INGRAM MICRO SECURITY

BUILDING RESILIENCE FOR ENTERPRISE WORKFORCE

at the Time of COVID Crisis

A PART OF: INGRAM MICRO ADVANCED SOLUTIONS IMAGINE NEXT.

BUILDING RESILIENCE FOR ENTERPRISE WORKFORCE AT THE TIME OF COVID CRISIS

Globally, the year 2020 has been a disruptive and transformative period for all of us. As countries all over the world implemented adaptive measures, organisations and members of the public had to reshape themselves to a new normal and accelerate their IT transformations for hybrid workforce environments.

Subsequently, as the world is shifting and recovering from pandemic, we have witnessed and will continue to anticipate the following changes in our daily work life:

- Remote working arrangements and standardisation to impact work practices.
- Increase in multi-stage cyber attacks introduces complexity and sophistication.
- Widespread expansion in cloud migration strategies.
- Rise in demand and use of collaborative tools to ensure business continuity.
- Major shift and embracing agile business model for digital transformation such as increasing e-commerce operations.

The state of remote working could lead to several cybersecurity challenges across all the business verticals.

With the post-pandemic “new normal”, organisations will need to consider and adapt several changes in their business processes, operations, and technologies for a secure environment.

These adjustments may align to reflect the changes in overall operating strategies, building secure enterprise architecture, and swiftly addressing a need for threat detection and response.

Enterprise

THREAT VECTORS FOR HYBRID WORKFORCE

The expansion in the attack vectors during the pandemic have exponentially revealed concrete weaknesses and vulnerabilities in the existing enterprise infrastructure.

The growth in using the same technologies to facilitate remote working environment have brought unprecedented challenges and threatened cybersecurity of the organisations worldwide.

At the edge of digital transformation, employees who work from home, IT Support and Security Teams have been forced to adapt within immature security establishment that lacks basic hygiene to secure the hybrid workforce. In order to address these concerns, it would be wise to lift the right level of resilience by preparing the organisation against the major threats known in between 2020 and 2021.

- Targeted phishing attacks causing losses due to lack of employee security awareness.
- Use of insecure remote work settings (home) to connect to seamless work environment.
- Increased in complex and multifaceted threats (ransomware, data breach, insider).
- Lack of professional expertise and core skillset in cybersecurity.

CURRENT STATISTICS OF ATTACKS

ATTACK STATISTICS

27% of COVID-19 cyberattacks targeted banks or healthcare organizations, and pandemic situation is credited for a 238% rise in cyberattacks on banks in 2020 (*Fintech News*)

Remote workforce has caused a security breach in 20% of the organizations (*Malwarebytes*)

30% of data breaches involve internal actors, confirmed data breaches in the healthcare industry increased by 58% in 2020 (*Verizon*)

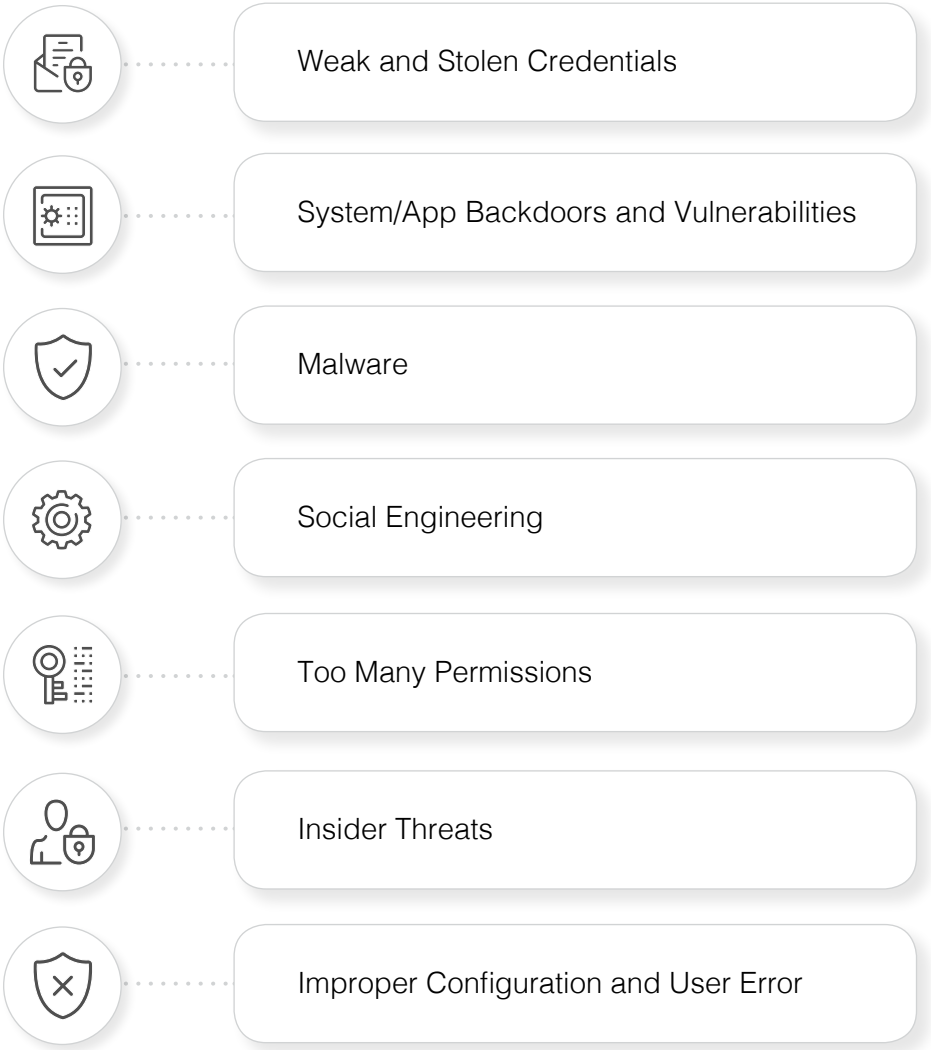
Ransomware attacks cost businesses an estimated $20 billion in 2020, having grown by over 50 times since 2015 (*Cybersecurity Ventures*)

80% of breaches contained customer PII (*Capita*)

More than 77% of organizations do not have an incident response plan (*Cyberint*)

68% of business leaders feel their cybersecurity risks are increasing (*Accenture*)

TOP 7 MOST COMMON CAUSES OF DATA BREACH (CYBER OBSERVER)



SOURCES

https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/

https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf

https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

https://cybersecurityventures.com/annual-cybercrime-report-2020/

https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

https://www.cybintsolutions.com/cyber-security-facts-stats/

https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/

CYBERSECURITY CHALLENGES & THREAT ACTORS OPPORTUNITIES SINCE COVID-19

KEY CHALLENGES IN MANAGING HYBRID WORKFORCE

Accessing Workspace (BYOD & Insecure Connectivity):

- With default work-from-home settings, employees are increasingly utilizing personal devices to access corporate network and cloud services instead of corporate devices
- Frequently connecting to insecure Wi-Fi network to initiate their daily work
- Constant use of third-party collaboration, teleconferencing, productivity, and file sharing tools has also introduced multifaceted threats

Assets Hygiene and Visibility:

- Misaligned and non-pragmatic approach for the remote monitoring of corporate vs. personal devices to maintain assets inventory and tracking
- Raising concerns over data movement (i.e., data-at-rest, data-in-transit, and data-in-use) across corporate and personal devices
- Lack of enforcement over remote access policy dictating “minimum” controls to be in place for utilizing personal devices for work (i.e., AV, Secure VPN, Patched, Secure Configuration)
- Corporate devices are not consistently connected which would impact the software applications, OS, and other security control updates
- Personal devices are prone to various system-related vulnerabilities

Work from Anywhere:

- Insurgence of home-based IoT devices or appliances appeal promising connectivity but exponentially increases the attack vectors
- In a default work-from-home setting, other family members in the house may also access the corporate device for personal use (i.e., shopping, banking)
- Employees connecting from multiple locations making conditional access policies complicated
- Shared apartment or roommates may impose several security concerns, such as, eavesdropping business conversations, shoulder surfing to gain work insights or competitive intelligence, etc.

Insider Threat (Remote Access Context):

- Ineffective or non-existence of insider threat monitoring programme and strategy
- Continuous access reviews for privileged users or administrators for high-value infrastructure targets
- Current economic climate causing employees to leave the organization, and thus raises significant concerns on corporate data or materials being maliciously or accidentally taken away from the enterprise systems

PROPOSED CYBERSECURITY SOLUTIONS

As we progress through the pandemic, a wide range of cybersecurity issues have brought up attention towards the need for robust and resilient enterprise environment. This has raised a concern for a lean, secure, and sustainable business approach in a cyberspace which could possibly be addressed by formalizing the key security processes and technologies, and their specifications as suitable to execute and operate the business.

A holistic view with several key elements has been drawn as given below which would help to focus on deriving an optimally secure workforce across various enterprises.

IDENTIFY

Adequate Secure Remote Access Policy and Enforcement

- Understand the spectrum of risks associated with remote working and hybrid environment
- Build and provision security best practices and procedures around remote working element
- Provide coverage for all types of remote workforce, including staff traveling overseas, home-based, contractors/third-party operating and accessing systems remotely
- Formal acceptance and adherence to the policy

IDENTIFY, PROTECT

Establish and Enforce BYOD Policy and provide adequate training

- Formalize the policy and provide clear dictation for the staff to adapt and follow strict security measures for using personal devices for work
- Alignment of security controls to allow staff accessing sensitive data from non-work sanctioned devices (i.e., MDM)

PROTECT

Deploy Advance Malware Protection Solution

- Deploy and enable next-generation AVs on users' workstations and servers to monitor active threats
- Able to counter malware through initial footprints, deep insights, context, behavioural patterns, and dynamic signatures

PROTECT

Enablement of Secure Remote Access VPN

- Deployment of secure VPN gateway solution that connects users to specific enterprise apps and services remotely
- Enforce access policies based on identity and context, and provide more fine-grained access for different groups of users (i.e., department specific, geo-location specific)

PROTECT

Establish Zero Trust Architecture (People, Devices, Network, Workloads)

- Solution to streamline trust-level assurance through overall identity management, conditional access policies, network hygiene, baselining users' access, and micro-segmentation across network boundaries
- Augmentation towards users' devices, workloads, application access (internal or third-party business apps), and network access (remote enterprise systems or third-party channels like cloud services)

PROTECT

Use of Secure Collaboration and Productivity Tools

- Enrolment of staff to utilize collaboration and communication platforms to provide business continuity in the remote work setting
- Easy to access using SSO or 2FA, provide multifaceted communication channels, facilitate secure file-sharing, and ensure the optimal security requirements

PROTECT, DETECT

Deploy Data Access Monitoring and Data Loss Prevention Solution

- Monitor the data-at-rest to determine any malicious activities performed by the perpetrator using DAM solution
- Establish a clear directive to identify the key data channels across the organization, prioritize, map, and monitor data-in-transit using DLP solution

PROTECT, DETECT

Deploy Identity Access Management (IAM) Solution

- Implement and refine appropriate identity solution (PIM/PAM with SSO/2FA) to enforce organization wide user access to enterprise assets (i.e., authentication, authorization, user accounts management, access management, governance, and reporting)
- Conduct regular access audits to improve and comply with regulatory compliance

PROTECT, DETECT

Establish Insider Threat Monitoring Programme

- Design adaptive access control to monitor and identify the norms across the organization's userbase
- Employ deception tools and techniques to determine the risk arising from behavioural activities tied to anomalous deviations from regular baseline

DETECT

Continuous Vulnerability Management Program

- Gather organization wide visibility across all assets and their status on individual vulnerabilities tied to a system, application, or network service
- Devise appropriate workflows for continuous assessment and remediation to close the patching cycle

DETECT

Threat Intelligence

- Prepare the TI platform to align the strategic, operational, and tactical matrix across the organisation to determine unknown threats using atomic TTPs and behavioural threat indicators (i.e. darkweb intel, hacker forums, publicly disclosed information, advisories, news/articles)
- Detect and counter any prevalent threats in the operational environment known via indicators of compromise (IOCs) to leverage and prioritise the response and recovery efforts

DETECT, RESPONSE

Enable Events Logging and Monitoring through SIEM Solution

- Configure, fine-tune, and triage alerts aggregated through various events on the systems or devices across the network to counter any threat activity
- Analyse the incident to determine the path and procedures for the incident response workflow response and recovery efforts

RESPOND, RECOVER

Deploy EDR Solution for comprehensive Incident Response and Forensics

- Provide continuous real-time monitoring, detection, and response against latest threats
- Prevent data breaches by identifying the early indicators of compromise through TTPs
- Proactively hunt for threats within the organization's environment for both on-prem and remote users
- Accelerate response to the incidents to minimize the impact

With broad and deep cybersecurity expertise in-house, Ingram Micro offers consulting and services to develop next-gen cybersecurity solutions to protect your businesses and assets, from start to end. Together with our strong representation of best-in-class vendors and solutions, we are able to tailor solutions to suit your business needs and environments.

TECHNOLOGY EXPERIENCE CENTER AND USE CASES FOR MANAGING SECURE WORKFORCE

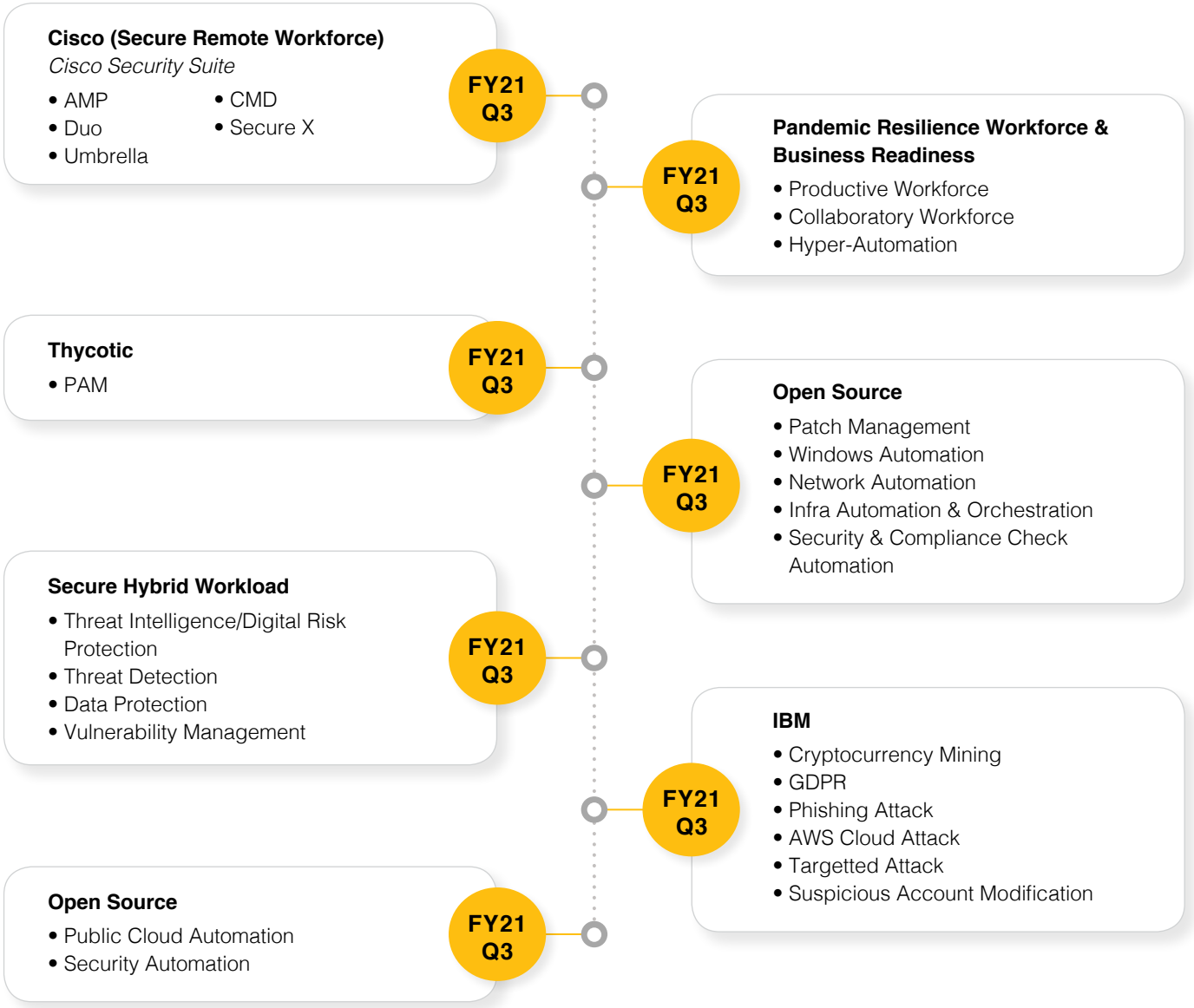
04

Introduction to TEC

At Ingram Micro's Technology Experience Center (TEC) for APAC, we showcase an integrated end-to-end matrix of Enterprise Infrastructure, On Prem, Cloud, RPA, Collaboration, Cybersecurity to IOT, that ensures our commitment to:

- Showcase a seamless integration and collaboration of world class cybersecurity solutions
- Propose solutions and conduct proof-of-concept and proof-of-value demonstrations for common to complex business use cases
- Accelerate your business success by empowering employees with secure access to the critical applications and resources they need in the cloud or on-premises
- Promotes industry collaboration and sharing of resources amongst vendors and channel partners
- Allows vendors to integrate and showcase solutions
- Ability to develop business use cases to support selling
- Provides a better value-added demonstration and proof-of-value platform to channel partners and end users

TECHNOLOGY EXPERIENCE CENTER SHOWCASE



The Technology Experience Center Showcase Road Map is subject to changes at the discretion of Ingram Micro.

More to come on SASE, Secure Remote Workforce, Cloud Security, Datacenter Modernization, Multi-Cloud Management, Open Source, Robotic Process Automation (RPA), etc! Stay tuned.

HIGHLIGHTS OF THE SECURE WORKFORCE SHOWCASE AT TECHNOLOGY EXPERIENCE CENTER (APAC)

Find out more about how we can help you build a Secure Workforce through our Technology Experience Center!

Key Highlights of the Secure Workforce Showcase:

Threat Management – How much do hackers know about your business?

- Is your organization the topic of discussion in cybercriminals chatter, darkweb or underground marketplaces?
- Learn how threat actors gather information about your organization's assets simply from the public domains.

Vulnerability Management – Does your vulnerability management programme need to be 'patched'?

- Are you adopting a risk-based approach in managing your vulnerability?
- Are you optimizing your vulnerability management solutions to manage your security posture?

Endpoint Protection – With an increase in remote working and BYOD, securing endpoints become more important than ever.

- We discuss how successful breaches exploit the slow detection and response to endpoint related threats.
- We can show you how you can effectively protect your endpoints and uncover indicators-of-compromise (IOC).

Data Protection – Who else is keeping your data?

- We discuss common issues on regulatory compliance and data leakage.
- Understand how you can deploy enhanced solution to effectively protect and monitor your information assets.

Security Monitoring – How do you 'stitch' the solutions together?

- We share some of the common use cases adopted within your industry.
- We can show you how different security solutions can be integrated to meet your business needs.

INGRAM MICRO®
SECURITY
Cybersecurity for Asia Pacific

Realize the Promise of Technology™

Let's be in touch

cybersecurityAPAC@ingrammicro.com