BLACK COMPUTER

Providing Security at Your Convenience

BLACK COMPUTER

SECURITY AT YOUR CONVENIENCE

ST Engineering
Electronics

ONE COMPUTER

DUAL OPERATING SYSTEMS

DUAL NETWORKS

SECURITY AT YOUR CONVENIENCE

ST Engineering
Electronics

What are the biggest cyber fears for enterprises?

What are the employees doing?

Are they exposing themselves to malware threats or social engineering scams? These often lead to unauthorised access of the corporate network and even theft of company data or sensitive information.

Are they posing as insider threats? Whether accidental or malicious, the threat is similar and will cause irreparable damage to the business operations, financial standing and industry reputation of the company.

What is in the corporate network?

Is company data being leaked by a compromised system or by an employee? Are Distributed Denial of Service (DDOS) attacks happening on the company's network or originating from it?

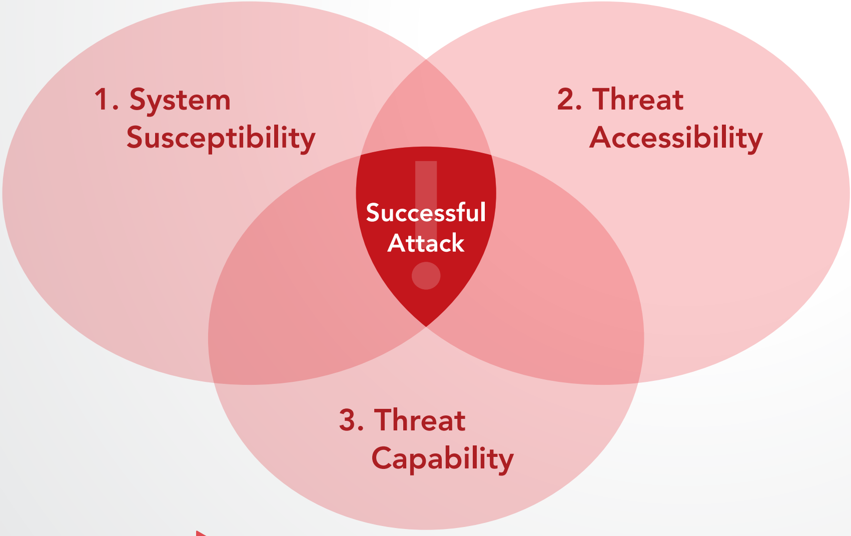
Did you know?

62% of business users report that they have access to company data that they probably shouldn't see.[1]

55% of cyber attacks in 2016 were carried out by insiders.[2]

[1] Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations, Ponemon Institute, August 2016. [2] IBM X-Force Threat Intelligence Index 2017

What are the ingredients of a successful attack?



1. System Susceptibility

The attackers need to learn the value and vulnerabilities of the target.

2. Threat Accessibility

The attackers need to deliver the attack to the system's attack surface, which requires logical or physical access to the target system.

3. Threat Capability

The attackers need to have the resources and skills to pull off the attacks.

What is the best strategy?

In the current cyber threat landscape, attackers are easily bypassing perimeter defence tools such as antivirus and firewalls, leveraging software and plug-in vulnerabilities to infect endpoints and ultimately reach corporate networks. **ISOLATION IS THE BEST STRATEGY.**

ST Engineering Electronics Black Computer is the solution. By separating the untrusted (internet) and trusted (intranet) systems with dual operating systems, it prevents the importing of malware from one network to another.

ONE computer TWO operating systems

Black Computer D100 (Desktop Version)

Black Computer L100 (Laptop Version)

Hardware that Protects against Threats coming from the Internet

The first-of-its-kind in the industry, ST Engineering Electronics Black Computer is one computer with two operating systems. It powerfully leverages hardware defined network isolation to protect against importing malware from unsecured networks and malicious programmes.

The Black Computer filters out 90% of threats. Even if it gets infected, it reduces the cyber attack surface at the endpoint. With a simple reboot of the system, it effectively removes malware from any infected surface.

It is the answer to the most vulnerable part of the computing environment – its endpoints. Time and again, the employee's computer has served as an opened door into the organisation for cyber criminals, it no longer will.

Hardware that Balances Security and Productivity

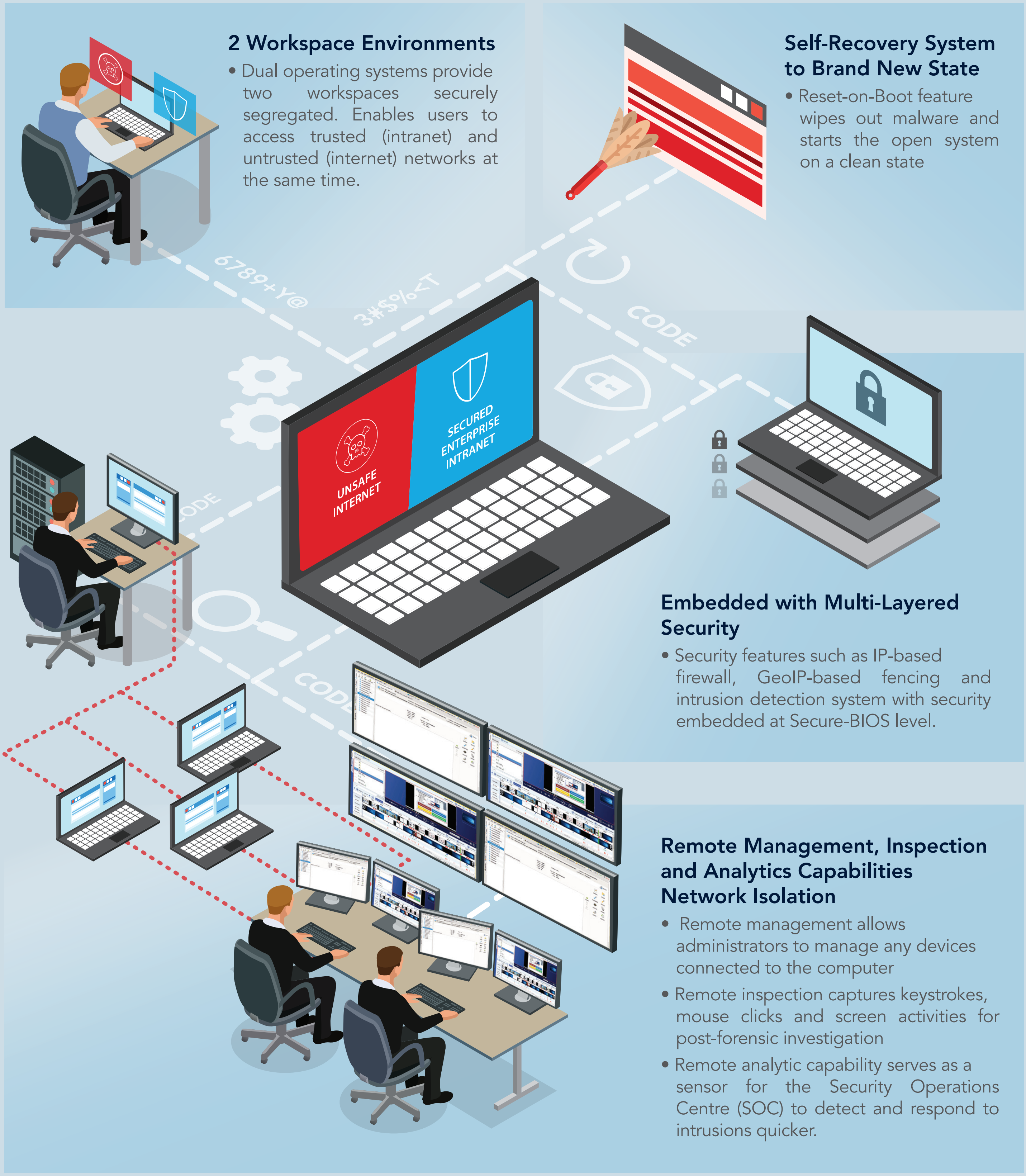
Backed by our deep engineering expertise and indigenous capabilities, ST Engineering Electronics Black Computer provides the critical physical segregation that eliminates the hassle of operating two separate computers. Users can quickly and easily access trusted (intranet) and untrusted (internet) networks at the same time, maintaining security while improving productivity.

Hardware that Protects the Trusted Network and Guards against Insider Threats

ST Engineering Electronics Black Computer strengthens enterprise endpoint security and protects information infrastructure. It enables innovative monitoring of user activity on all computers inside the organisation. Each endpoint serves as a sensor, enabling cyber security personnel to analyse network activity and discover patterns and unusual activity.

Upon any detection of threats, the Black Computer can immediately push down policies from the backend, such as dynamic white listing of USBs, and perform remote forensics from the command centre. Time taken for risk mitigation is significantly reduced.

Fourfold Protection



2 Workspace Environments

- Dual operating systems provide two workspaces securely segregated. Enables users to access trusted (intranet) and untrusted (internet) networks at the same time.

Self-Recovery System to Brand New State

- Reset-on-Boot feature wipes out malware and starts the open system on a clean state

Embedded with Multi-Layered Security

- Security features such as IP-based firewall, GeoIP-based fencing and intrusion detection system with security embedded at Secure-BIOS level.

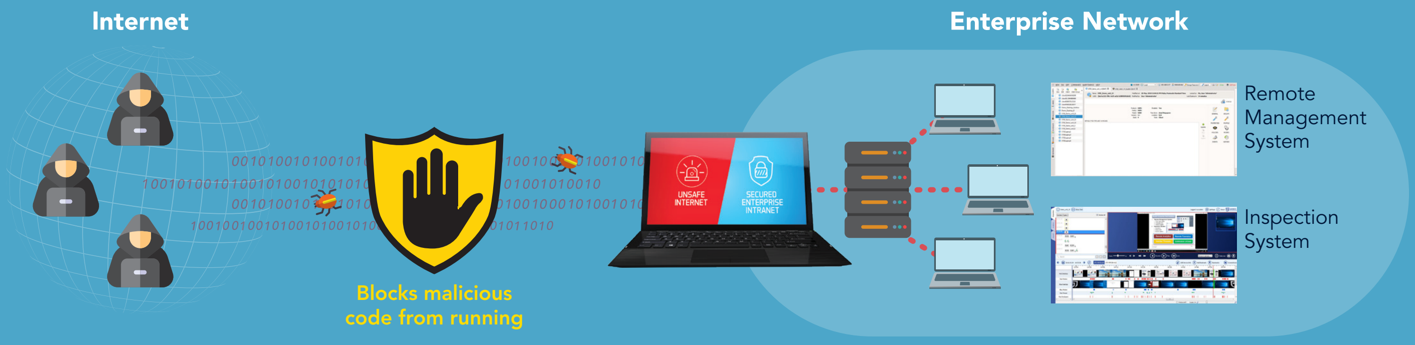
Remote Management, Inspection and Analytics Capabilities Network Isolation

- Remote management allows administrators to manage any devices connected to the computer
- Remote inspection captures keystrokes, mouse clicks and screen activities for post-forensic investigation
- Remote analytic capability serves as a sensor for the Security Operations Centre (SOC) to detect and respond to intrusions quicker.

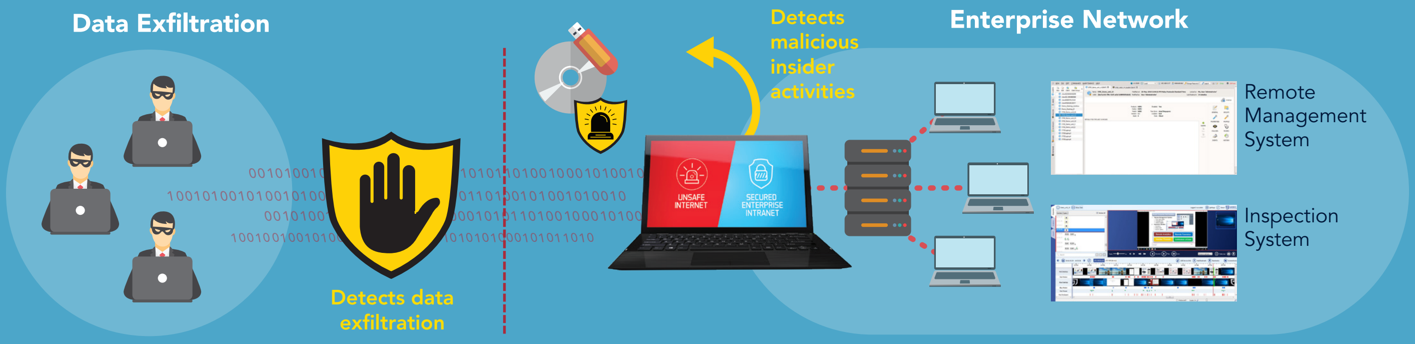
Use Cases

With its segregated workspaces and built-in security features, ST Engineering Electronics Black Computer is the complete solution that covers all threat aspects to provide full protection coverage for organisations.

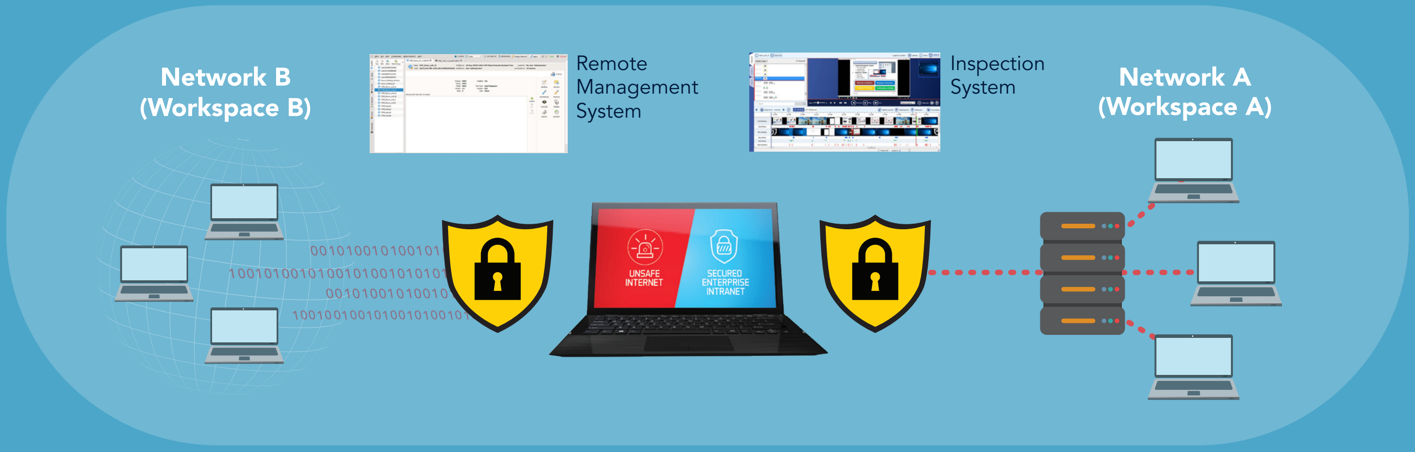
Protecting Networks from Outsider Threats



Protecting Networks against Insider Threats



Protecting Segregated Networks



About ST Engineering Electronics

ST Engineering is a global technology, defence and engineering group specialising in the aerospace, electronics, land systems and marine sectors. The Group employs about 22,000 people across offices in Asia, the Americas, Europe and the Middle East, serving customers in more than 100 countries. Its employees bring innovation and technology together to create smart engineering solutions for customers in the defence, government and commercial segments. Headquartered in Singapore, ST Engineering reported revenue of S$6.62b in FY2017 and it ranks among the largest companies listed on the Singapore Exchange. It is a component stock of the FTSE Straits Times Index, MSCI Singapore and the SGX Sustainability Leaders Index.

The Electronics sector specialises in the design, development and delivery of Information and Communications Technology (ICT) products, solutions and services addressing the needs of Smart Cities for Connectivity, Mobility and Security. Its deep technological and engineering expertise straddles business domains in Rail & Road engineering, Satellite Communications, Public Safety & Security, Cybersecurity, Artificial Intelligence, Training & Simulation, Managed Services and Defence C4ISR. It has presence in more than 30 global cities across North America, Latin America, Europe, Africa, the Middle East, China, India and Southeast Asia. For more information, please visit **www.stengg.com**.

ST Engineering
Electronics

ST Engineering Electronics Ltd.
100 Jurong East Street 21, S(609602)
T: (65) 6568 7118 Fax: (65) 6568 7226
E: infosec.mktg@stengg.com W: www.stengg.com