

RemoteKill®



GDS Transnational Enterprise Laptop Tracking and Security

<p>1 device in 1 location GX9472 Geolocation source Wi-Fi Triangulation Public IP: 24.130.84.37</p>	<ul style="list-style-type: none"> JG893BFG26PNCMC93BF KBH29HFKD7H340VH327 GF93GV89H29X90NB97M MV90G30JN75TGEI8V7P 	<p>*** SYSTEM LOCKED *** Enter Password:</p>
<p>Real-time Tracking and Geolocation</p>	<p>Remote Kill™ Emergency Data Encryption</p>	<p>Remote Kill™ Hard Drive Lockout</p>

Real-Time Tracking and Anti-Theft Protection

EXO5 with Remote Kill® provides real-time device tracking and strong defenses against data theft. This cloud-based solution enables IT administrators to track, encrypt and disable computers that are lost or stolen, ensuring sensitive data doesn't get into the wrong hands.

Features

Real-Time Platform

Unlike existing solutions that check-in once a day, EXO5 with Remote Kill™ works in real-time, allowing for immediate response to compromised devices.

Next-Gen Tracking and Geolocation

EXO5 Wi-Fi triangulation can track devices to within 25 feet. Unlike older GPS technologies, it works indoors and in high-rise urban areas.

Hard Drive Lockdown

Remote Kill® disables lost or stolen laptops with boot sector encryption and lockout.

Out-of-Band Emergency Encryption

Following a theft or loss event, Remote Kill™ encrypts selected files and folders. Out-of-band encryption protects data from even formerly authorized users such as terminated employees.

Enterprise Interface

The EXO5 web application can support up to 1,000,000 devices within a single account, with the ability to delegate Remote Kill authority to groups and managers.

Works both Online and Offline

Remote Kill® provides instant data protection for devices that connect to any internet connection. Offline Remote Kill™ provides a "curfew" setting for devices, automatically encrypting and locking laptops that fail to connect to a network connection with a set period of time.

US Government-Standard Security

The EXO5 agent and administration console implement SSL protocols in combination with

"A laptop is stolen every 53 seconds."

"50% of all mobile device users store passwords, personal info, and credit card details on their devices."

"Average cost from laptop loss is \$53,000."

"Stolen DuPont laptop containing the recipe for Kevlar®, obtained by Chinese competitor, results in over \$1.5 Billion in annual lost revenue."

RemoteKill®



1024-bit RSA key-protected communications. Your data is always private and secure.

Benefits

"Average cost of recovering from a single corporate data breach in 2010: \$7.2 Million."

"Well-implemented security policies reduce laptop theft by 85%!"

Aggressive and Proactive Information Security

Remote Kill® data encryption and hard drive locking are reversible, enabling IT staff to aggressively disable devices at the first sign of trouble. Devices that are later found can be quickly re-enabled and returned to service.

Endpoint Protection

By monitoring its assets consistently, your organization protects itself from a critical security risk: the loss of company PCs containing VPN profiles, saved passwords, and other sensitive data that could be used to compromise your infrastructure.

Cost Savings

By preventing losses and improving resource allocation, Remote Kill® dramatically reduces costs associated with unnecessary purchases and replacements.

Stay Out of the Headlines

Losing customer or sensitive data can quickly lead to negative news exposure. Remote Kill® protects your organization from the negative publicity and significant liabilities of data theft.

Protect Proprietary and Privileged Information

Customer databases, offline e-mail storage, confidential documents – they're all examples of data that could spell disaster in the hands of a competitor, legal adversary, or former employee. Remote Kill® ensures that a lost laptop doesn't lead to lost secrets.

The Cloud Advantage: Low Cost and Rapid Deployment

The EXOS cloud-based service saves you from hidden costs - most deployments can be completed in a single afternoon. There are no servers to set up or maintain, and installation of the client agent requires no end-user interaction. All administration features are accessed with a web browser. Pay only for what you need, without any setup or maintenance fees.

For More Information
 Contact
info@CampusSafetyProducts.com
 to find out how you can achieve
 world-class IT asset controls.

