ST Engineering

FINANCIAL SERVICES

SAFEGUARD FINANCIAL ASSETS AND CUSTOMER PRIVACY

WITH ST ENGINEERING DATA DIODE

As a repository of extremely valuable data including personal and corporate information, bank account and credit card numbers, financial organisations are one of the most heavily targeted sectors by cyber criminals. In addition to the higher frequency of cyber-attacks, financial institutions are facing more aggressive enforcement, higher fines and regulatory costs, and growing third party liability.

US$80m

fine paid by Capital One for the 2019 data breach that exposed the personal information of more than 106m customers and credit card applicants.

- Financial Times

238%

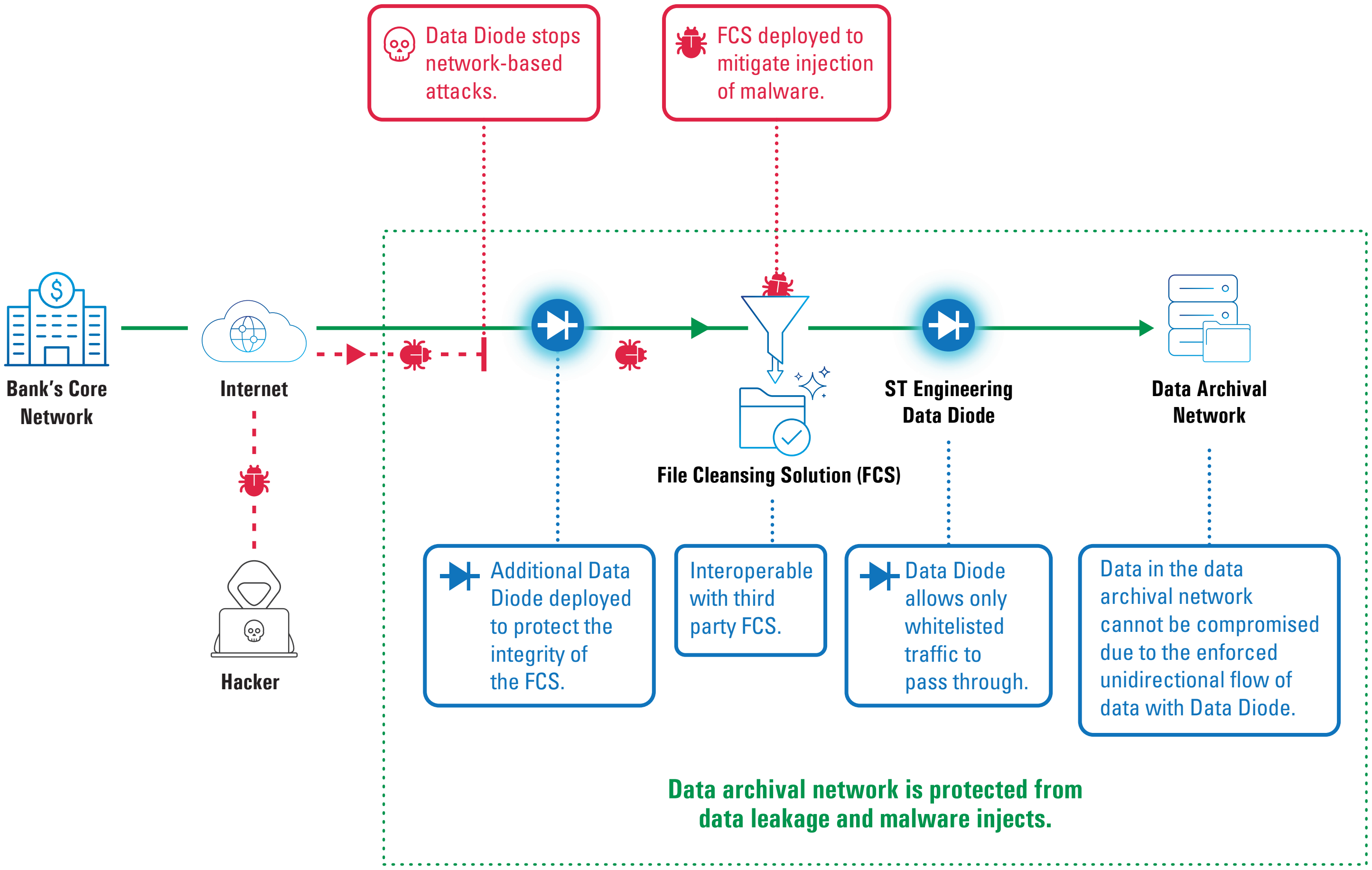
increase in attacks targeting the financial sector from February to April 2020.

- VMware Modern Bank Heists 3.0 Threat Report

Challenges of

Protecting data archival network

- Securely store and backup crucial bank data, while preventing malware injects to data archival network from the internet and external networks
- Ensure compliance with industry security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss
- Protect the integrity of data in data archival network



Data Diode stops network-based attacks.
FCS deployed to mitigate injection of malware.
Bank's Core Network
Internet
Hacker
File Cleansing Solution (FCS)
ST Engineering Data Diode
Data Archival Network
Additional Data Diode deployed to protect the integrity of the FCS.
Interoperable with third party FCS.
Data Diode allows only whitelisted traffic to pass through.
Data in the data archival network cannot be compromised due to the enforced unidirectional flow of data with Data Diode.
Data archival network is protected from data leakage and malware injects.

ST Engineering Data Diode enables **mitigation against malware injects to data archival network** via Secure Files Cleansing Solution, while preventing unauthorised access to data archival networks to ensure data integrity.

Creates network separation between bank's core networks and data archival networks.

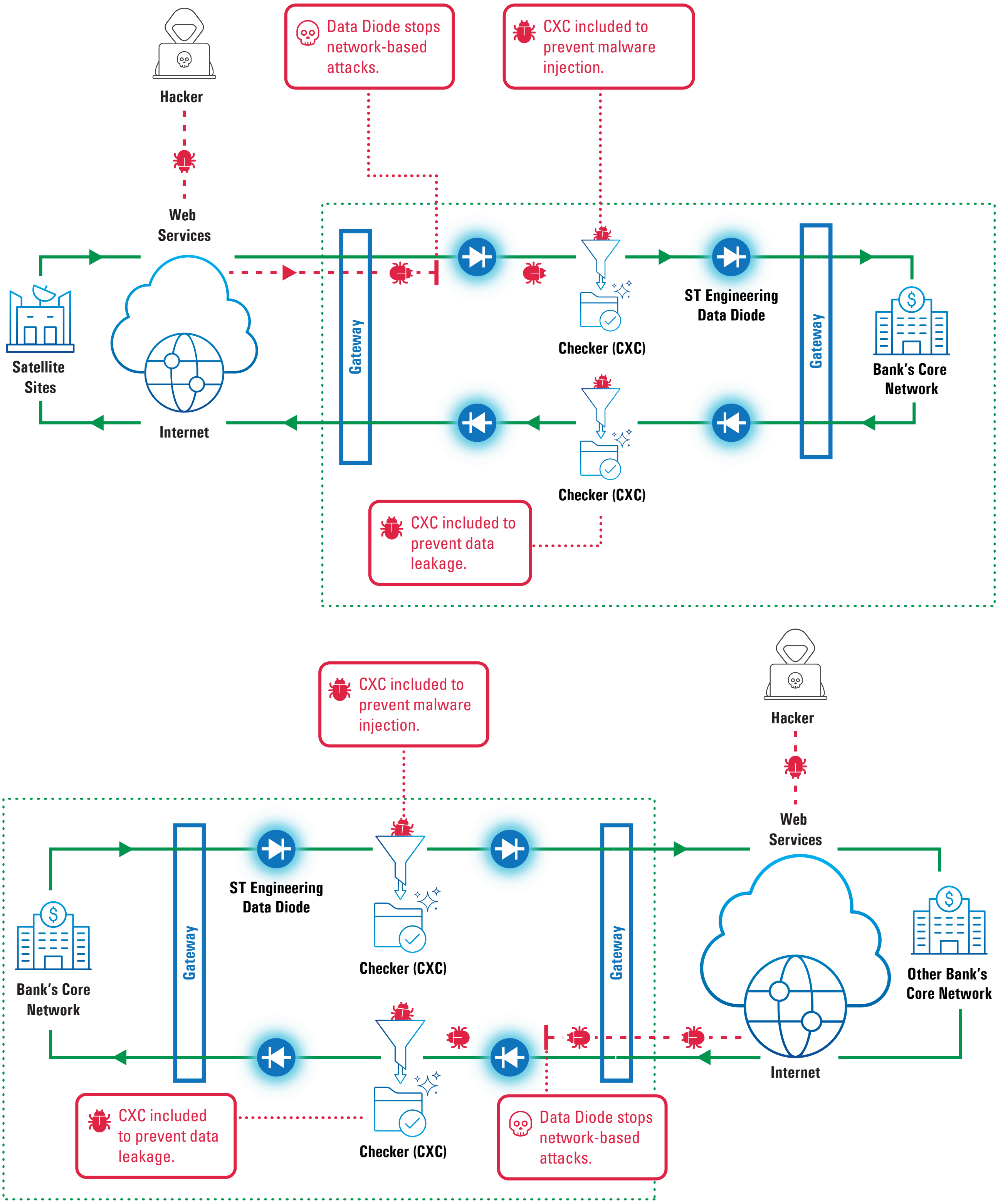
Prevents network-based cyber-attacks to data archival networks from the internet and external networks.

Minimal downtime requirements through high-availability (failover) configuration.

Challenges of

Protecting bank's core network

- Allow access to bank's core network over the internet, while preventing bank's core network from cyber-attacks
- Ensure compliance with government security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss



Data Diode stops network-based attacks.

CXC included to prevent malware injection.

CXC included to prevent data leakage.

CXC included to prevent malware injection.

CXC included to prevent data leakage.

Data Diode stops network-based attacks.

Bank's Core Network is protected from data leakage and malware injects by Secure e-Application Gateway.

ST Engineering Secure e-Application Gateway enables real-time **bi-directional HTTP(S) web services transactions over the internet** while protecting the bank's core network from malicious injects and data leakage through Secure e-Application Gateway.

Mitigates against application layer attack via application layer payload checker (CXC)

Mitigates against network layer attack via ST Engineering Data Diode

100% checks on all inbound and outbound traffic.

Minimal downtime requirements through high-availability (failover) configuration.

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.

Learn more at:

CONTACT US: Email: cybersecurity@stengg.com LinkedIn: linkedin.com/st-engineering-cybersecurity

PROTECT GOVERNMENT SERVICES AND PUBLIC TRUST

WITH ST ENGINEERING DATA DIODE

Cyber-attacks on government agencies can obstruct essential services, disrupt the lives of citizens, destroy public trust and jeopardise national security. As recent cyber-attacks show, hackers highly value government data and are well skilled and extremely motivated for their mission.

1.1 billion

citizen records were leaked in the 2018 breach of Aadhaar, India's centralised biometric ID system.

- Business Insider India

U.S. government agencies

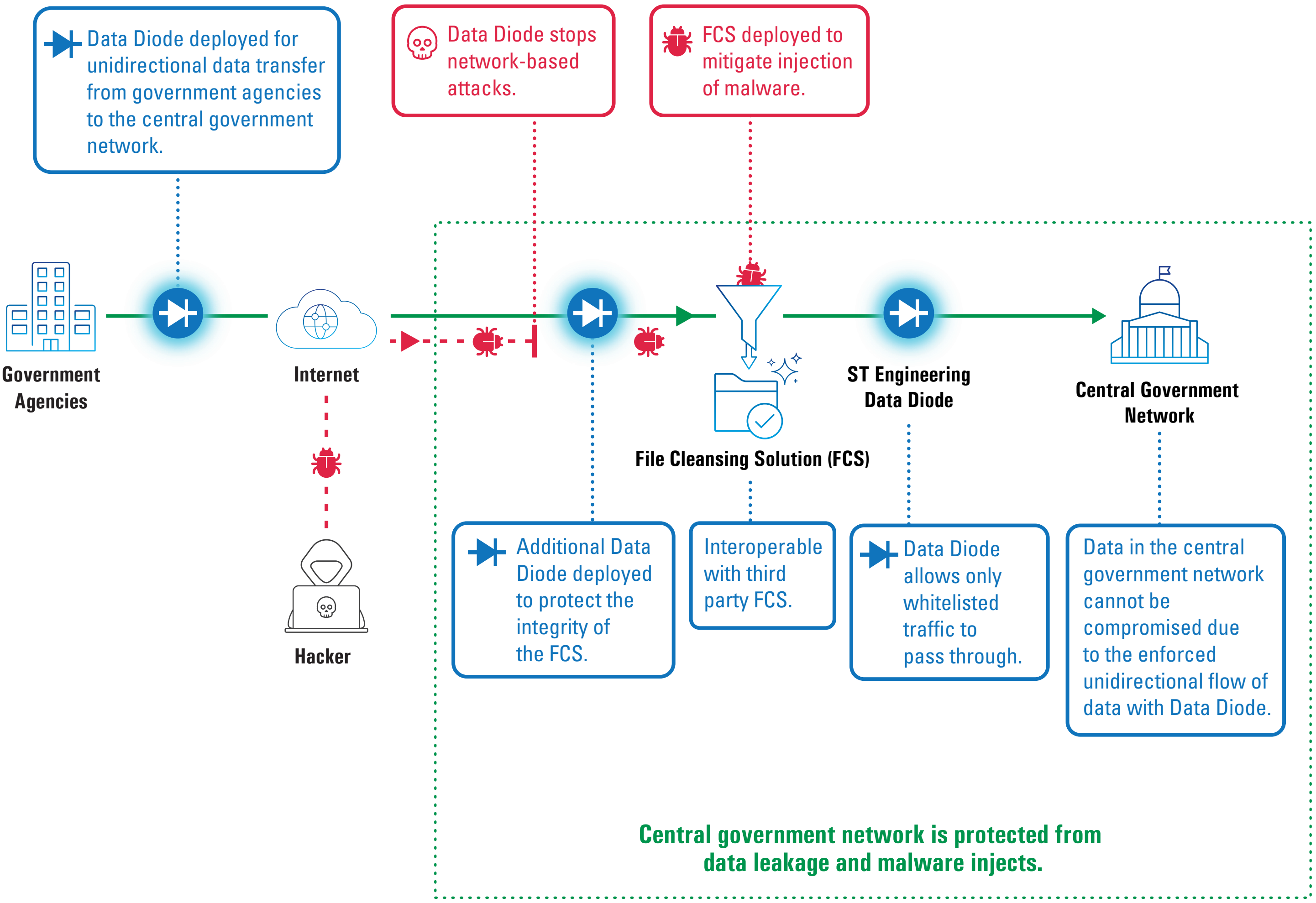
including the Treasury, Justice and Commerce departments, were attacked in the largest and most sophisticated attack the world has ever seen in 2020.

- Reuters

Challenges of

Protecting central government network

- Securely send and receive data across the internet, while preventing the central government systems against malware injects and network-based cyber-attacks from the internet and external networks
- Ensure compliance with government security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss


Data Diode deployed for unidirectional data transfer from government agencies to the central government network.
Data Diode stops network-based attacks.
FCS deployed to mitigate injection of malware.
Government Agencies
Internet
Hacker
File Cleansing Solution (FCS)
ST Engineering Data Diode
Central Government Network
Additional Data Diode deployed to protect the integrity of the FCS.
Interoperable with third party FCS.
Data Diode allows only whitelisted traffic to pass through.
Data in the central government network cannot be compromised due to the enforced unidirectional flow of data with Data Diode.
Central government network is protected from data leakage and malware injects.

ST Engineering Data Diode enables **mitigation against malware injects to central government** via Secure Files Cleansing Solution, while preventing data leakage from central government.

Creates network separation between government agencies and central government.

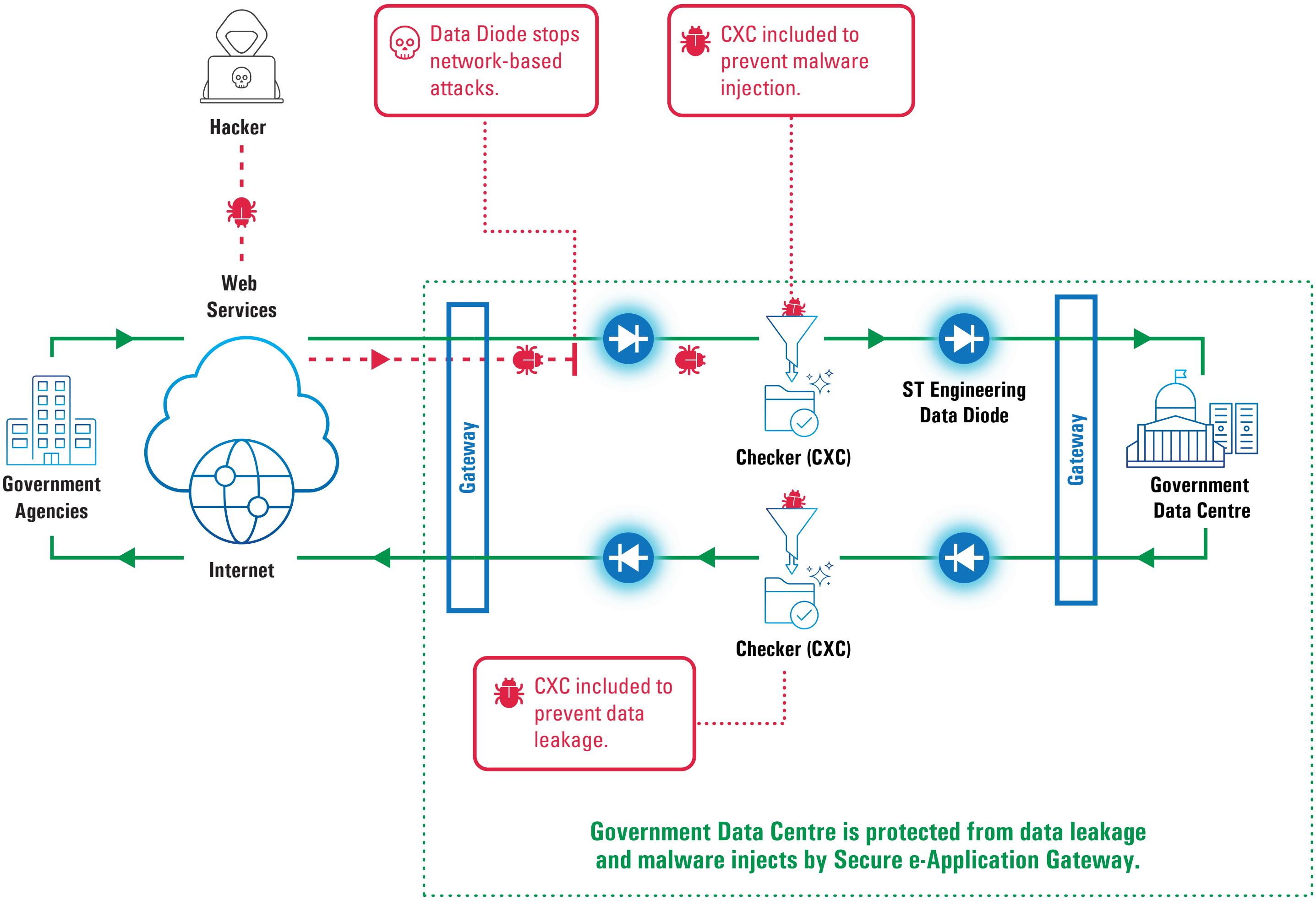
Scalable throughput for extremely high data transfer requirement (more than 500 Mbps).

Minimal downtime requirements through high-availability (failover) configuration.

Challenges of

Protecting government data centre

- Allow access to government data centre over the internet, while preventing government data centre from cyber-attacks
- Ensure compliance with government security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss



Data Diode stops network-based attacks.

CXC included to prevent malware injection.

CXC included to prevent data leakage.

Government Data Centre is protected from data leakage and malware injects by Secure e-Application Gateway.

ST Engineering Data Diode enables real-time **bi-directional HTTP(S) web services transactions over the internet** while protecting the government data centre from malicious injects and data leakage through Secure e-Application Gateway.

Mitigates against application layer attack via application layer payload checker (CXC)

Mitigates against network layer attack via ST Engineering Data Diode

100% checks on all inbound and outbound traffic.

Minimal downtime requirements through high-availability (failover) configuration.

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

www.stengg.com/cybersecurity

SAFEGUARD PATIENT LIVES AND DATA

WITH ST ENGINEERING DATA DIODE

Healthcare is the most heavily targeted sector for cyber-attacks. The broad attack surfaces, legacy system limitations and weak security posture leave healthcare providers highly vulnerable to financially motivated cyber criminals. With the confidentiality, integrity, and availability of patient data, medical devices and healthcare ecosystems at stake, cybersecurity is absolutely critical to healthcare organisations.

50^x

more valuable on the black market than financial information, personal health information is the reason why the healthcare sector is a prime target for cyberattacks.

- Forbes

109

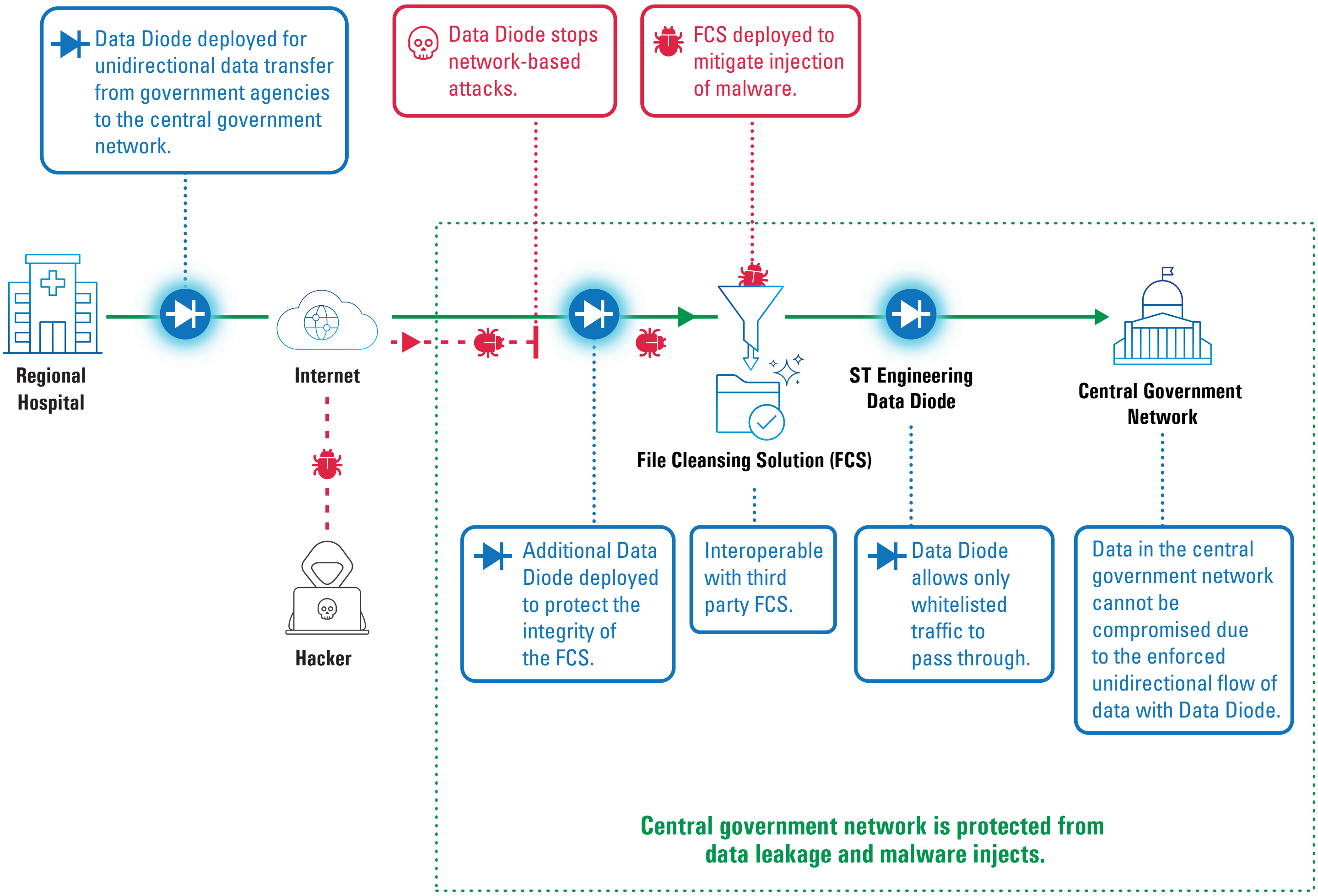
attack attempts per healthcare organisation every week, making healthcare the most targeted sector.

- Check Point Research report 2021

Challenges of

Protecting central government network

- Securely store and receive hospitals' data records, while preventing malware injects to central government network from the internet and external network
- Ensure compliance with industry security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss



Data Diode deployed for unidirectional data transfer from government agencies to the central government network.

Data Diode stops network-based attacks.

FCS deployed to mitigate injection of malware.

Regional Hospital
Internet
Hacker
File Cleansing Solution (FCS)
ST Engineering Data Diode
Central Government Network

Additional Data Diode deployed to protect the integrity of the FCS.

Interoperable with third party FCS.

Data Diode allows only whitelisted traffic to pass through.

Data in the central government network cannot be compromised due to the enforced unidirectional flow of data with Data Diode.

Central government network is protected from data leakage and malware injects.

ST Engineering Data Diode enables **mitigation against malware injects to central government network** via Secure Files Cleansing Solution, while preventing data leakage from central government.

Creates network separation between central government and regional hospitals network.

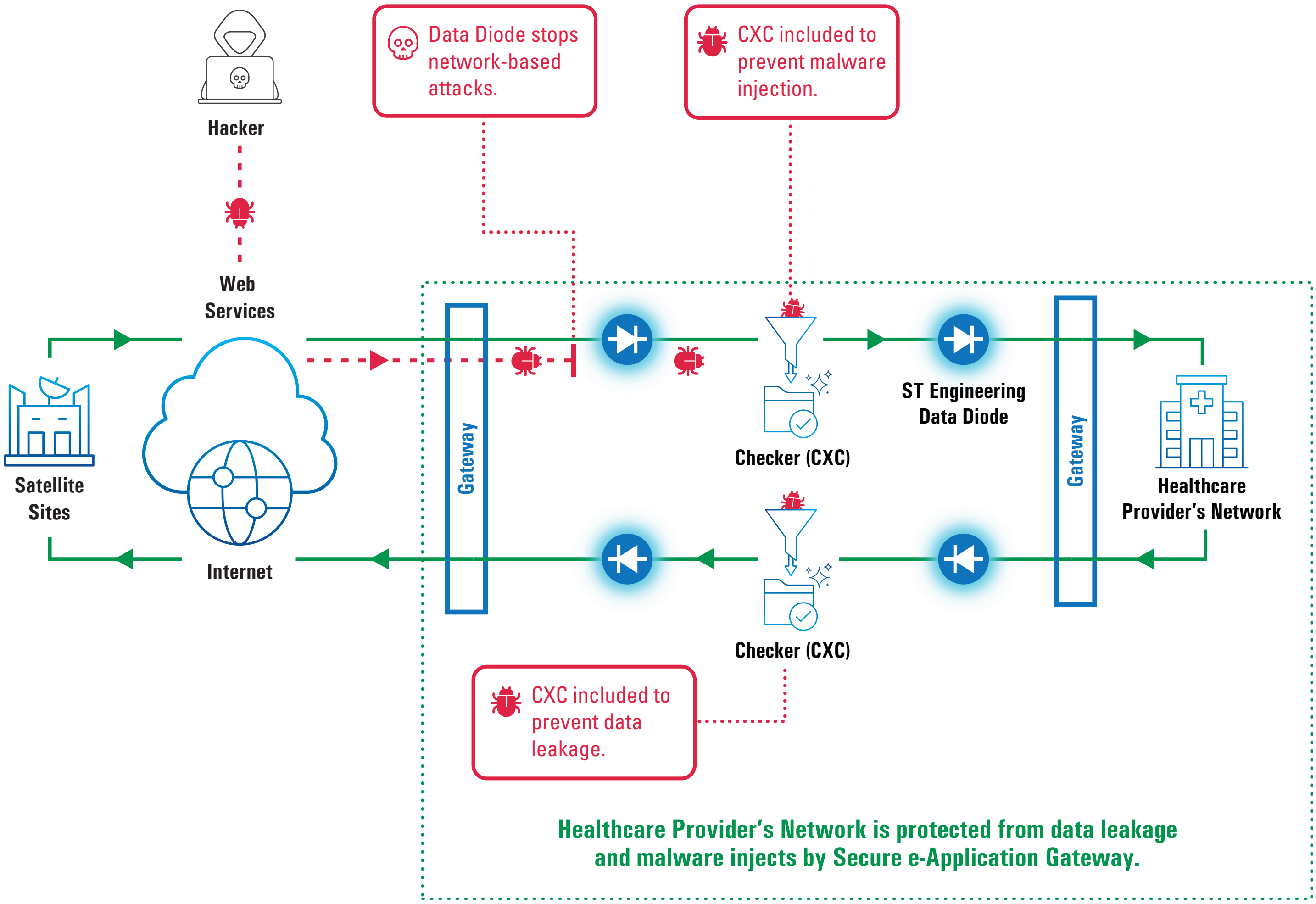
Prevents network-based cyber-attacks to central government networks from the internet and external networks.

Minimal downtime requirements through high-availability (failover) configuration.

Challenges of

Protecting healthcare provider's network

- Allow access to healthcare provider's network over the internet, while preventing healthcare provider's network from cyber-attacks
- Ensure compliance with government security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss



Data Diode stops network-based attacks.

CXC included to prevent malware injection.

CXC included to prevent data leakage.

Healthcare Provider's Network is protected from data leakage and malware injects by Secure e-Application Gateway.

ST Engineering Data Diode enables real-time **bi-directional HTTP(S) web services transactions over the internet** while protecting the healthcare provider's network from malicious injects and data leakage through Secure e-Application Gateway.

- Mitigates against application layer attack via application layer payload checker (CXC)
- Mitigates against network layer attack via ST Engineering Data Diode
- 100% checks on all inbound and outbound traffic.
- Minimal downtime requirements through high-availability (failover) configuration.

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

www.stengg.com/cybersecurity

ST Engineering

HIGH-TECH MANUFACTURING

PROVIDE INDUSTRIAL-STRENGTH CYBERSECURITY

WITH ST ENGINEERING DATA DIODE

Cyber-attacks on manufacturing plants can disrupt and even halt production, causing damage to company reputation, share price and consumer confidence. Theft of intellectual property is common in cyber-attacks which can lead to loss of market share and the company's eventual demise. As latest reports show, the cost of cyber-attacks is high and the frequency is increasing.

US$6.9m

paid by the manufacturing sector to cyber criminals in 2019, representing 62% of total ransomware payments.

- Kivu Consulting 2019 Paid Ransomware Report

73%

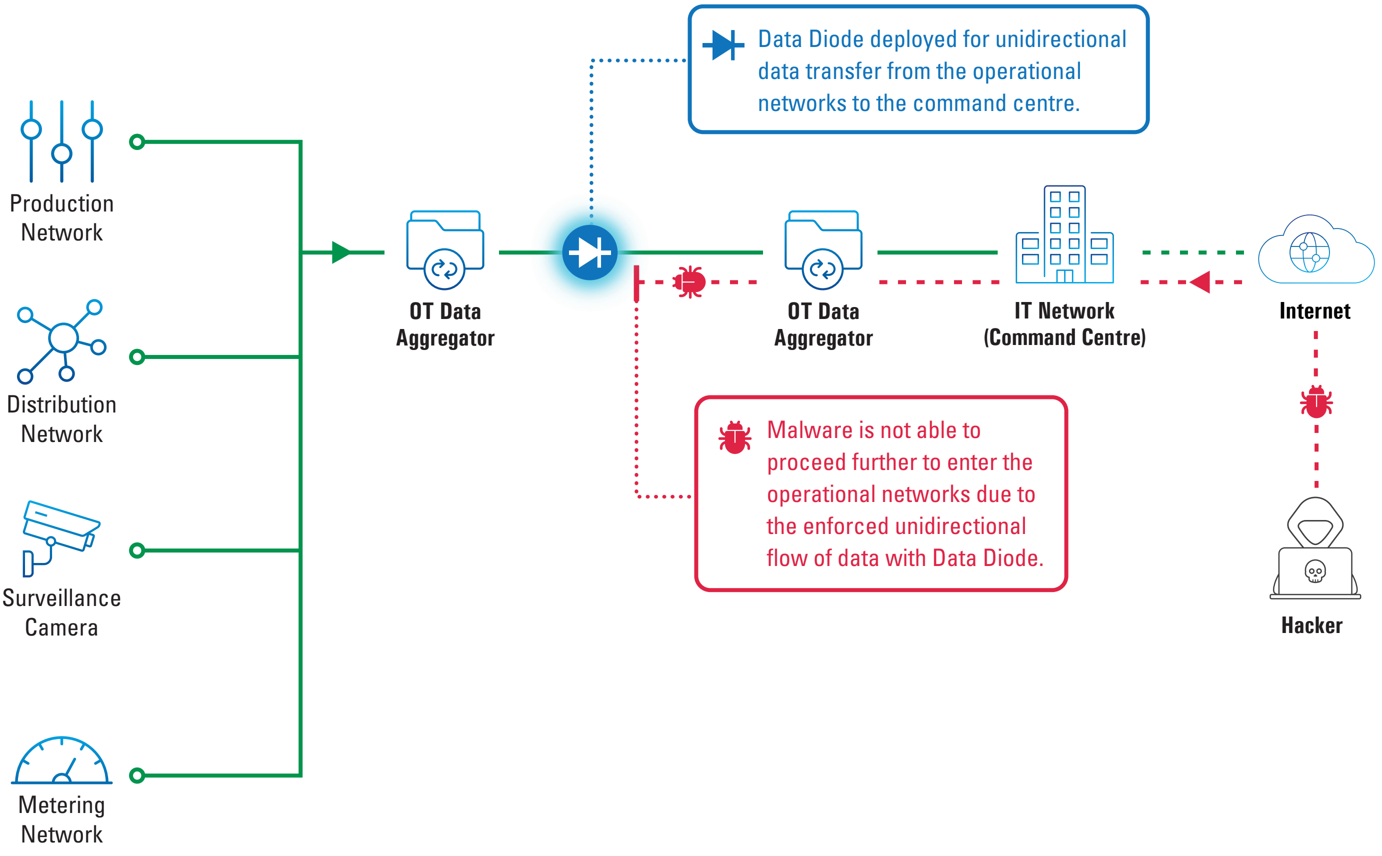
of manufacturing data breaches are financially motivated.

- Verizon Data Breach Investigations Report 2019

Challenges of

Monitoring operational data

- Allow real-time monitoring of manufacturing operations, while safeguarding operation systems against cyber-attacks from the internet and external networks
- Ensure compliance with industry security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss



Data Diode deployed for unidirectional data transfer from the operational networks to the command centre.

Malware is not able to proceed further to enter the operational networks due to the enforced unidirectional flow of data with Data Diode.

OT/IT Networks

Operational network is protected from network-based attacks.

ST Engineering Data Diode enables the **unidirectional transfer of operational data from the operational network to the enterprise network**, while preventing network based attacks to the operational networks.

Creates network separation between key operational systems and enterprise network or the internet.

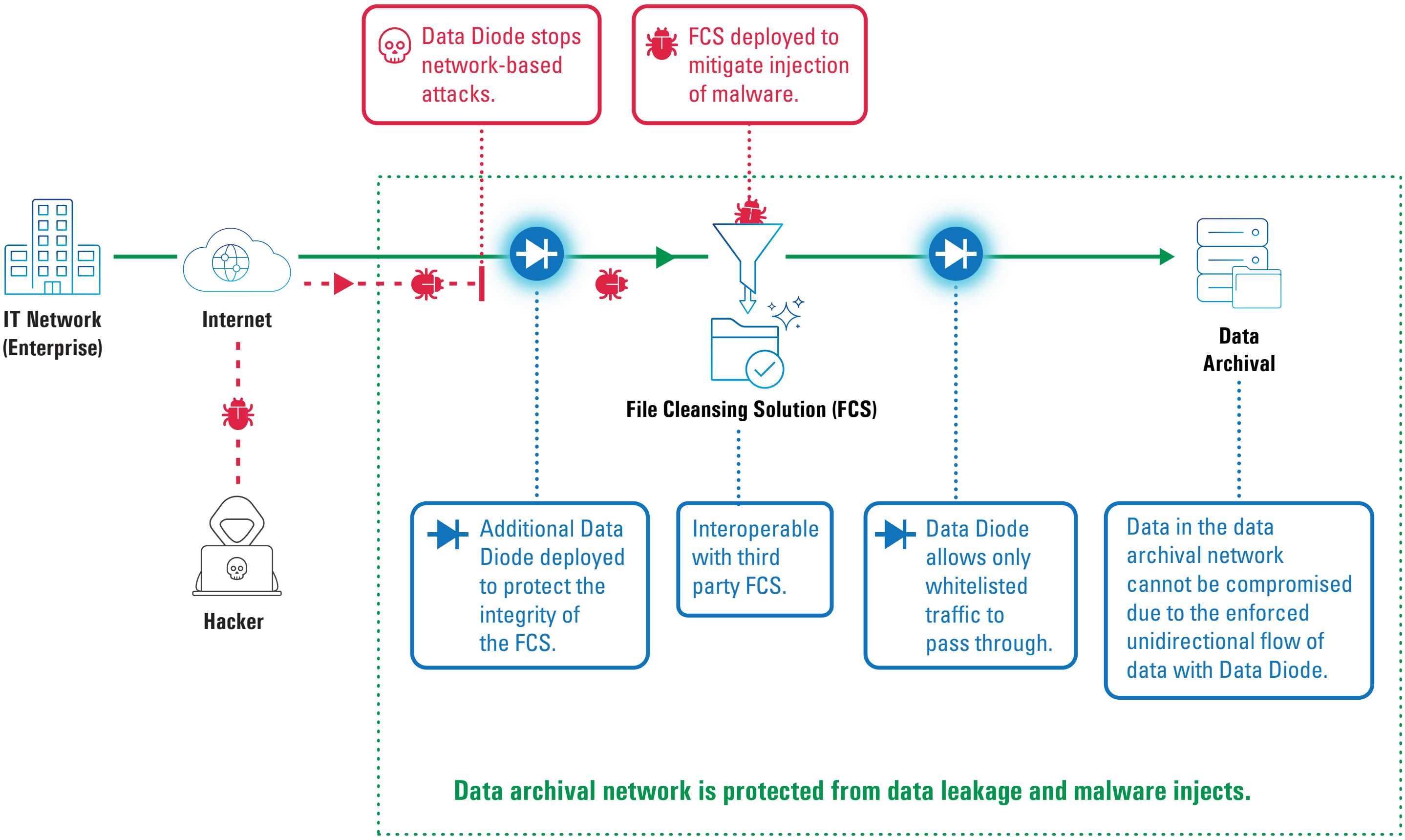
Minimal downtime requirements through high-availability (failover) configuration.

Allows real-time monitoring of all operational systems.

Challenges of

Protecting data archival networks

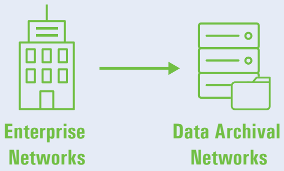
- Secure backup and storage of data, while preventing malware infection of data archival network from the internet and external IT networks
- Protect integrity of files in data archival network
- Ensure compliance with industry security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss



Data Diode stops network-based attacks.
FCS deployed to mitigate injection of malware.
IT Network (Enterprise)
Internet
Hacker
File Cleansing Solution (FCS)
Data Archival
Additional Data Diode deployed to protect the integrity of the FCS.
Interoperable with third party FCS.
Data Diode allows only whitelisted traffic to pass through.
Data in the data archival network cannot be compromised due to the enforced unidirectional flow of data with Data Diode.

Data archival network is protected from data leakage and malware injects.

ST Engineering Data Diode enables the **unidirectional transfer of files to data archival networks**, while preventing data leakage and theft.



ST Engineering Data Diode ensures only whitelisted traffic is allowed to pass through, protecting organisations from data breaches and malicious threats in the manufacturing plants. Files Cleansing Solution can be further integrated to ensure only malware-free files enter data archival network.

Creates network separation between enterprise network (internet facing) and data archival network.

Minimal downtime requirements through high-availability (failover) configuration.

100% prevention of any data leakage.

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

www.stengg.com/cybersecurity

ST Engineering

TRANSPORT / UTILITIES

SAFEGUARD THE CYBERSECURITY OF INFRASTRUCTURE

WITH ST ENGINEERING DATA DIODE

Cyber-attacks on critical infrastructures including aviation, rail transport, water and power plants can have disastrous consequences. If cyber criminals gain access and control over the operational systems of these infrastructures, they can cause major disruptions to daily essential operations, injuries or even loss of lives and shatter the trust of citizens.

186%

increase of ransomware attack attempts globally on the transportation sector since June 2020.

- Check Point Research report

300%

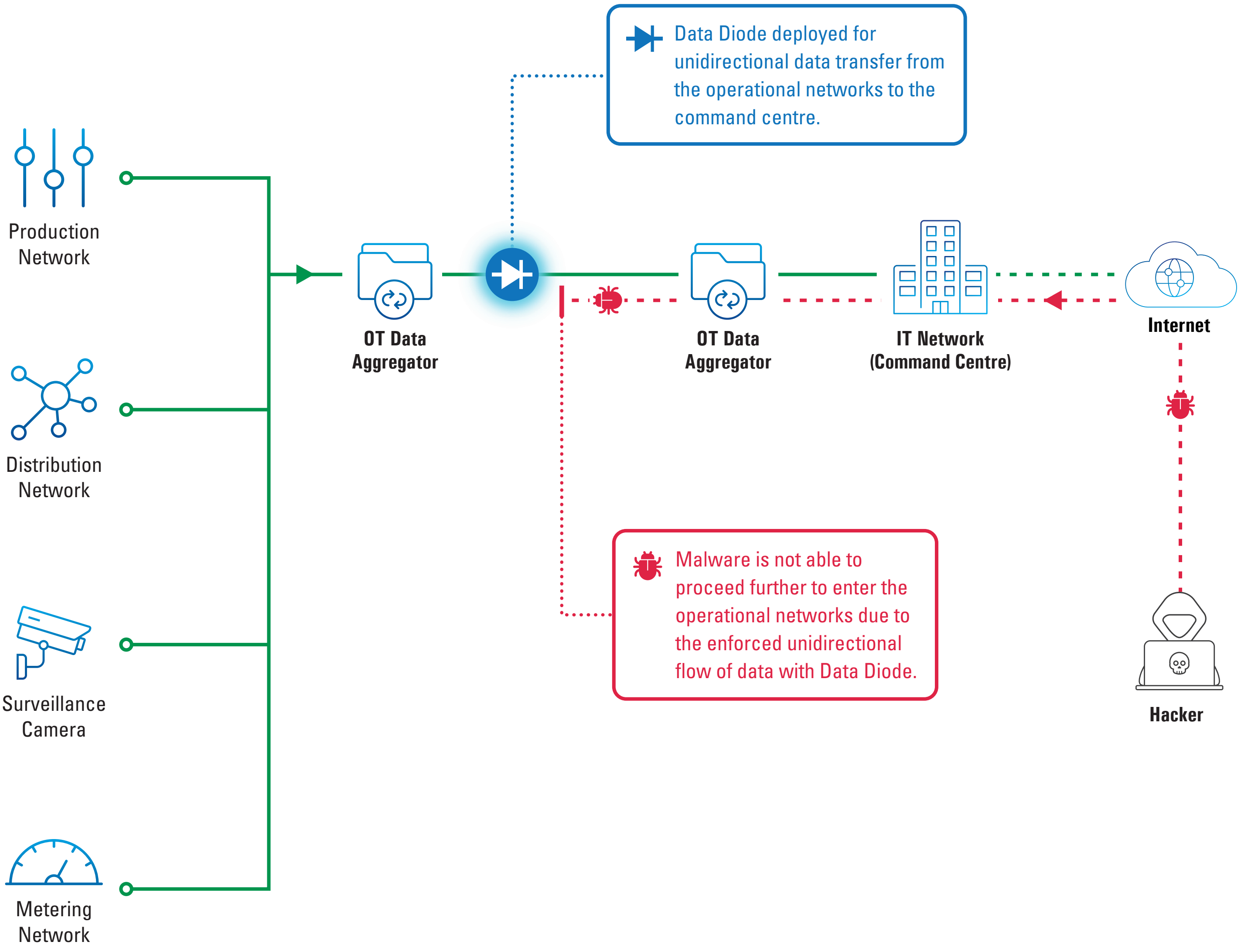
surge in cyber-attacks on IoT (Internet of Things) devices in 2019.

- Forbes

Challenges of

Monitoring operational systems

- Allow real-time monitoring of airport, transport and utilities operations, while safeguarding operation systems against cyber-attacks from the internet and external networks
- Ensure compliance with industrial security regulations (including CC EAL 4+), while providing high end-to-end throughput without data loss

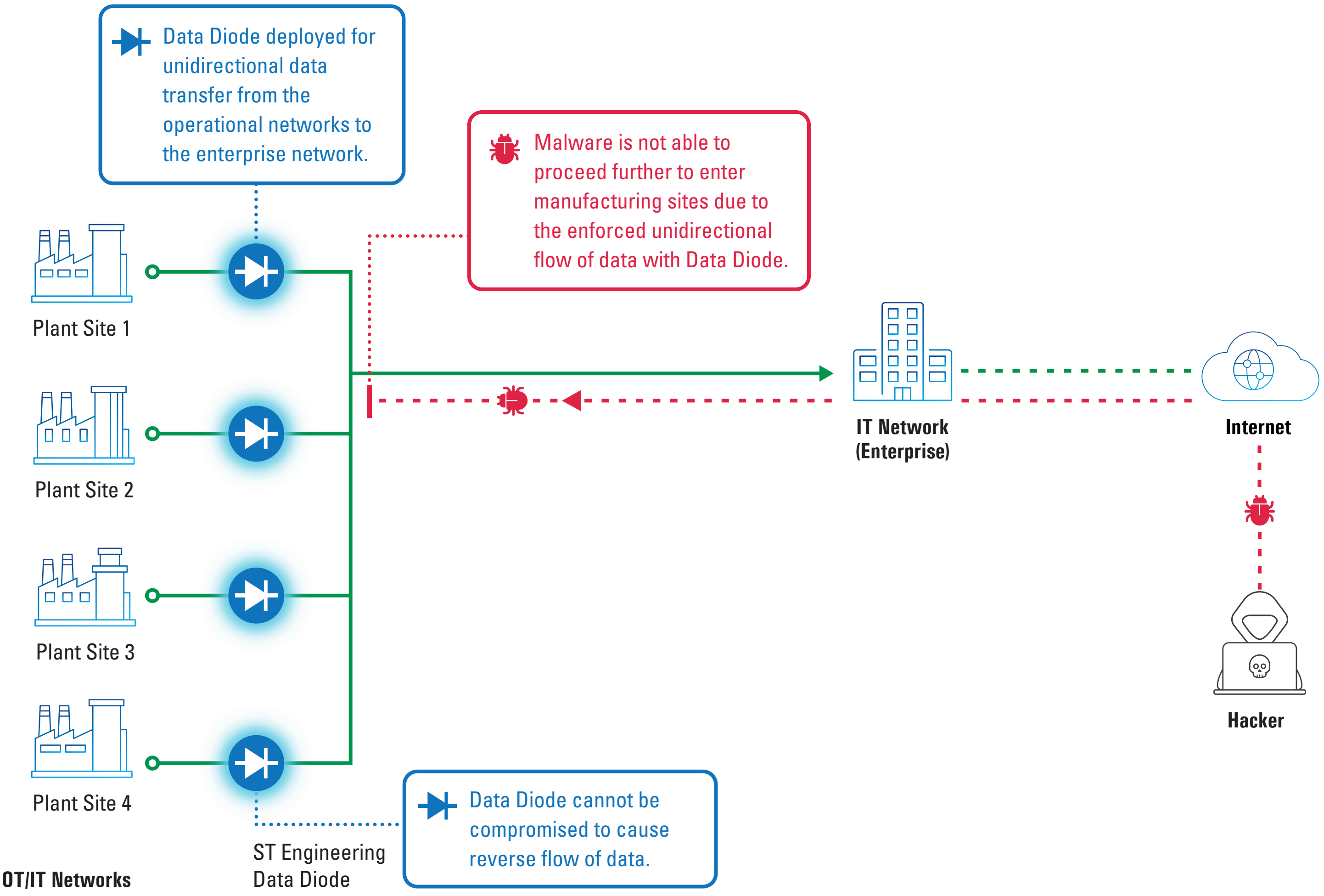


Data Diode deployed for unidirectional data transfer from the operational networks to the command centre.

Malware is not able to proceed further to enter the operational networks due to the enforced unidirectional flow of data with Data Diode.

OT/IT Networks

Operational network is protected from network-based attacks.



Data Diode deployed for unidirectional data transfer from the operational networks to the enterprise network.

Malware is not able to proceed further to enter manufacturing sites due to the enforced unidirectional flow of data with Data Diode.

Data Diode cannot be compromised to cause reverse flow of data.

ST Engineering Data Diode enables real-time, **non-intrusive monitoring of airport, transport and utilities operational systems via unidirectional files transfer or OT data replication** while preventing network based cyber-attacks to the key operational systems.

Creates network separation between key operational systems and enterprise network or the internet.

Minimal downtime requirements through high-availability (failover) configuration.

Allows real-time monitoring of all operational systems.

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

www.stengg.com/cybersecurity