ST Engineering

威雲科技 WeiCloudTech

GOVERNMENT & PUBLIC SECURITY

保護政府服務及公眾信任
WITH ST ENGINEERING DATA DIODE

針對政府機構的網路攻擊會阻礙基本服務、擾亂公民的生活、破壞公眾信任並危及國家安全。正如最近的網路攻擊所顯示，駭客高度重視政府資料，且以熟練的技術非常積極地執行任務。

2018 年，印度中央政府的生物辨識系統 Aadhaar 遭受到攻擊，而洩漏了 11 億筆的公民紀錄。

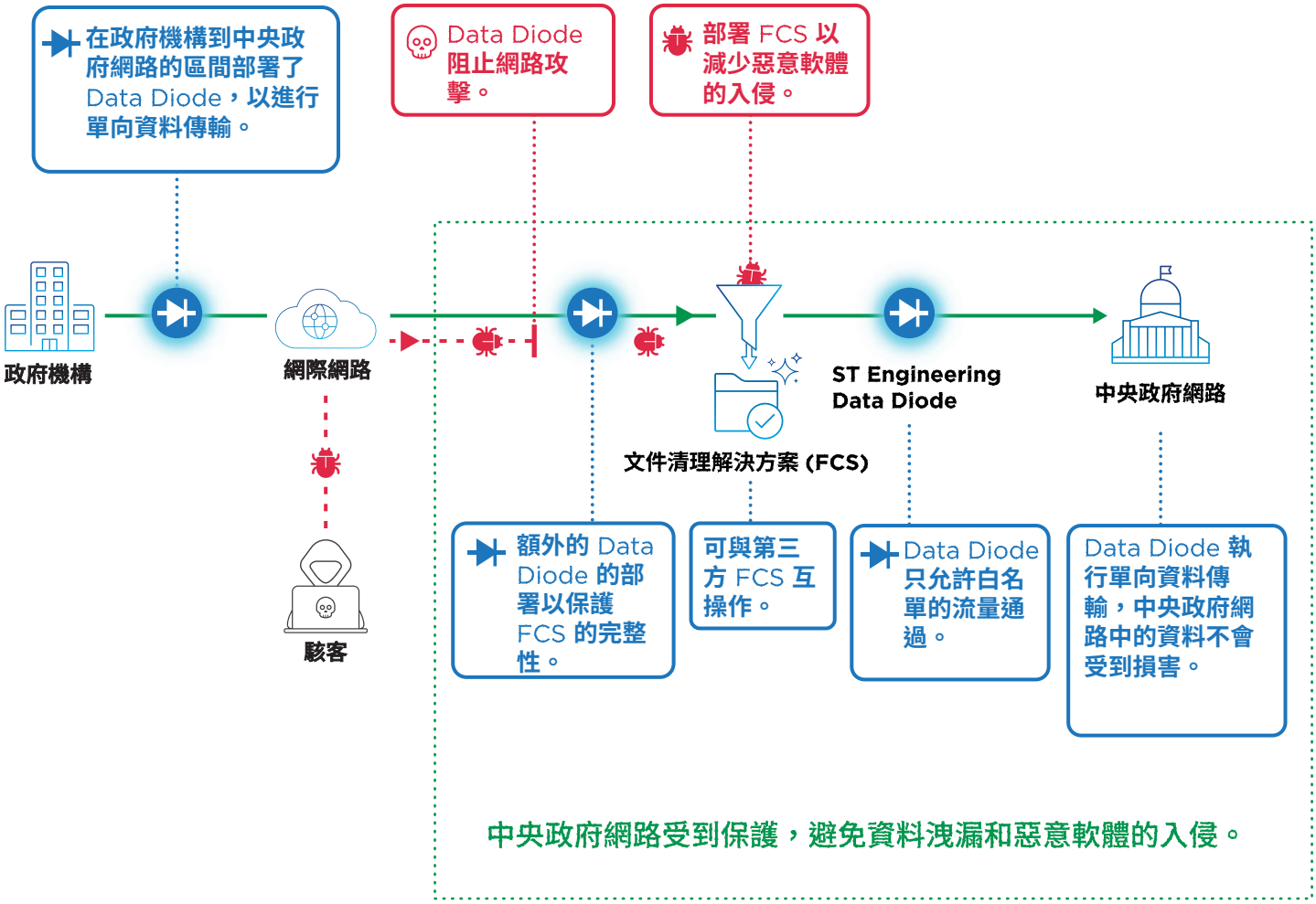
- Business Insider India

美國政府機構在 2020 年遭受到世界上有史以來規模最大、最複雜的網路攻擊，受到影響範圍包括財政部、司法部和商務部。

- Reuters

保護中央政府網路的挑戰

- 透過網際網路安全地傳送和接收資料，同時防止中央政府系統免於遭受來自網際網路和外部網路的惡意軟體入侵和網路攻擊。
- 確保符合政府安全規範 (包括 CC EAL 4+、NITES 認證)，同時提供端到端的高傳輸量且無資料遺失。



ST Engineering Data Diode 可透過安全文件清理解決方案降低惡意軟體對中央政府的入侵攻擊風險，同時預防中央政府的資料洩漏。

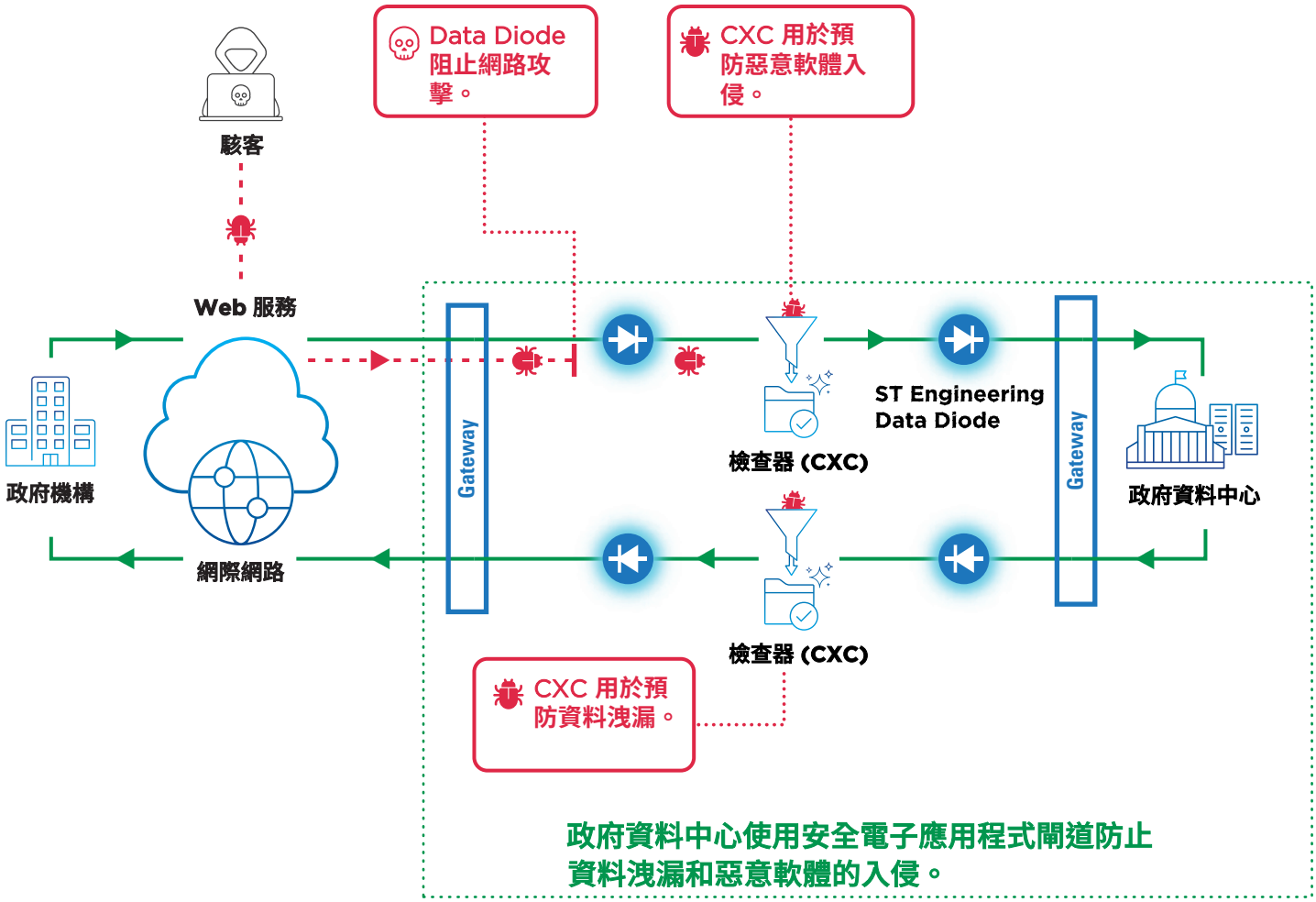
在政府機構和中央政府之間建立網路分離。

可擴充的傳輸量，滿足極高的資料傳輸要求 (超過 500 Mbps)。

透過高可用性 (故障轉移) 配置，將停機時間要求降至最低。

保護政府資料中心的挑戰

- 允許透過網際網路存取政府資料中心，同時預防政府資料中心受到網路攻擊。
- 確保符合政府安全規範 (包括 CC EAL 4+、NITES 認證)，同時提供端到端的高傳輸量且無資料遺失。



ST Engineering Data Diode 在網際網路上實現了即時的雙向 HTTP(S) 網路服務交易，同時透過安全文件清理解決方案保護政府資料中心免於受到惡意軟體的入侵和資料洩漏。

- 透過應用層負載檢查器 (CXC) 緩解應用層攻擊。
- 透過 ST Engineering Data Diode 降低網路層攻擊風險。
- 對所有入站和出站流量進行 100% 檢查。
- 透過高可用性 (故障轉移) 配置，將停機時間要求降至最低。

About ST Engineering Data Diode

- Up to **20Gbps** Unidirectional Media Transfer Rate
- **High Throughput** Files Transfer (More than 5TB of files per day)
- **Zero-Loss*** Files Transfer (*No more than 1 File lost in 5 Million Files Transfer)
- **Files Lost Detection** capability for ease of operation & maintenance
- **Integrated Management Portal** for ease of deployment, operation & maintenance
- Configurable for **High Availability** (without additional hardware/software)
- **Low Total Cost of Ownership** (ease of deployment, operation & maintenance; no dependencies on external proxies, no need for regular updates and patches)

ABOUT ST ENGINEERING INFO-SECURITY

An industry leader in cybersecurity with over two decades of experience, our mission is to deliver a holistic suite of trusted cybersecurity solutions to help government and ministries, critical infrastructures and commercial enterprises stay cyber safe in the accelerated digital economy.

Backed by indigenous capabilities and deep domain expertise, we offer world-class cybersecurity products and solutions spanning from cryptography, cross-domain solutions to industrial control systems (ICS) cybersecurity solutions.

To sustain a robust cyber-resilient ecosystem in the areas of People Process and Technology, we help our clients increase their cybersecurity preparedness with our managed security services and cybersecurity professional services including consultancy, vulnerability assessment, penetration testing, risk and compliance services.

www.stengg.com
cybersecurity@stengg.com

DOP1121

www.stengg.com/cybersecurity

ST Engineering

威雲科技 WeiCloudTech

HIGH-TECH MANUFACTURING

提供工業級的網路安全
WITH ST ENGINEERING DATA DIODE

針對製造工廠的網路攻擊可能會擾亂甚至中斷生產，進而損害公司聲譽、股價和消費者信心。智慧財產權盜竊行為在網路攻擊中很常見，這可能導致市場佔有率的喪失和公司破產。根據最新報告顯示，網路攻擊的代價高昂，且頻率不斷的增加。

2019 年製造業向網路犯罪分子支付了 690 萬美元，佔勒索軟體支付總額的 62%。

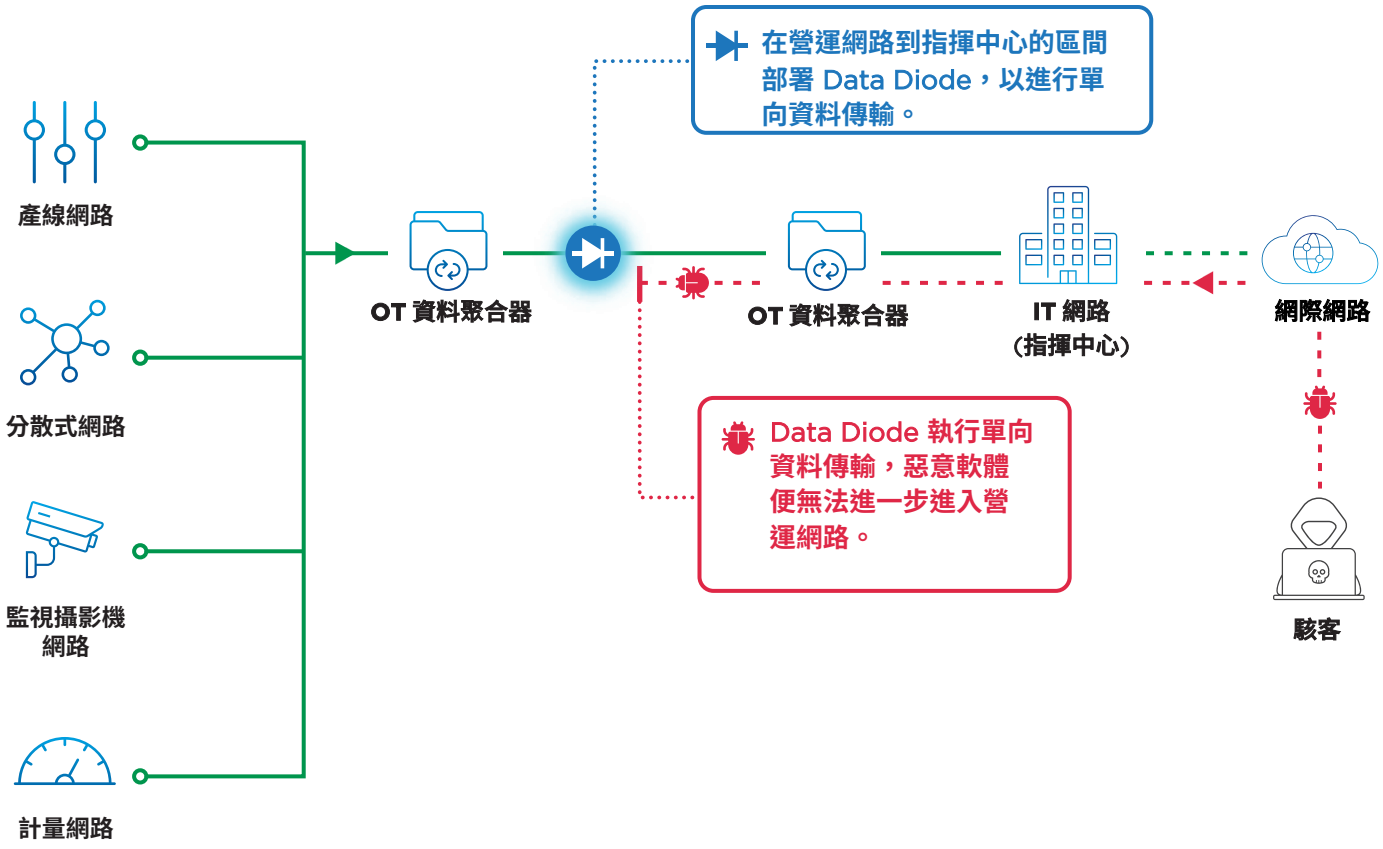
- Kivu Consulting 2019 Paid Ransomware Report

73% 的製造資料洩露事件是出於金錢目的。

- Verizon Data Breach Investigations Report 2019

監控營運資料的挑戰

- 允許即時監控製造操作情況，同時保護作業系統免於遭受來自網際網路和外部網路的網路攻擊。
- 確保符合工業安全規範 (包括 CC EAL 4+、NITES 認證)，同時提供端到端的高傳輸量且無資料遺失。



OT/IT 網路

營運網路受到保護免於遭受網路攻擊。

ST Engineering Data Diode 能夠將營運資料從營運網路單向傳輸到企業網路，同時預防對營運網路進行的網路攻擊。

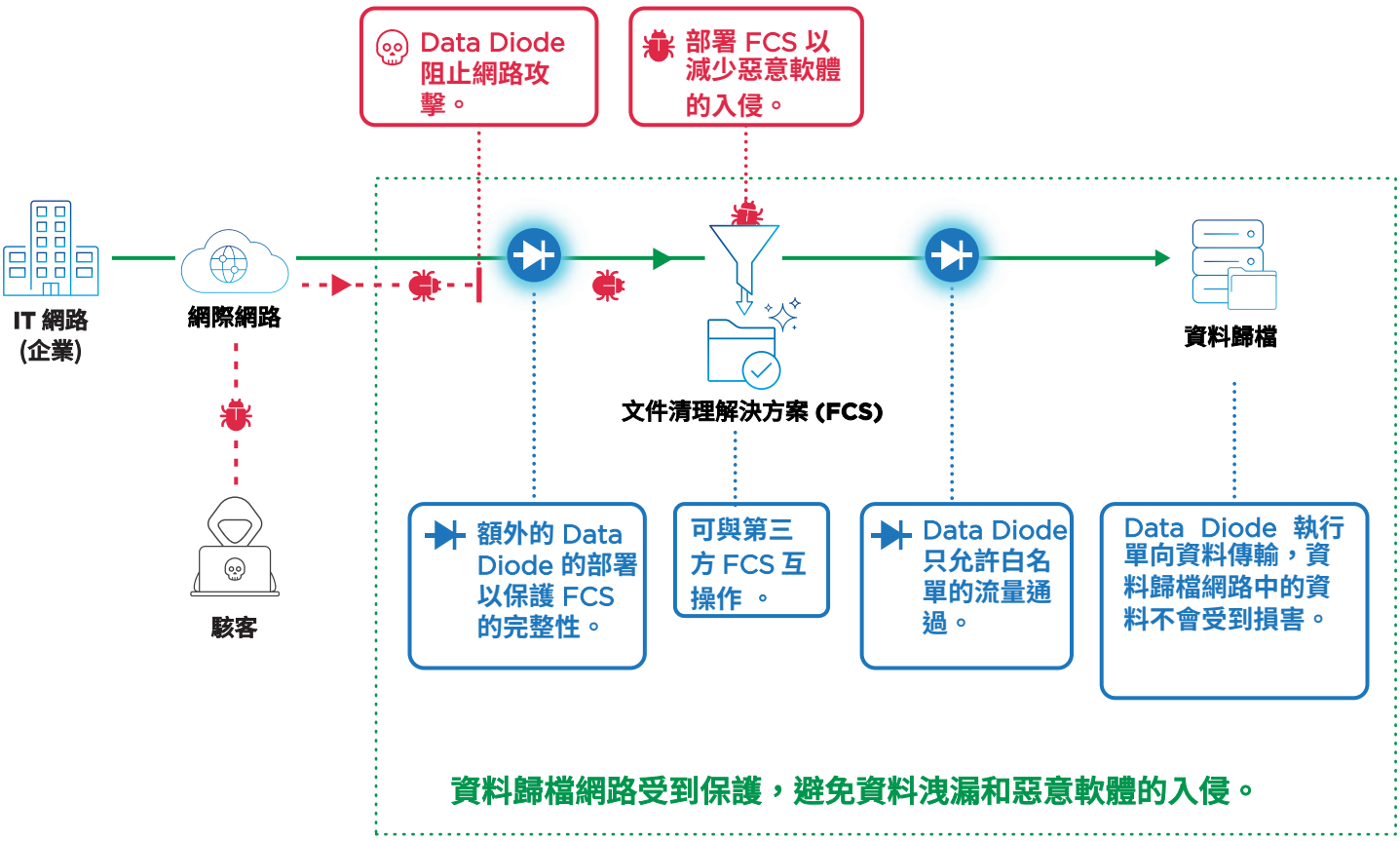
在關鍵操作系統和企業網路或網際網路之間建立網路分離。

透過高可用性 (故障轉移) 配置，將停機時間要求降至最低。

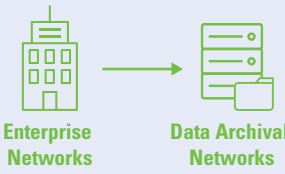
可對所有操作系統進行即時監控。

保護資料歸檔網路的挑戰

- 安全地備份和儲存資料，同時預防來自網際網路和外部 IT 網路的資料歸檔網路的惡意軟體感染。
- 保護資料歸檔網路中文件的完整性。
- 確保符合工業安全規範 (包括 CC EAL 4+、NITES 認證)，同時提供端到端的高傳輸量且無資料遺失。



ST Engineering Data Diode 讓文件單向傳輸到資料歸檔網路，同時預防資料洩漏和竊取。



ST Engineering Data Diode 確保只允許白名單流量通過，可保護組織免受製造工廠發生的資料洩漏和惡意威脅影響。文件清理解決方案 (FCS) 可以進一步整合，以確保只有未包含惡意軟體的文件可以進入資料歸檔網路。

在企業網路和資料歸檔網路之間建立網路分離。

透過高可用性 (故障轉移) 配置，將停機時間要求降至最低。

100% 防止任何資料洩漏。

About ST Engineering Data Diode

- Up to **20Gbps** Unidirectional Media Transfer Rate
- **High Throughput** Files Transfer (More than 5TB of files per day)
- **Zero-Loss*** Files Transfer (*No more than 1 File lost in 5 Million Files Transfer)
- **Files Lost Detection** capability for ease of operation & maintenance
- **Integrated Management Portal** for ease of deployment, operation & maintenance
- Configurable for **High Availability** (without additional hardware/software)
- **Low Total Cost of Ownership** (ease of deployment, operation & maintenance; no dependencies on external proxies, no need for regular updates and patches)

ABOUT ST ENGINEERING INFO-SECURITY

An industry leader in cybersecurity with over two decades of experience, our mission is to deliver a holistic suite of trusted cybersecurity solutions to help government and ministries, critical infrastructures and commercial enterprises stay cyber safe in the accelerated digital economy.

Backed by indigenous capabilities and deep domain expertise, we offer world-class cybersecurity products and solutions spanning from cryptography, cross-domain solutions to industrial control systems (ICS) cybersecurity solutions.

To sustain a robust cyber-resilient ecosystem in the areas of People Process and Technology, we help our clients increase their cybersecurity preparedness with our managed security services and cybersecurity professional services including consultancy, vulnerability assessment, penetration testing, risk and compliance services.

www.stengg.com
cybersecurity@stengg.com

DOP1121

www.stengg.com/cybersecurity

ST Engineering

威雲科技 WeiCloudTech

TRANSPORT / UTILITIES

保護基礎設施的網路安全

WITH ST ENGINEERING DATA DIODE

針對關鍵基礎設施(包括航空、鐵路運輸、水和發電廠等)的網路攻擊可能會導致災難性的後果。如果網路犯罪分子獲得對這些基礎設施作業系統的存取和控制權，他們會對日常基本運作造成重大干擾、人員受傷甚至危害性命，並失去公眾的信任。

自 2020 年 6 月以來，全球試圖對交通運輸部門進行勒索軟體攻擊的比例增加了 186%。

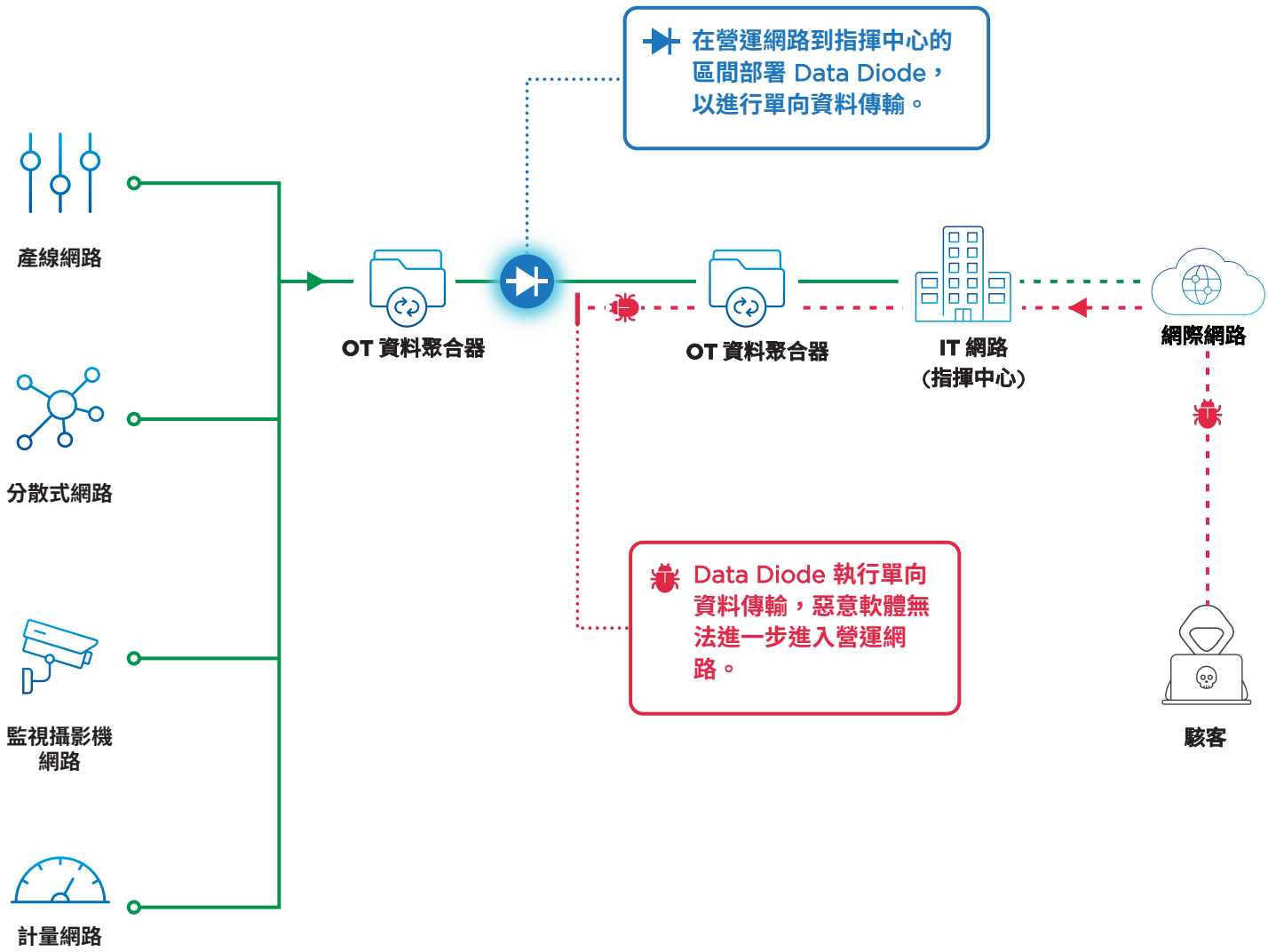
- Check Point Research report

2019 年對 IoT (物聯網) 設備的網路攻擊激增了 300%。

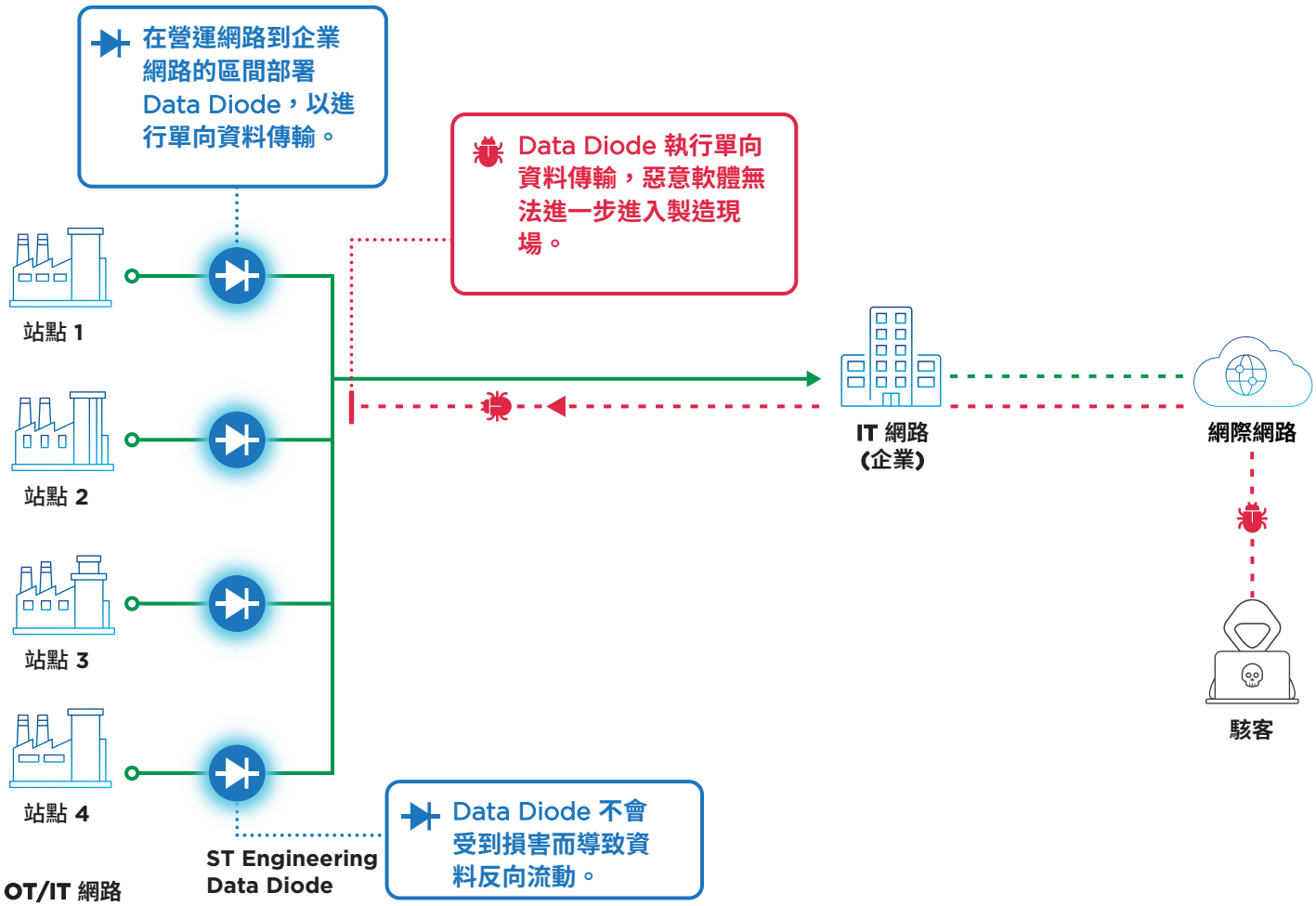
- Forbes

監控作業系統的挑戰

- 允許即時監控機場、運輸和公用事業營運的運作情況，同時保護作業系統免於遭受來自網際網路和外部網路的網路攻擊。
- 確保符合工業安全規範 (包括 CC EAL 4+、NITES 認證)，同時提供端到端的高傳輸量且無資料遺失。



營運網路受到保護，免於遭受以網路為基礎的攻擊。



ST Engineering Data Diode 透過單向文檔傳輸或 OT 資料複製，實現對機場、運輸及公用事業運營系統的即時、非侵入式監控，同時預防對關鍵營運系統進行的網路攻擊。

在關鍵操作系統和企業網路或網際網路之間建立網路分離。

透過高可用性 (故障轉移) 配置，將停機時間要求降至最低。

可對所有操作系統進行即時監控。

About ST Engineering Data Diode

- Up to **20Gbps** Unidirectional Media Transfer Rate
- **High Throughput** Files Transfer (More than 5TB of files per day)
- **Zero-Loss*** Files Transfer (*No more than 1 File lost in 5 Million Files Transfer)
- **Files Lost Detection** capability for ease of operation & maintenance
- **Integrated Management Portal** for ease of deployment, operation & maintenance
- Configurable for **High Availability** (without additional hardware/software)
- **Low Total Cost of Ownership** (ease of deployment, operation & maintenance; no dependencies on external proxies, no need for regular updates and patches)

ABOUT ST ENGINEERING INFO-SECURITY

An industry leader in cybersecurity with over two decades of experience, our mission is to deliver a holistic suite of trusted cybersecurity solutions to help government and ministries, critical infrastructures and commercial enterprises stay cyber safe in the accelerated digital economy.

Backed by indigenous capabilities and deep domain expertise, we offer world-class cybersecurity products and solutions spanning from cryptography, cross-domain solutions to industrial control systems (ICS) cybersecurity solutions.

To sustain a robust cyber-resilient ecosystem in the areas of People Process and Technology, we help our clients increase their cybersecurity preparedness with our managed security services and cybersecurity professional services including consultancy, vulnerability assessment, penetration testing, risk and compliance services.

www.stengg.com
cybersecurity@stengg.com

DOP1121

www.stengg.com/cybersecurity