Datasheet

Extended Detection and Response (XDR)

Intuitive, Comprehensive Security for Efficient Incident Response

Organizations need to protect an ever-increasing attack surface with more devices, identities, applications and data across a growing and heterogeneous infrastructure targeted by sophisticated attack techniques.

Many security solutions rely on multiple additional technologies and third-party integrations to achieve comprehensive threat prevention, detection and response.

Embedded into our industry-leading prevention and detection technologies, XDR delivers consistently top-ranked protection and detection of ransomware and advanced attacks. It unifies and automates threat and risk management across endpoints, identities, network, SaaS productivity applications, cloud workloads, mobile devices, and beyond. XDR enables organizations to reduce their attack surface, remediate incidents faster and improve operational efficiency while alleviating security skills gaps and alert fatigue.

Users benefit from out-of-the-box analytics and advanced heuristics which automatically correlates disparate alerts, enabling quick triage of incidents and rapid attack containment through automated and guided response. The XDR platform detects attacks faster and with more accuracy, exposing the full scope of the attack by connecting events and incidents over time and delivering deeper context and actionable guidance through the Incident Advisor.

↳ **Automatic Incident Consolidation:** Combines observations and events across the business environment into unified incidents, accelerating response and streamlining workflows.

↳ **Advanced Threat Detection:** Leverages built-in machine learning algorithms for accurate threat identification.

↳ **Clear Visual Attack Chain:** Delivers an intuitive, real-time graphical representation of the attack chain facilitating understanding and confident, decisive actions.

↳ **Seamless Threat Response:** Provides guided or automated responses directly within the GravityZone XDR platform.

XDR is a cloud-delivered product for organizations that want to run the technology in-house. Bringing data from endpoints, identities, network, SaaS applications, cloud workloads, mobile devices and more to the platform expands visibility far beyond just managed endpoints. Integrating each XDR sensor can be accomplished in minutes by following the guided steps.

MyCyberIQ
STAY AWARE. STAY SMART. STAY SECURE.™

At-a-Glance

XDR is a cloud delivered solution built to secure the entire business environment. The solution provides detection and response capabilities across an organization's users and systems, including endpoints, identities, network, SaaS applications, cloud workloads, mobile devices and beyond.

With an easy-to-use interface, XDR is designed to intelligently analyze and automatically correlate and triage security events from across the organization, resulting in a key set of benefits to organizations looking to secure complex environments.

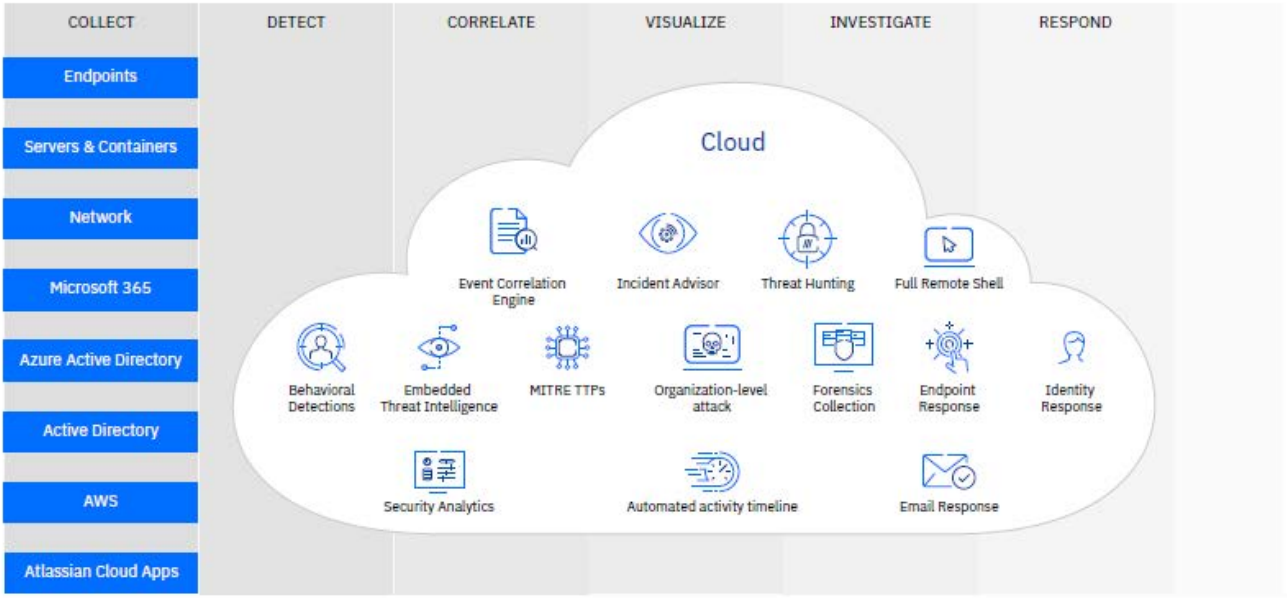
Key Benefits

↳ **Enhanced Efficiency and Cost Saving:** Consolidation of the most comprehensive set of security and risk analytics capabilities boosts security efficiency and reduces costs.

↳ **Rapid Response:** Automated, real-time incident correlation and analysis with human-readable insights enable fast, one-click responses directly from within the XDR platform.

↳ **Value out-of-the-box:** Turnkey deployment of native XDR sensors – no custom rules or integrations needed - empowers teams of any size or experience level, eliminating complexity.

↳ **High Detection Fidelity:** High detection accuracy and minimum noise allows faster attack prevention.



Productivity Applications	Clouds	Identity	Network	Business Applications
Monitor, analyze and respond to Microsoft 365 and Google Workspace events.	Collects and processes information about configuration changes and user activity. Monitor and analyze security events from AWS and Azure.	The sensors collect and process user sign-in activity, configuration changes and other activity. Monitor, analyze and respond to events from AD and Azure AD.	Collects and processes network traffic across the environment. Monitor and analyze network traffic for signs of an attack.	Integrates with Atlassian Cloud applications to monitor and analyze security events from Confluence, Jira, and Bitbucket.

For organizations looking for a managed service, our MDR offers comprehensive support by leveraging XDR and a global team of SOC analysts and threat researchers. The team helps to monitor, detect and respond to cyber threats 24/7.