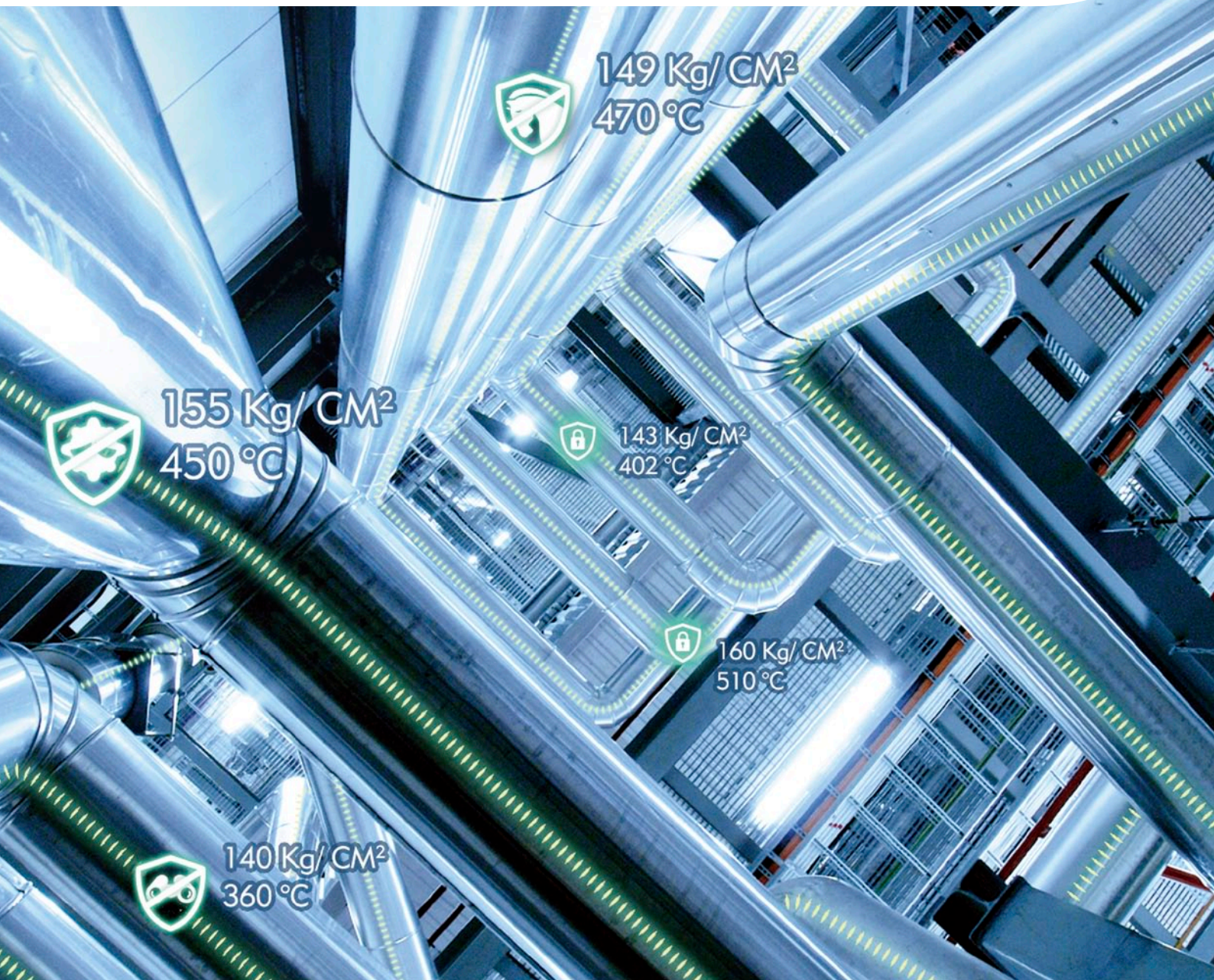
白皮書

IDS/IPS 助陣
進階控管產業網路資安



回顧以往，僅有企業區域網路 (LAN) 管理者，需費心思索資訊安全防禦，至於產業機台、裝置因不具連線能力，或採用封閉式網路，因此多無資安顧慮。然今隨著各行各業紛紛走向 IP 通訊化、物聯網化，導致資安威脅驟增，如何為產業網路做好資安風險管控已是不容忽視的重要課題。

隨著工業 4.0、智慧工廠或工業物聯網等趨勢浪潮席捲，過去大量「與世隔絕」的機台設備，開始向 IP 通訊靠攏。新漢網路通訊事業群協理劉宏益指出，因遠端監控與預防保養需求，製造業者串聯工控網路與網際網路，讓資安風險急遽增高。

又例如醫療產業希藉行動、遠距醫療照護，提高服務水準的同時，亦需將資料安全納入考量，確保病患隱私。各產業已開始留意資訊安全議題，著手導入產業防火牆，一來確保遠端連線安全，二來順勢遏阻可疑的資訊交換。

IDS/IPS 智能分析　與防火牆相輔相成

防火牆是發展歷程逾 20 年的老技術，它僅能依據 IP 或 MAC 位址等基本資訊，簡單比對來者是否名列黑名單，如果是便加以攔阻，如果不是就予以放行；惡意人士相當嫻熟防火牆運作原理，也不斷研究如何以正常外表包覆惡意軟體的方式，藉此矇混過關。故針對防火牆日誌 (Log) 再做進一步檢查與分析，補防火牆之不足，方能阻止有心人士乘隙入侵。

例如整合具有入侵偵測／防禦 (IDS/IPS) 進階功能的資安設備，借助智能控制與比對引擎，自動濾除掉防火牆難以辨識的惡意封包，甚至還能結合產業用特殊協定或慣性行為模式比對，進一步阻斷可疑連線，使其無法潛入產業網路與位於網路底層的終端設備。

分散式架構嚴控資安風險　防制災情、遏止擴散

企業網路將安全機制集中部署在網路出口，即為內外資料進出的閘道，但產業網路的重點保護對象是機台、裝置，故應將資安設備分散佈署在產業網路下每個子網域的出入口，就近提供防護。如此一來，即使某個子網域中已有機台受到惡意軟體感染，但當惡意軟體隱藏在資訊中企圖潛越，IDS/IPS 一經察覺問題資訊，即可丟棄封包、或切斷該網路對外連線，進而將惡意軟體限縮在子網域內，不致讓病毒擴散至整個產業網路。

曾有製造業主管透露，過去一些跳電或故障停機事件，乍看之下似有合理解釋，但若深入剖析，會發現機台中毒恐怕才是問題徵結。對於高度倚重生產線持續高效率運作的製造業者而言，病毒或惡意程式引發的機台設備故障，輕則造成生產作業短暫中斷、影響產能，重則釀成製程報廢、原物料盡付東流，乃至於衝擊交期，損失可謂不輕。

有鑑於此，新漢推出的產業型防火牆，兼具 VPN、防火牆與 IDS/IPS 功能，提供整合型防禦措施，一次解決產業網路的各種安全威脅。劉宏益表示，新漢提供的 IDS/IPS 引擎，擁有豐富的特徵資料庫可供比對，可以透過日誌分析、安全性資訊和事件管理 (SIEM) 關聯分析等途徑，深入挖掘出埋藏在正常表象之中的異常程式或檔案。且即便工廠內部的機台採用浮動 IP，搭配虛擬私有網路 (VPN) 穿透層層限制，總部仍能在遠端監看現場。

當業者厲精圖治，藉由設備走向 IP 通訊化、物聯網化來提升管理、營運效率的同時，對於產業網路的資安風險也不能等閒視之。故應導入 VPN、防火牆與 IDS/IPS 等整合式防禦機制，將病毒、惡意程式屏蔽在產業網路外，藉以保護位於產業網路底層的終端裝置，消弭干擾機台設備正常運作的潛在風險，更可防堵駭客入侵，杜絕機密智財、隱私外洩。

新漢股份有限公司創立於 1992 年，事業單位橫跨多媒體、車載電腦、IoT 智動化、網通、智能監控及醫療資訊六大領域，並於五大工業國設有子公司提供全球營銷服務。積極迎接物聯網浪潮，新漢擴大產品組合，並致力於物聯網、機器人、車聯網、工業 4.0 及產業網安的新興應用。

www.nexcom.com