5G Security Innovation with Cisco
思科的5G網絡安全創新

Cisco Systems (HK) Limited
思科系統（香港）有限公司

5G touches almost every aspect of the way we live our lives. It is not just about faster, bigger or better, it is about utilizing 5G as an enabler to a series of services that we all will consume in every aspect of our lives. 5G will increase in wireless capacity by 1,000 times and connect 7 billion people and 7 trillion "things", estimates a joint initiative between EU Commission and European ICT. The Winter Olympics in South Korea in February 2018 have made a major 5G trial - cameras attached to bobsleds are streaming live video showing the navigator's view racing down the course. This 5G technology is due to be rolled out by South Korean wireless carriers next year. In Canada, the US and elsewhere, mobile carriers are running tests and investing in new radio equipment and cell sites.

As we move into the 5G era, we are also seeing attacks that are more sophisticated. In the world of 5G, traditional siloed security and add-on edge appliances have limitations, are complicated and costly. Security today does not interoperate enough with the network and there will be gaps if we follow the same approach with 5G. Now is the time to consider the security implications and cyber risk profile that come with 5G.

5G Security Architecture: Visibility and Control

The 5G's evolving architectural nature and an expanding threat surface call for an integrated end-to-end approach to cybersecurity. Service provider needs security innovations based on visibility and control for the entire 5G network, up to all applications, to ensure a secure delivery of new cases with service assurance.

Visibility refers to the ability to see and correlate information from the carrier cloud to baseline proper behavior and then to measure deviation from that norm. Sources of visibility come from traditional network measurements (netflow, open flow, etc.), but the need to measure all aspects of a flow, from all elements of the carrier cloud to the application to the end customer, has changed what data is collected and where we get it. An example of the new visibility includes the use of application level probes that are synthetically generated and travel through the network to get a clear picture of how an application is behaving. Another example is where the Path Computation Element, which has a near real time database representing the network topology, is queried programmatically to determine the impact of a potential mitigation action on critical service classes for DDoS. Once all of the telemetry is gathered, a security controller and workflow will analyze it and determine, based on policy, suggested mitigation and controls to be applied. In Cisco, we have an iterative loop

5G網絡正影響著我們生活不同層面：它不但有著更快的速度、更高的效能或更好的服務，還能創造新的服務，為我們的生活帶來更多前所未有的便利。由歐洲聯盟委員會及歐洲資訊及通訊業共同研究估計，5G將會令無線網絡容量增加1,000倍，能連接70億人口及7兆件「物件」。2018年二月在南韓舉行的冬季奧運會試行了一項5G應用，在有舵雪橇上安裝攝影機，就可以把車手於比賽時的視野畫面串流直播出來。南韓的無線網絡供應商預計明年會推行5G技術。加拿大、美國及全球多個地方的流動網絡供應商也正在試行及投資在新的無線電儀器及基站。

正當我們邁向5G的年代，我們同時見到更多更複雜的攻擊。在5G的環境中，傳統單點式安全系統及在網絡邊沿附設的安全應用存在限制，而且既複雜又成本昂貴。若果網絡和安全系統之間並不相容，勉強利用它來運行5G只會製造更多漏洞。現在，我們必須全面檢視5G會帶來的安全問題及風險。

5G安全架構: 可視性及可控性

不斷演進的5G架構特性及不斷擴展的攻擊面，要求一個整合而全面的網絡安全策略。服務供應商必須在整個5G網絡以至所有應用上增加「可視性」和「可控性」，以確保服務交付的安全性。

「可視性」是指掌握供應商雲端裡的資訊、比對與正常情況的差異程度，並提供有用訊息的能力。傳統網絡流量監測，例如Netflow、Open Flow等，是可提供一定程度的可視性；但複雜的5G網絡環境：由供應商雲端到應用到終端客戶，能產生不同流量的起源，亦可從不同角度分析流量等，均影響了資訊的來源及收集方式。例如，在應用裡放置人工深測器，讓它在應用中流動，就能顯示應用實際表現。又例如，為了找出DDoS攻擊會為重要級別的服務帶來甚麼樣的潛在影響，可以利用Path Computation Element（路徑運算元素），它是一個運算程式，能夠提供網絡拓撲（Network Topology）近乎即時的數據。當收集所有遙測數據後，網絡安全工具或程序會分析這些數據，然後根據政策判斷相應的防護及控制行動。思科亦採用了一個不斷學習的循環系統：思科Talos全球威脅研究團隊讓我們的客戶能夠第一時間知悉最新的威脅情報，他們的思科產品也能立即全面獲得保護。這樣可減省服務供應商的壓力，讓他們可專注在其他更重要的服務上。

of constant learning. The Cisco Talos research team keeps our customers ahead of the game by its threat research and deployment of mitigation rules into our full portfolio of products, removing that burden from the Service Provider allowing them to focus on their core competencies.

Control refers to the actions taken to mitigate an attack. Some controls are taken proactively while others are applied after an attack takes place. There are two types of attacks. Day zero attacks are threats that we don't previously have a fingerprint for. Typically they are deviations in known good behavior of the carrier cloud and applications that request service and state from it, are identified by the security controller and some action is then taken to mitigate the attack or to get additional visibility, an action sometimes taken to properly identify the adversary. Day one attacks are threats that we have a signature or fingerprint for and, quite often, a mitigation strategy exist in advance to handle the attack. Controls take the form of modifications to the carrier cloud to apply quality of service changes in per hop behavior to minimize the impact of an attack, or take the form of physical and virtual security assets applied as close to the source of the threat as possible in order to minimize collateral damage.

5G Security Innovation: AI and Deep Learning

Innovation in the way that we apply the information we have, in a close loop iterative process, is a recent innovation in threat visibility and mitigation. This is where automation, orchestration and NFV meets security to solve today and tomorrow's security needs. The three elements of the closed loop iterative process are policy, analytics, and the application delivery cloud (the whole transaction from the application to the networks used to serve it). Operators can now apply innovative methods to correlate geo-location information to behavioral analytics, compare those against policy in the context of a threat to the carrier cloud, and ascertain the nature of that threat and actions about it with far greater clarity. Visibility and control properly applied to the advanced threats of today offer the carrier cloud a level of protection. We must continue to evolve, grow and get smarter to keep our networks safe and resilient in the time of attack.

Cisco's 5G security architecture combines artificial intelligence (AI) and deep learning to create a network that will orchestrate both physical and virtual resources with equal proficiency resulting in optimal network efficiencies. Network and context information is automated with shared telemetry and cloud processing to lower the time to detect and respond. With this unique approach, Cisco has successfully lowered the time to detection from the industry average of 100 to 200 days to as low as four hours.

In the end, security is about finding threats faster, fixing them faster and learning all of the time. The benefits of a 5G security architecture include better optimization and new economic opportunities for mobile service providers and their customers. In fact, Cisco is committed to building a secure network not only for 5G, but also all other networks across different sectors and purpose, because we believe that security is foundational to every business in the digitization era.

「可控性」則指減低攻擊的能力，可以是主動防禦攻擊，亦可以是攻擊發生後的應對。攻擊可分為兩種，一種是「零時差攻擊（Zero Day Attack）」，即是還沒有修補方法的攻擊。通常它們會令供應商雲端及應用出異常狀況，網絡監控工具就能夠偵測到，然後產生相應行動或觸發它去取得更多相關資訊，有時候甚至會採取更積極的行動把該威脅鑒辦出來。至於Day One Attack則指其修補方法已經被公開，應對方法就是依循修補方法在供應商雲端上作出變更，在網絡流量中的封包排程行為（per-hop behavior）中實行服務質量改變以把攻擊的影響減至最低，或是在最接近威脅源頭的地方執行實體或虛擬的網絡安全措施，以避免周邊架構遭受影響。

5G網絡安全創新: 人工智能及深度學習

透過愈來愈多可掌握的資訊，並把資訊回饋到程序裡以產生不斷演進的循環，這些技術均把「可視性」及「可控性」大大提高。自動化、運算編配（orchestration）和網絡功能處擬化（NFV）等技術現已配合網絡　安全來滿足今天和未來的需求。政策、分析，以及應用交付雲端（Application Delivery Cloud）三個元素，形成了一個密封的演進循環。營運商現可透過創新方法，把地理位置資訊串連到行為分析，然後對比威脅在供應商雲端環境下的政策，大大提升判斷該威脅性質及相應方法的準確度。「可視性」和「可控性」能應對於今天所見到進階威脅，向供應商雲端提供高度的防護能力。當然，我們必須持續地革新、演進及更有效地保護網絡，萬一受到攻擊都能夠第一時間復元。

另外，思科的5G網絡安全架構結合人工智能及深度學習，能夠有效地編配實體或虛擬資源，以達致最佳網絡效能。網絡和情境資訊能自動與遙測數據結合並在雲端時已被處理，大大減低偵測和應對攻擊的時間。透過這個獨特的方法，對比起業界的平均威脅偵測時間（time-to-detection）100至200天，思科已能夠將其縮短至4小時。

網絡安全就是快速地找到威脅、修補和不斷學習。對於5G流動服務供應商來說，出色的安全系統能讓他們向客戶提供更優化服務，甚至創造新的契機。其實，不只是5G網絡必須建構安全的網絡，思科亦致力把以上的網絡安全策略及技術應用到不同產業及用途，因為在這個數碼化時代，網絡安全是任何業務發展的重要基石。