Quick Guide:

IBM Security

the I.T. insider

IBM Security Solutions

IBM has a powerful family of enterprise security solutions which adopt a zero-trust approach to security: never trust, always verify and assume a breach for maximum security. It's core suite of products includes:

Cloud Pak Security Platform
IBM Cloud Pak for Security is an open security platform that connects to your existing data sources to generate deeper insights and enables you to act faster with automation. Whether your data resides on IBM or third-party tools, on-premises or multiple cloud environments, the platform helps you to find and respond to threats and risks — all while leaving your data where it is. So, you can uncover hidden threats, make more informed risk-based decisions and respond to incidents faster. With IBM's SaaS version of Cloud Pak, you can simplify how your organisation deploys a zero-trust architecture across the enterprise – one that 'never trusts, always verifies and assumes a breach' for maximum security.

Data Security

IBM Guardium
IBM Guardium Data Protection for Databases is a comprehensive data security platform that offers a full range of functions across different environments, from file systems to databases and big data platforms. It probably best fits those enterprises committed to IBM and are familiar with its software and systems, as well as those wishing to add security analytics along with compliance, database protection and encryption within a single product.

Identity and access management

IBM Verify
IBM Security Verify allows IT, security and business leaders to protect their digital users, assets and data in a hybrid multicloud world while enabling technical agility and operational efficiency as a cloud-native solution. Beyond single sign-on (SSO) and multifactor authentications (MFA), Verify is a modernised, modular IDaaS that provides deep AI-powered context for risk-based authentication and adaptive access decisions, guided experiences for developer consumability and comprehensive cloud IAM capabilities, including user management, access recertification campaigns and identity analytics.

SIEM

IBM QRadar
IBM QRadar provides security information and event management (SIEM). It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviours. Delivering threat intelligence to continuously improve detection, it provides real-time visibility of IT infrastructure which can be used by security teams to prioritise threats and respond quickly to reduce the impact of incidents.

SOAR

IBM Cloud Pak
IBM Security SOAR, formerly Resilient is designed to help security teams respond to cyber-threats with confidence, automate with intelligence and collaborate with consistency. It captures and codifies established incident response processes into dynamic playbooks to guide and empower teams with the knowledge to resolve incidents. It helps teams accelerate and orchestrate their response by automating actions with intelligence and integrating with other security tools. It also allows teams to visualise and understand security incidents to prioritise and take action.

Mobile Security

IBM Maas360
IBM Maas360 simplifies the management and security of end point devices: smartphones, tablets, laptops, wearables and IoT. Unified endpoint management (UEM) delivers IT and security leaders the technology needed to manage and secure all devices and endpoints. Using an AI approach to UEM with Watson, organisations can manage all endpoints and everything in between – including apps, content and data.

The IBM security range brings clients excellent performance coupled with a wealth of enterprise features particularly when it comes to their journey to hybrid multicloud environments. The flexibility available enables clients to build an eco-system that is economically targeted to meet their specific needs whilst taking care of their organisation in the face of an increasing threat landscape.