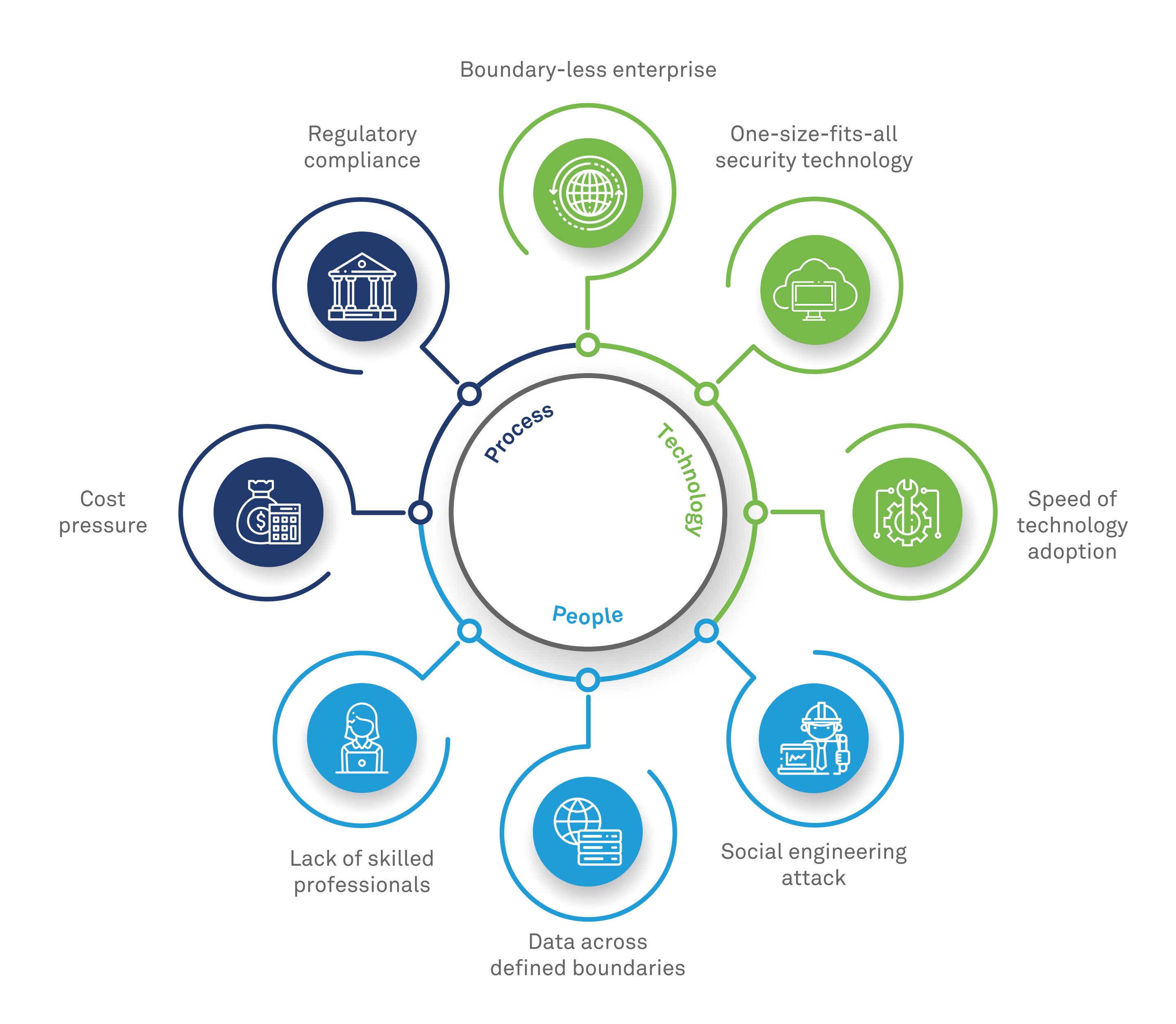
Eliminating the complexity in cybersecurity with Artificial Intelligence

Proliferation of mobility combined with faster internet has increased the scope of connected systems. What was once on-premise applications, with access restricted to corporate-approved devices, are now 'Appified' and 'Cloudified' for anywhere, anytime and any device access. This transformation has reduced the enterprise boundary and moved users, data and device out from within the enterprise perimeter.

The threat landscape, as a result, has changed. Fraudsters have developed sophisticated skills and capabilities, and the lack of cybersecurity professionals-with the requisite skills and knowledge to counteract cyber-attacks-poses a challenge.

Cybersecurity involves multiple issues related to people, process and technology (see figure 1). Cyber defenders are grappling with traditional, commercial off-the-shelf (COTS) security solutions that are built as one-size-fits-all, for all industries and segments. These security solutions heavily rely on predefined signatures for detection and prevention, and totally lack the context for human behavior. Fraudsters have found sophisticated ways to evade signature-based technology and are exploiting humans to gain access to the enterprise.



Boundary-less enterprise
Regulatory compliance
One-size-fits-all security technology
Cost pressure
Process
Technology
People
Speed of technology adoption
Lack of skilled professionals
Social engineering attack
Data across defined boundaries

Figure 1: Challenges faced in cybersecurity

Disruptions in traditional industries, and proliferation of pay-as-you-go models, are leading enterprises to enable 'Change' initiatives in addition to optimizing 'Run' investment. This, combined with the fact that government and regulators have placed priority on data security and privacy, is forcing CISOs to look at the most recent security technologies to develop, implement, continually monitor and report compliance.

Artificial Intelligence: The future of cybersecurity

Cybersecurity is crucial, as any failure affects the entire enterprise ecosystem and its stakeholders. Artificial Intelligence (AI), which is driving a revolution in almost every industry, can be the catalyst in increasing the effectiveness of cybersecurity.

Human intervention is significant in cybersecurity. Benefits of adopting AI are obvious in use cases involving voluminous event reviews and real-time monitoring. AI complements security efforts by providing persistent monitoring, and enabling a contextualized view. It can automate to learn and adapt instantly, and enable synchronous actions across security technologies.

Properly designed and implemented, AI technology can:

- Bridge the gaps in security technology
- Help build next generation security teams
- Introduce security culture into the enterprise
- Handle voluminous and repetitive transactions
- Bring human and environmental context to security
- Enable continuous monitoring and reporting of compliance requirements

Bridging security technology gaps: Enterprises are constantly looking at adopting the latest and more innovative technologies that enable business growth. The fact that these emerging technologies may only have basic inbuilt security features need not be a hindrance to early adoption. AI can provide contextualized security, which augments the built-in security in niche products. Security teams can leverage AI to build adequate monitoring capabilities using the context of the solution deployed.

Multiple real-time monitoring and reporting capabilities can be built using AI algorithms. For instance - AI integrates with the enterprise ecosystem and provides real-time contextualized alerts when data is uploaded to cloud storage, subsequently followed by download, and deletes the action when using a different environment. It can monitor upload/download files to cloud storage and for access by employees.

Build next generation security teams: Producing actionable intelligence from Threat Intelligence (TI) is a subjective and humongous effort for security analysts, due to the volume and variety of intelligence. AI technology can assist their human counterparts by gathering TI, perform initial impact assessment of the intelligence by factoring in the enterprise landscape and then map the intelligence for action. AI plays the first and second responder roles and helps the security analysts with the required information for decision-making.

Instill security culture in the enterprise:
As per the Verizon data breach report[1] 43% of breaches begin with a social engineering attack. The axiom “employees are the weakest link in the security chain” is truer in today’s context than ever before. Enterprises confront this challenge by raising awareness amongst employees via emails, posters and mandatory training. But the effectiveness of any training diminishes with time, if not practiced frequently.

A successfully defended security threat by using the right technology is a point-in-time success for the security team. Fraudsters will target again with enhanced customized attacks to circumvent the controls. This puts employees as the last line of defense to detect the threat.

AI can deliver continuous lessons for enterprise users. It will enable customized cybersecurity learning experiences. focused on user based on their behavior, contextualized to the user, enabling insights into attack type and the focus of the attack.

AI has the inbuilt capability to learn and provide custom training to users.
It sensitizes employees on security through visualizing the security posture of the systems used by employees via scoring;
For instance AI bots connect email security gateways, collate all relevant information of blocked emails belonging to the phishing category, and do pattern recognition.

Handle large and repetitive events:
As anywhere, anytime and any device access increases, the attack surface also grows exponentially. This generates additional security events, forcing the enterprise to deploy additional resources for triaging, analysis, reporting and mitigation. A large volume of events at the Security Operations Center is commodity malware infections.

AI technology can identify the class of malware, and its criticality. Based on the infection observed, AI can intelligently build contextualized remediation steps for the user as self-help. This way a sizable chunk of the manual process is hyper-automated using AI.

Bridge human and operating environment context gap in cybersecurity:
Today's security problem is complex and involves human actions and the surrounding environment (location, device, user privilege and role). A properly designed and deployed AI, can observe, learn and add the required context to the event, providing accurate information for analysis. This will ensure the incident is escalated for further analysis, if the AI added context raises a red flag.

For instance: A laptop loss is reported stolen, the security team and IT are notified - this could be a regular incident in many organizations. AI can contextualize this event with information: does it belong to a senior executive, sales, or an R&D employee? Is the laptop HDD encrypted? Another instance: A large firewall deny event, the security team is notified: a typical analysis will lead to the identification of the end system trying to connect. AI can contextualize the event with malicious traffic, malware infection history, and server sensitivity.

Continuous monitoring and reporting:
Data and privacy regulations have become high priority action areas for management. Enterprises are mandated to define, implement and continuously monitor the effectiveness of the controls, and report compliance to the competent authorities. Companies have dedicated in-house staff or have outsourced compliance management, leading to a significant increase in the cost of security.

AI is an efficient and cost-effective way to achieve compliance. AI can continuously monitor all the deployed controls and alert compliance in case of irregularities. After achieving a mature stage, AI can be trained for auto-remediation, so that the control status is automatically reinstated.

An army of AI bots can provide a unified, layered security for the enterprise - sufficient to counter the capabilities of advanced cyber-attacks and enhance the overall security position of the enterprise.

Reference:

1 - http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

About the author

Sridhar Govardhan
General Manager and Head of Cybersecurity, Wipro Ltd.

Sridhar's core competency, accumulated over 18 years of professional experience, are in the business-critical domain of Cyber Defense, Information Protection and Regulatory Compliance. He spearheads organizational initiatives in building self-defensible networks, cloud security and promoting security conscious behavior in employees.

Sridhar has acquired 11 industry-recognized certifications in the domains of IT, Information Security, Security Framework and Secure Enterprise Architecture (SABSA, CISA, CISM). He holds a bachelor's degree in engineering and M. Tech from BITS Pilani; he has two patents (pending) in Cognitive Security.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**