicators and more. By integrating it within the service, Accenture can significantly accelerate incident detection, analysis and response, mitigating the impact of security incidents.

Together, Accenture and Google can build and manage customized security programs for organizations with complex environments that require more than a turnkey solution. This approach is well suited for global organizations that need to protect large attack surface areas and high volumes of assets. It is also useful for companies needing to comply with local regulations related to data residency and sovereignty, leveraging the flexibility of Accenture's global, regional and national Cyber Fusion Centers.