

Investing in next gen security solutions to propel modernization and digital transformation efforts in 2021

Dec 29, 2020



- Sudeep Das, Technical Leader, IBM Security Systems, IBM India/South Asia

2020 witnessed the threat landscape in India changing and evolving quickly, data breaches, ransomware attacks, privacy failures, and other cybersecurity challenges are now on everyone's radar screen more than ever. Yet most businesses still struggled with effectively preparing for them. Challenges that continue to hold companies back include:- complex regulatory requirements, lack of alignment on security strategy as well as cybersecurity and compliance maturity, frequent organizational changes, security skills shortages, uncertainty regarding security "best practices" and lastly insufficient practice of plans for responding to a cybersecurity incident — that is if they have an incident response plan at all.

A recent IBM and Ponemon Institute study highlighted that 41% of the respondents from India review and test their cybersecurity incident response plan (CSIRP) only once each year. This is an alarming fact, specifically in the light of the current pandemic since many organizations had to overnight shift to a Hybrid work environment leading to many unforeseen risks.

Further, as per our 2020 Cost of Data Breach report, Indian companies witnessed an average of ₹140 million total cost of a data breach in 2020, an increase of 9.4% from 2019. Additionally, companies with fully deployed security automation were able to detect and contain a breach 27% faster than those with none. Showcasing the importance of technology preparedness.

We believe the next wave of the tech security landscape will be enhanced by these five trends helping organizations innovate and be prepared for all present and future uncertainties.

5 key Security Tech trends that must be at the heart of every organization's security strategy

Security to drive modernization efforts as new threat actors emerge

Organizations are optimizing and scaling their existing tools leading to more coverage of their infrastructure across on-Prem, operational technology (OT) infrastructure as well as cloud infrastructure and services.



Moving beyond the IT perimeter with Zero Trust Framework

There is a renewed vigour on combining Identity, Data, Network and Devices security into a common analysis platform to better deliver security context and build on an organization's Zero Trust journey.



Adoption of Security from the Cloud

With lack of skilled personnel being a major inhibitor to maximize the efficacy of security investments, we are seeing more and more organizations evaluating Security-as-a-Service.



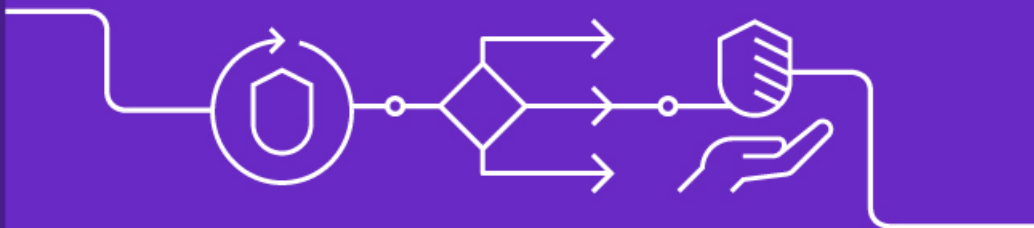
AI/ML-powered security to become ubiquitous

Companies will look to move forward from proof of concepts to large-scale deployment of AI-based security insights and leverage the power of machine learning to monitor risks across all security controls.



Automation and Orchestration will become the core of security strategies

Investments in orchestration and automation technologies can help ensure security incidents are addressed in a systematic and compliant manner.



Source: IBM India | Dec. 2020

Blog Categories

[Secure](#)