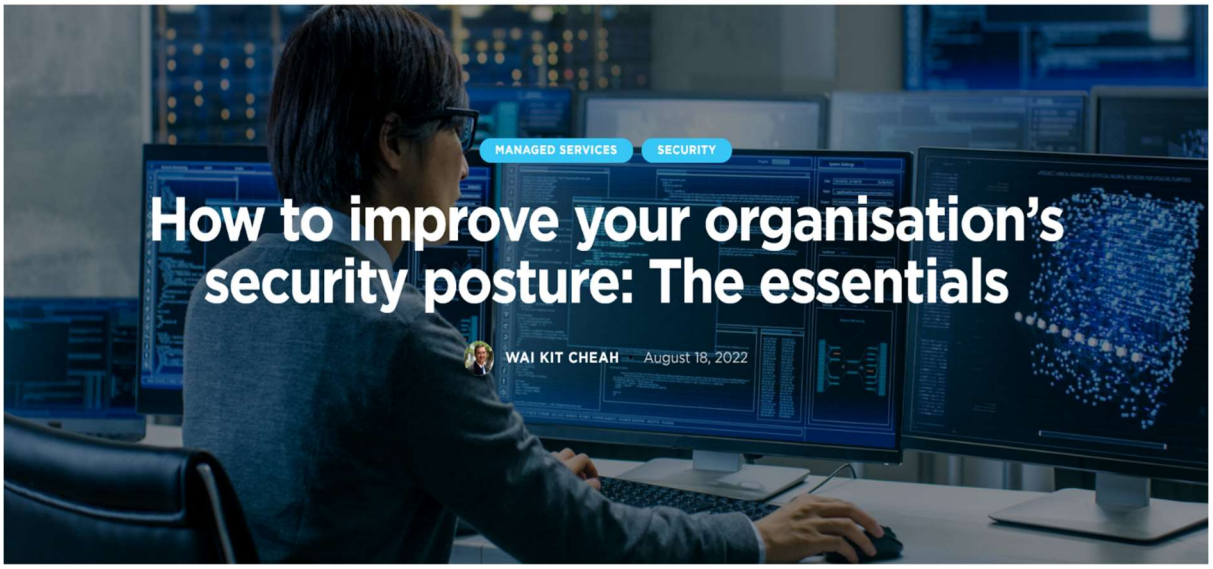


With the rapid pace of digitalisation and distributed workforce, many companies in Asia Pacific struggle to level up their security posture with evolving ransomware and malware threats.

Moreover, when there is inadequate cyber awareness amongst employees, the danger of being compromised is a lot higher. This is concerning as Asia Pacific was the most targeted region for cybersecurity attacks in 2021.

Hybrid work and hacker ingenuity increasing threats to cybersecurity

Advanced Persistent Threats (APT) such as zero-day exploits, fileless malware, and ransomware are always evolving in nature and scope to penetrate devices and networks at any time, making it essential to re-consider your detection and response controls.

Anti-virus software alone is no longer adequate to guard against these threats. Organisations should consider Endpoint Detection & Response (EDR) solutions which leverage on machine learning and behavioural analytics, not just signature-based, to detect for malicious threats.

Yet another challenge is that hackers are now clever enough to evade the traditional defences that organisations set up to prevent ransomware and malware attacks. After hacking into your network, attackers can penetrate backup systems and corrupt the data in them, or just encrypt the data along with your organisation's IT infrastructure backbone.

It is essential to build a better, dynamic security posture that proactively identifies and stops sophisticated malware and ransomware threats even as they evolve. That's how you can *See More, Stop More.*

Cybercriminals are resourceful and dangerous enough to compromise even those companies with the highest levels of security, including accounts with multi-factor authentication controls. Cybersecurity risks and weak spots are always lying around in your network, infrastructure, and even in locations beyond the observation of your security systems and processes. Your organisation is as strong as your weakest link.

How do you evaluate your security posture?

In order to improve your organisation's security posture, it is necessary to assess and examine your internal and external security controls. Prior to doing so, the first step is to identify the assets your organisation own, especially the ones you will need to protect. Without asset visibility, or understanding of your infrastructure ecosystem, it is impossible to understand which vulnerabilities and threats are relevant to your organisation.

Answering these five key questions will help you determine the security posture of your organisation:

1. Do you understand how you collect, process, store and manage critical data in your organisation?
2. How robust and up to date is your organisation's cybersecurity strategy?
3. Do you have the systems and processes to accurately assess vulnerabilities on your organisation's IT infrastructure, network, and devices to evolving threats?
4. Are your security controls documented, established and strong enough for the posture you require based on your organisation's risk appetite?
5. Do you train your employees on cyber awareness and are you prepared with an Incident Response Plan?

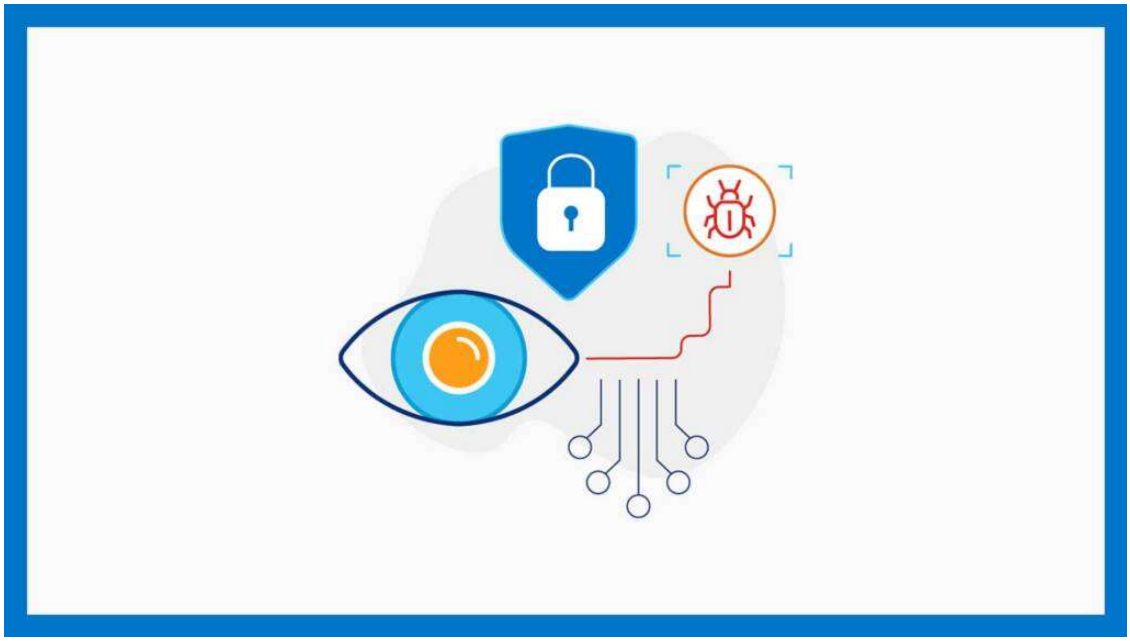
Better security posture is all about seeing and seeing more threats

Achieving the kind of security posture needed to effectively counter evolving cyber threats means organisations must constantly conduct thorough security risk assessments to identify all possible vulnerabilities.

Of course, these vulnerabilities include those beyond the perimeter of the network. In other words, you need to be able 'see' more of your organisation's network, devices, and external cloud services, to improve your organisation's security posture. However, from what we're

seeing, this is beyond the capabilities of traditional cybersecurity systems and processes deployed in many organisations in Asia Pacific.

Accurately identifying and assessing the IT inventory and comprehensively mapping the attack surface are key to start building a better security posture and thwarting evolving threats. Along with it, measuring and quantifying cyber risks in the context of your business environment is very important to improving security posture. This is where Lumen can help you.



Map security posture to organisation's business objectives

As organisations go through their digital transformation journey, cybersecurity function needs to be perceived as a business enabler. By aligning your cybersecurity strategy with your business objectives and applying the right level of cybersecurity controls, it enables your business towards regulatory compliance, business resiliency, maintaining brand reputation and market trust.

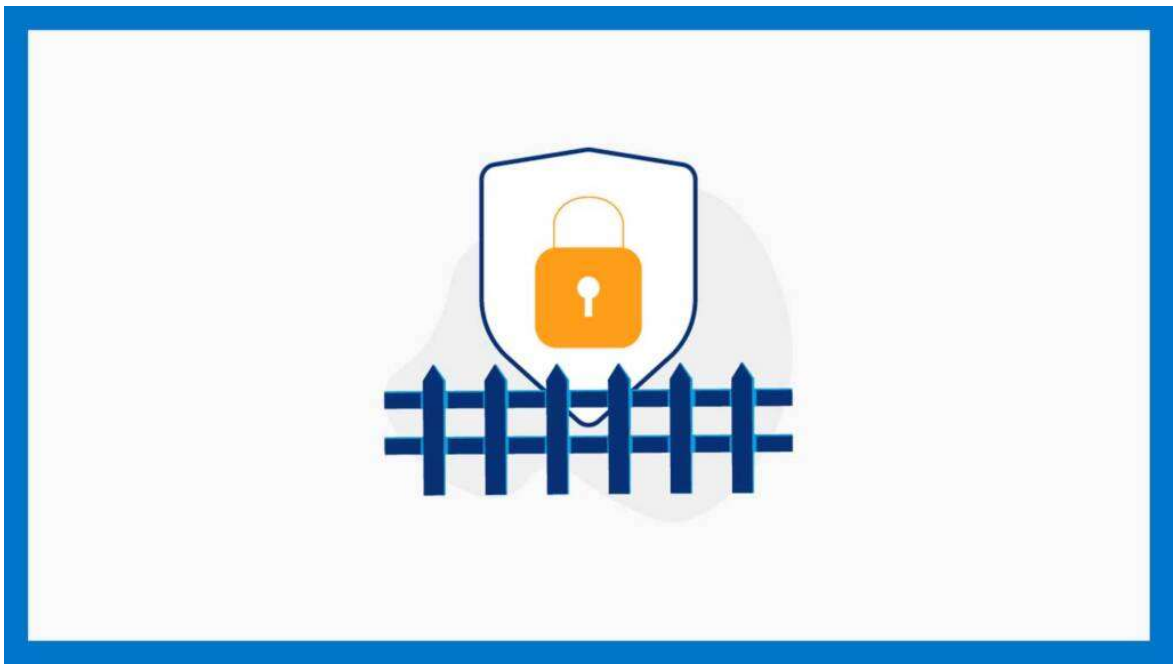
In order to achieve this alignment, it is necessary to have a champion with the cybersecurity experience, technical foundation, strong business acumen and excellent communications at C-level or Board level. Unfortunately, such talents are scarce. Organisations who cannot afford a full-time internal champion or CISO could leverage on a *CISO-as-a-Service* instead.

To mitigate risks, we apply the appropriate controls or risk treatment. Very often, the decision on what level of risk treatment to apply is based on an organisation's willingness to accept a loss, or in other words, its risk appetite. Typically, the cost to protect an asset should not exceed the projected loss of the asset. Therefore, it is crucial to identify your organisation's "crown jewels", their value and understand what does it take to protect them.

In fact, at Lumen, we often find ourselves helping organisations, both large and small, to develop the strategy in a manner that enables them to optimise their security investments and protect the "crown jewels" using a top-down, risk-based approach.

Use a layered defence to strengthen security posture

To help you establish a better security posture , Lumen® Connected Security provides a layered defence by preventing ransomware, malware attacks, and other APTs. Our solutions enable your organisation to defuse, disarm, and ensure the real-time remediation of cyber threats. In addition, our 24/7 SOC proactively creates policy-based rules using advanced threat intelligence feeds and behavioural analytics engines.



At Lumen, we leverage on automation capabilities to enrich, triage, remediate cyber threats and quickly restore impacted endpoints to pre-infection state. Automating cybersecurity enables us to respond quicker, alleviate risks, eliminate or reduce errors and *stop more* threats.

As mentioned earlier, insider threats are equally important, if not, more than external threats. Common cybersecurity tools and processes can fail if users do not follow safe behaviours and learn to distinguish between malicious and legitimate activities. Most breaches and data-loss incidents can be traced to a failure to understand how risk changes over time – morphed or evolved.

Hackers can exploit unseen vulnerabilities in your network and devices at any time. It is essential to understand your organisation's attack surface, vulnerabilities, risks and build a robust security posture now to ensure business continuity and growth.

Want to learn more about how Lumen can help your organisation assess and develop a better security posture? Contact us for a consultation today!

We See More, so we can Stop More

Our experts are here to help!

Contact Us