The Real Answer to Cybercrime Prevention
如何有效預防網絡犯罪

CITIC Telecom International CPC Limited
中信國際電訊（信息技術）有限公司

Major Menace to the Modern Enterprise

Organizations today have learned to increasingly leverage the benefits of modern business ICT tools to enhance productivity, reduce cost, and accelerate workflow. While this Digital Transformation can bring great advantages, it also brings greater risk. High rates of utilization of digital applications and data open up organizations to the menace of a wide and growing range of sophisticated threats and attacks. Ironically, even as the modern enterprise operates with more efficiency in the cyber world, this technological environment is potentially riskier than ever. Indeed, just one successful hacker attack may render a company inoperative, with the further possibility of long-term financial and operational damage.

The only approach to this modern problem is to adopt a proactive stance against digital threats. In this escalating war between attackers and defenders, it is important to maintain the edge in this "cyber arms race".

The situation is actually quite analogous to biological evolution. As viruses and other pathogens mutate, organisms evolve their immune systems to defend against these new threats. Therefore, we can look to nature for ideas on how to devise realistic and practical ways to keep updated with state-of-the-art protective measures that not only neutralize existing sophisticated threats, but can also maximize protection against emerging, unknown threats.

A Scientific Approach

To defend against the attacks, one must understand not only the attackers' strategy, but also their weapons. IT security experts leverage a sandboxing approach to discover the true nature of zero day malware before it enters into a customer's environment. The "sandbox" simulates a normal IT environment, but isolates the potentially malicious software in a specially quarantined space, to monitor the software's behavior. Then, security experts observe what happens when the unknown software runs, and behavior patterns can be analyzed. The sandboxing technology can help to find out the malware carriers and how malware is executed on an infected system, as well as how hackers clean up their trail.

CITIC Telecom CPC's TrustCSI™ ATP (Advanced Threat Protection) security solution has been created in precisely this manner, to utilize the analogy of laboratory research to equip digital infrastructure with state-of-the-art protective measures that not

現今企業面臨的主要威脅

隨着資訊科技日益發達，企業紛紛開始將資訊及通訊科技（ICT）工具應用至商業層面，以提高生產力、降低成本及加快工作流程。雖然這種「數碼轉型」可為企業帶來巨大優勢，但也伴隨更大風險。當數碼應用程式和大數據的使用率愈來愈高，企業也隨之面臨更廣泛、複雜及具攻擊性的資訊安全威脅。事實上，黑客只需成功攻擊企業系統一次，便能令公司無法運作，甚至造成長遠的財務和營運上的損失。

要破解這一困局，就是要主動出擊，積極應對數碼科技帶來的威脅。在這場不斷升級的「網絡軍備競賽」中保持優勢。

資訊安全威脅的情況其實與生物進化非常類似。隨着病毒和其他病原體發生變異，生物的免疫系統會強化來抵禦各種新病毒。我們不妨效法大自然，尋找實用和可行的設計靈感，令防護措施可以持續更新、強化，達到盡善盡美。這些措施不僅能抵擋現有複雜的威脅，還能防範各類未知攻擊。

科學化防禦策略

為了有效抵禦攻擊，不僅需洞悉攻擊者的策略，還要了解他們的武器。資訊安全專家利用「沙盒」技術偵測各種零日攻擊，防止這些病毒侵入客戶的系統。「沙盒」模擬正常的系統環境，並把潛在的惡意程式放置在特定隔離空間，以監察它們的一舉一動。接着，資訊安全專家會觀察這些不明程式的運作，並分析相關行為模式。「沙盒」技術能找出病毒是隱藏在甚麼程式，還可了解系統受感染的情況，及黑客如何清理他們的踪跡等。

中信國際電訊 CPC的TrustCSI™ ATP進階威脅防護方案正運用了以上技術，以實驗室般的偵測方式，為企業的系統抵擋現存的安全威脅，還能夠防範各類未知攻擊。

此外，TrustCSI™ ATP更能突破傳統安全解決方案的局限，全面並準確地處理各種複雜威脅、惡意程式和針對性攻擊，包括勒索軟件、挖礦劫持以及其他類型的零日攻擊。

事實上，TrustCSI™ ATP只是中信國際電訊CPC其中一項最先進的創新方案。自公司在2001年成立以來，一直致力為企業

only neutralize existing threats, but can also maximize protection against the unknown threats.

The advanced approach that TrustCSI™ ATP utilizes makes it fully capable of handling sophisticated, purpose-built malware and targeted attacks which cannot be detected by traditional signature-based security solutions. Attacks thwarted by TrustCSI™ ATP include ransomware, cryptojacking and other types of zero-day attacks.

TrustCSI™ ATP is actually one of the latest innovations from CITIC Telecom CPC, which has long been providing enterprises with secure ICT solutions since its founding days in 2001. Beginning with its pioneering Private Network solution, the company has offered its Information Security Solutions suite since 2006, gradually expanding to today's comprehensive portfolio of advanced ICT solutions, all developed through real world and best-in-class technologies from technology partners.

Comprehensive Organizational Protection

As an example, a finance industry customer uses a combination of TrustCSI™ ATP and CITIC Telecom CPC's Managed Security Service (MSS) to protect its enterprise network infrastructure, including its email system. The customer also takes advantage of CITIC Telecom CPC's SmartCLOUD™ EPS (End-Point Backup Service) solution to backup its email on cloud, for added redundancy.

TrustCSI™ ATP is able to overcome the intimidating volume of millions of daily emails this finance customer receives, which may overwhelm other security systems. Even though the customer has already deployed various anti-spam, anti-virus and anti-phishing mechanisms, those protective measures are not effective against advanced malware which constantly evolves into new variants capable of bypassing traditional security defenses. Just one successful attack from such malware will incur serious consequences for this financial services company, particularly compromising its reputation.

By having TrustCSI™ ATP monitor its millions of daily emails, the customer is protected against all types of advanced threats. TrustCSI™ ATP diligently and exhaustively inspects every URL and attachment in every email. Suspicious files are submitted to the isolated sandbox environment for further analysis. The unknown attachments are opened and executed in the sandbox, and TrustCSI™ ATP observes and analyzes the behavior of the unknown objects (such as system changes, exploit efforts, site visits, subsequent downloads, etc.) in order to uncover these obscured factors. In this manner, TrustCSI™ ATP can protect the enterprise against advanced attacks by creating a customized signature that is automatically deployed to the firewall, blocking further attack attempts at the first line of defense.

Protection Above and Beyond

Suitable for typical enterprise deployment scenarios across a variety of attack surfaces (including email, web applications, and

提供各種安全的ICT解決方案：從開創先驅的專用網絡方案開始；至2006年推出的信息安全方案；再逐步發展到現時全面且領先的ICT解決方案組合。中信國際電訊CPC的ICT解決方案均利用技術夥伴的頂尖技術，並結合多年的實際經驗所開發，有效配合企業的各種需要。

全面保護企業利益

例如一位金融業客戶同時使用了中信國際電訊CPC的TrustCSI™ ATP和信息安全管理服務（MSS）組合來保護企業的基礎網絡設施，當中包括其電子郵件系統。客戶還使用了SmartCLOUD™ EPS（端點備份服務）解決方案將其電子郵件備份到雲端平台。

在使用TrustCSI™ ATP前，儘管該名客戶已經部署並安裝了各種反垃圾郵件、防毒和反網絡釣魚機制的程式，但這些防護措施並不足以對付不斷變種的進階惡意程式。這些惡意攻擊只要成功一次，便能對這名客戶帶來嚴重的影響，對企業聲譽的損害更是難以估計。因此，客戶便揀選了TrustCSI™ ATP服務來處理每天數以百萬計的電子郵件收發，而據了解，這個異常龐大的數量往往令其他服務供應商的安全系統不勝負荷。

透過TrustCSI™ ATP監控每日數百萬封的電子郵件，客戶電郵系統得以保護以抵抗各種類型的進階威脅。TrustCSI™ ATP可詳盡地檢查電郵內的每一個URL和附件，並把可疑文件提交到完全隔離的「沙盒」環境作進一步分析。TrustCSI™ ATP將在沙盒中開啟及執行所有未知的附件，同時觀察和分析它們的行為（例如系統更改、利用漏洞、網頁訪問、後續下載等），從而揭開這些不知名因素所帶來的威脅。通過這種方式，TrustCSI™ ATP隨即在防火牆上自動部署相應的病毒特徵，第一時間遏止進一步攻勢。

持續的高水平防護

TrustCSI™ ATP適用於多個企業部署方案，能夠應對不同層面（包括電子郵件，互聯網應用程式和企業網絡）的攻擊。然而，它只是中信國際電訊CPC眾多的信息安全解決方案中的一員。除TrustCSI™ ATP外，全面的TrustCSI™ 託管式安全服務還提供世界級的技術配置，24x7安全運作中心（SOC）無間斷支持，並由獲得專業認證的安全專家作全天候安全監控；能詳細檢查發生的每一宗安全事件，並主動偵測及回應各類型的潛在威脅，為客戶及早消除危機，防患未然。TrustCSI™ 專業安全管理服務進一步增強企業的安全優勢，令更複雜的資訊安全問題也無所遁形。

TrustCSI™ 旗艦系列中的另一項產品是最近新增的TrustCSI™ Secure AI。此服務透過人工智能技術，把生物免疫系統的模式發揮得更淋漓盡致。TrustCSI™ Secure AI具有強大的自學能力，能通過從經驗中學習以預防新型攻擊。

enterprise networks), TrustCSI™ ATP is by no means the only ICT security solution CITIC Telecom CPC offers. The company's portfolio also includes fully managed security solutions that feature round-the-clock monitoring and support by its 24x7 Security Operations Centers (SOCs), world-class facilities staffed by industry-certified security professionals who help customers monitor, detect and mitigate security threats, checking every single security incident that occurs to proactively detect and respond to potential threats before they damage the enterprise. This professional managed service further enhances a business's security posture, above and beyond the sophisticated measures handled by TrustCSI™ ATP.

Another offering within the TrustCSI™ flagship family is the recently added TrustCSI™ Secure AI, which further extends the biological immune response analogy with Artificial Intelligence to bring a new approach to enterprise cyber defense, enabling TrustCSI™ Secure AI to have a powerful self-learning ability that can anticipate new attacks, by learning from experience.

Essentially, the overall theme to CITIC Telecom CPC's answer for modern enterprises wishing to be protected against the wide range of ever-evolving threats, even as these businesses take advantage of Digital Transformation, is continuous improvement. Indeed, the company's motto is "Innovation Never Stops", and because criminals are not ceasing their efforts to overcome defensive measures, the only way to win in the cyber arms race is to stay ahead, with persistent refinements, continuous innovation, just as biological systems never cease to adapt, grow, and evolve.

為協助企業在「數碼轉型」的時代中把握機遇，中信國際電訊CPC時刻精益求精，致力抵禦各種不斷進化的安全威脅。事實上，網絡犯罪分子從不放棄任何摧毀安全防禦系統的機會，中信國際電訊CPC貫徹「創新不斷」的經營理念，因為要在「網絡軍備競賽」中保持優勢，便要不斷改進、力求創新 — 就像生物免疫系統一樣：從不間斷地調整、成長和進化。