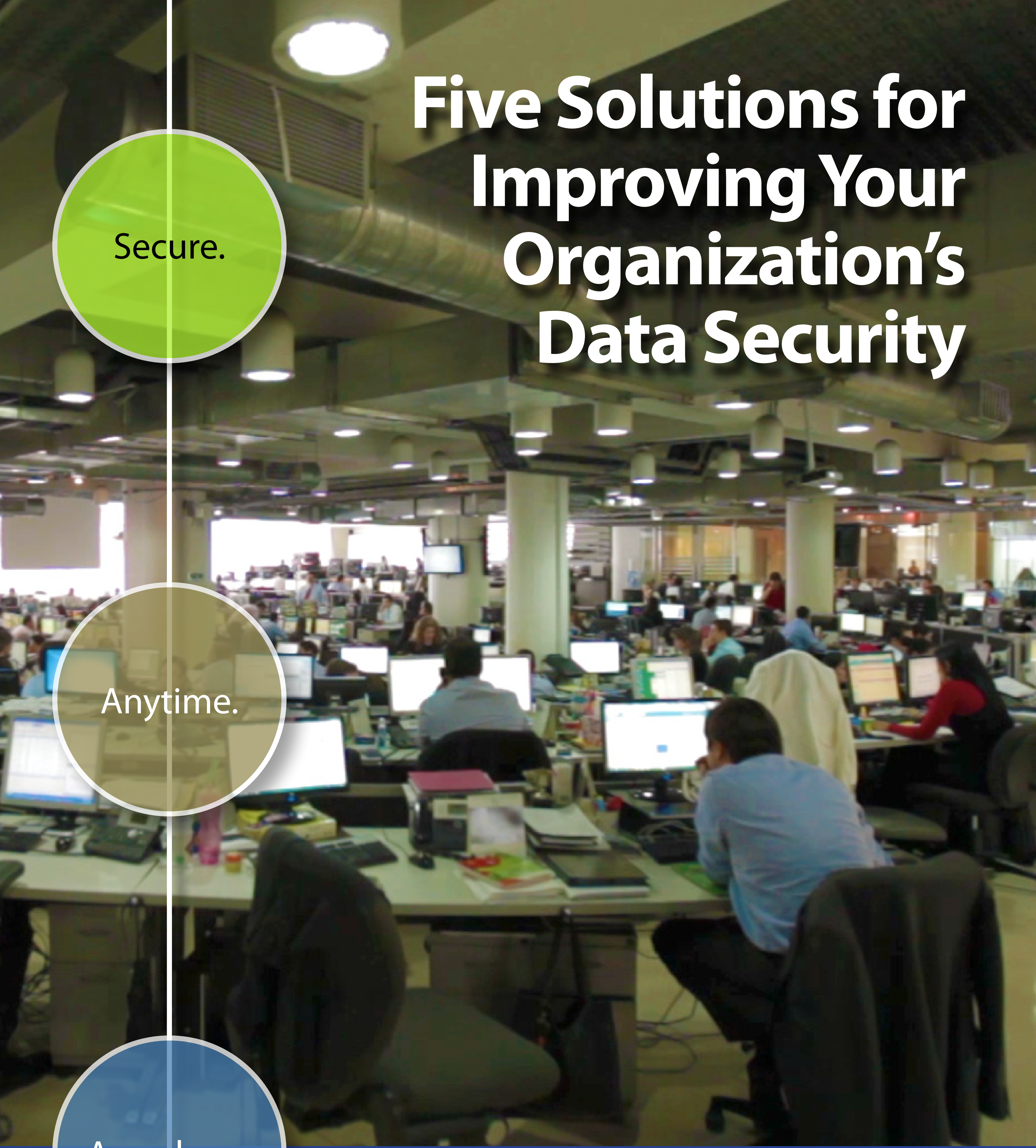
Five Solutions for Improving Your Organization's Data Security



KANGURU™

Secure. Anytime. Anywhere.

Five Solutions for Improving Your Organization's Data Security

Introduction

It's a sobering fact that in this day and age, hackers want your information, and are willing to go to great lengths to get it. The stakes are high, and every company struggles to keep up with data security in some form or another. With new technologies rolling out every day, and new ways to access data on a global scale, IT Administrators face a daunting task. Company data is the most important asset for any organization, and for hackers, it's the new gold rush.

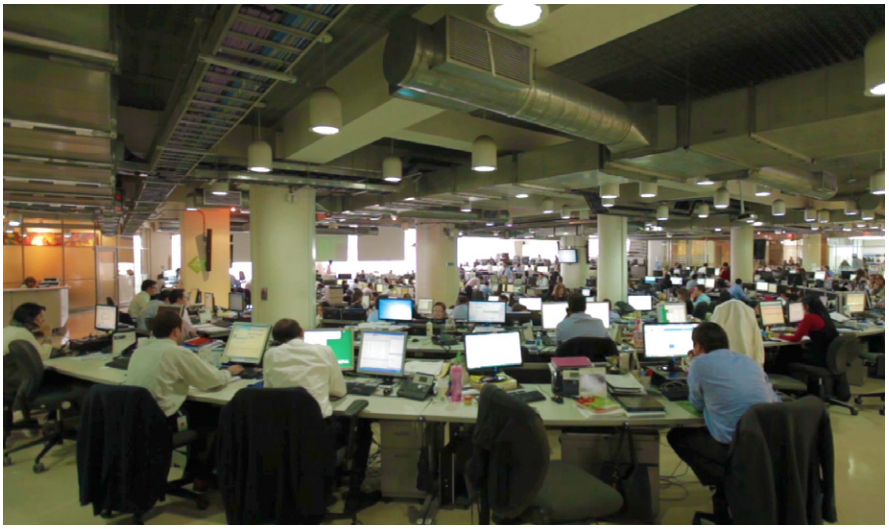
The threats can come from both sides - from outside of the organization, as well as from the inside. Employees often have other matters in mind besides data security which can make it difficult to implement best practices and enforce strong security policies. Staff will usually choose the path of least resistance, seeking quick convenience and volatile work-arounds over what often might be considered "cumbersome" security policies. It can be difficult to enforce data security and compliance with security regulations when staff may be unable, or unwilling to follow standards.

Developing good security policies that automatically protect data is the best way to ensure the organization's data remains safe from prying eyes, as well as careless employees. With the right security measures in place, supervisors can immediately see results that not only greatly reduce the risks, but make their jobs a whole lot easier with options that protect data automatically.

Five Ways You Can Improve Your Organization's Data Security:

- Create a Company-Wide Security Mindset
- Enforce Secure Products that Encrypt & Protect Data Automatically
- Remotely Manage Your Organization's Secure USB Drives Around the World
- Protect Your Network Infrastructure from Malware, Viruses and Data Breach with Cloud-Based Endpoint Security
- Enforce Only Trusted Secure Firmware USB Devices to Protect Infrastructure from Potential Third-Party Malware Attacks

IT Administrators and managers may notice problems immediately within the organization, and may begin feeling overwhelmed with trying to manage and protect all of the organization's data assets. The good news is that by finding the right scalable and flexible security solutions to meet the present as well as future needs, the right solution will grow and flex with the company, without accumulating enormous additional costs. With strategic and well-placed steps made over time, organizations can see immediate improvements to their data security.



1 Create a Company-Wide Security Mindset

This is often easier said than done. Although it's easy to say in theory, this may be a difficult task to implement. However, without having the right people on board, putting any policy in place will simply hit a brick wall. The people most invested in the success of the company need to have the right mindset first about how to keep information safe before best practices can be implemented. Company data is the most important asset for any organization, and executives need to realize that a breach of that data could be detrimental to the business.

For larger companies, it is often more difficult to change company culture, because there might be a multitude of bureaucratic hoops to jump through. Open communication, and dedication is the key. Don't be discouraged when executives push back stating concerns with costs or that it might be too labor-intensive. Demonstrate the risks objectively, yet firmly, and help them realize that not investing in good data security could be a huge gamble when faced with the risks and potentially crushing costs of a data breach. *(See Exhibit A to make a strong case.)* Assure them that there are options available that can be very cost effective, as well as easy to implement, that will greatly reduce or eliminate those risks.

Remind them that the costs associated with the alternative - a data breach, malware attack, or virus, could be debilitating to the organization. Exhibit A is a chart of just a few of the costs involved with a nightmare scenario:

Exhibit A: The Potential Cost of a Data Breach

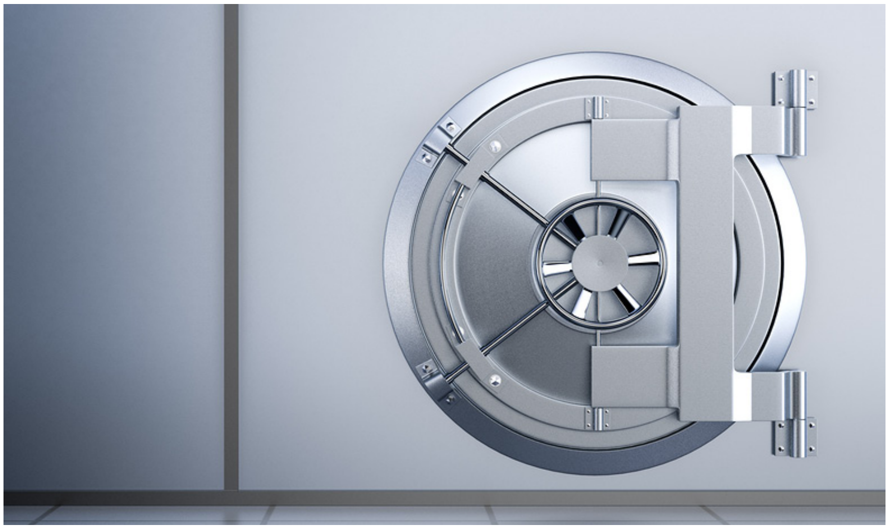
FINES	For organizations that must comply with specific security standards, stiff fines could be imposed that might cost the company millions. In some cases, fines could be instituted *per record*, which would add up enormously when you consider just one unencrypted USB device could carry hundreds of thousands of records.
EMBARRASSING CLEAN-UP, INVESTIGATIONS, COURT COSTS	If breached records included financial information or personal information of clients and customers, the clean-up effort could become colossal. Besides the initial embarrassment, the clean-up could involve: • An apology letter sent out to every client or customer • Free Credit card / bank account protection for every client (paid for by you) • Lost business due to all attention being given to dealing with clean-up effort • Frustrated employees / staff from dealing with angry customers - low morale • Negative press, news outlets, Google searches might eat up the incident for weeks or even months • Endless investigations could cost the company millions and go on for years • Relationships would have to be restored and new trust developed • Endless litigation and court battles could go on for years, between you and customers, clients, vendors, or any hackers who may have been caught.
IRREPARABLE DAMAGES, REVAMP OF THE BUSINESS	If the breach included sensitive company information, an overhaul of the way you do business could be in order. This could essentially be a "start over" with new business strategies, vendors, customers, employees, markets, or sales teams. Your unforgiving customers may never come back, and you will have to develop new trust relationships with clients. Even worse, if the incident created irreparable damages, the cost to fix could be insurmountable.
FOLLOW-UP	At this point you will end up installing new data security defensive technologies anyway after the fact, (which your customers would remind you that the measures should have been installed in the first place.)
RESTORE REPUTATION	Present and future business could suffer from a tarnished reputation. Gaining new business, and retaining older clients will be a difficult struggle for years to come. Your organization will have to develop new marketing strategies, a new message, and potentially a whole new rebranding campaign.

You should honestly ask if any of the above scenarios are worth the risk. By not installing safety measures in data security now, an organization could leave itself vulnerable to any of the above potential scenarios. Is saving a few dollars by not installing security measures now really worth the risk?

Middle management, especially may have difficulty in trying to get different departments on board with vastly different skill sets. However, when staff are left to their own devices, the doors often open wide for hackers to get in. Start by adapting better habits with day-to-day habits within your area, and then move on to other major players in the company. Invest in open-minded communication and open dialogue with decision-makers, and demonstrate the importance of protecting the data of the organization.

It's important to note that even if executives are open-minded about implementing good security policies, staff and employees may not be so open. When making an investment in technology, you also need to make the investment in those who use that technology. Since data security is usually the last thing on their minds, they will often seek the path of least resistance, choosing ease and convenience over protecting the data they work with every day. You will need to help them understand why it is so important and ensure that they are aware of how high the stakes really are. A good place to start is with good data security training. Listen to their concerns and assure them that policies are in place to protect data as well as themselves. There are solutions available that will not sacrifice the convenience of working from day to day. Security policies are NOT unnecessary, or a waste their time. Help them understand that the importance of data security is paramount to the success of the organization, and could even protect them from making a terrible mistake with the company data, the most important asset.

Security is also a team effort. This is especially important when one person is out for a day or if someone quits unexpectedly, because too many major errors are caused when daily routines are thrown off. A company with team-oriented data security ingrained in every step will be better prepared to handle situations from becoming a catastrophe.



2 Enforce Secure Products that Encrypt & Protect Data Automatically

Working with data day in and day out, it's easy for employees to put security on the backburner. Don't expect staff to make security a high priority or assume they are protecting data when working with sensitive company information. Chances are more likely they are not. By making encryption automatic, employees can adapt to security policies much more comfortably when there are no cumbersome tasks or long instructions. When automatic structures are in place, data is automatically encrypted and protected, and can take the responsibility off of the employee. Staff may react to sudden changes, so implementing small, systematic changes can make enormous and immediate improvements to the organization's overall security.

USB Security

A number one sea change that can go a long way in protecting data for a high-security environment is by enforcing the exclusive use of hardware encrypted USB drives. There is no better way to protect data from hacking than with locally-stored data. In addition, you could implement strong remote management for your organization's secure USB drives and administrate their whereabouts anywhere in the world.

USB VS. Cloud Storage

Some news stories have frightened organizations into thinking that USB is vulnerable, and it could be, if highly-sensitive information is carelessly stored on non-encrypted USB drives, or if untrusted thumb drives are haphazardly allowed on the network. As a result, fear has caused certain organizations to go so far as to ban or block the use of USB ports altogether- essentially throwing the baby out with the bathwater so to speak. However, the fear is misplaced. By removing the convenience of USB outright, it only exacerbates the problem because then the only alternative is to share business information across the world wide web - which opens up a whole new set of vulnerabilities.

Any data on a shared network is vulnerable to hacking, and relying on cloud storage for storing information can open up multiple avenues for cyber-criminals. Where is the data actually being stored? Does one really know who is accessing it? The evening news is filled with stories of data being compromised almost every day over shared internet channels.

Locally-stored and password protected data is the best way to know exactly where the data is, who has access to it, and with good management, it cannot be compromised.

The Mistake of Using Unencrypted USB in a Secure Environment

Because USB flash drives are convenient, one of the biggest mistakes an organization can make is to allow employees to use non-encrypted memory sticks, or flash keys to store sensitive company information when they should be using **AES hardware encrypted, secure USB drives**. Unencrypted USB drives have their place for transferring information that is not of a sensitive nature, but they should have no place in an organization where security is a vital component. Hardware encrypted USB drives are the best way to protect data because it is physically contained within the cryptographic chip itself. Secure flash drives contain the data inside the drive in your hand under password protection, providing a confidence that you simply can't get anywhere else. Furthermore, if the flash drive were ever lost or stolen, the encryption components prevent the information from being accessed or compromised in any way.

Hardware encrypted, secure USB drives can prevent the data from being accessed without the consent of the owner, and remote management of secure USB drives can prevent the owner from becoming an agent for a data breach.

A hardware encrypted USB flash drive that is remotely managed is even better for protecting company data. Hardware encrypted, secure USB drives can prevent the data from being accessed without the consent of the owner, and remote management of secure USB drives can prevent the owner from becoming an agent for a data breach.

With hardware encrypted USB drives, data is automatically secured through the use of AES hardware encryption and password protection. Depending on the complexity of the cryptographic module, the level of defense can be from commercial encryption measures, all the way up to highly-certified, military grade, brute-force protection.

Software Encryption VS. Hardware Encryption

Some organizations use software encryption to encrypt data on USB flash drives. However, software encryption can leave something to be desired. Software Encryption is software based, where the encryption of a drive is provided by external software to secure the data. Software encryption options are available on the market as a cheaper alternative to hardware encrypted drives, but the disadvantages tend to outweigh the benefits. It often requires numerous updates to keep up with hacking techniques, could be quite slow, and may require complex driver and software installations. Software encryption also may not provide the full security that businesses are expecting, to keep sensitive information from falling into the wrong hands. Though software encryption is better than having no encryption at all, it may still be vulnerable to user error, leaving data vulnerable to fall through the cracks and be susceptible to potential thieves. Since software encryption requires users to follow certain procedures in order to secure the data, users may forget - or choose to ignore certain aspects of the encryption process.

With hardware encryption on secure USB drives, the AES encryption process is handled automatically, built right in with a small chip inside the drive itself. Once original data is encrypted, it becomes undecipherable in the background and is locked away under encrypted storage within the drive. If a thief were to try to gain access to the data without the password, the attempt is by all practical means impossible. But once the user enters their private password, the data is decrypted instantly, and made fully available to the user.

Finding Hardware Encrypted USB to Fit the Specific Needs of Your Organization

There are a variety of hardware encrypted USB options that ensure solid security for any level organization, from military and Enterprise, to energy, utilities and SMBs. However, there may be better solutions - one preferred over another, depending on the specific needs of your organization. For example, some secure USB drives contain password keys directly on the drive itself, but this could be cumbersome, slow, and get dirty or stop working properly over time. Also, someone looking over a shoulder could easily see the password being keyed in, making the process vulnerable.

Other secure USB drives plug-in as any typical USB device normally would, but then opens up a secure password window on the computer screen in order to allow access to the secure partition. Once the correct password requirement is met, the encrypted device becomes accessible. This option makes it easy for the user to access their data quickly and conveniently by plugging in the drive into any USB port, entering the password securely on screen, and gaining immediate access to the drive's secure partition.

There are several options to choose from, but as with most products, some are expensive and others are more cost effective. Expensive may not necessarily be the best option, but you also don't want to skimp on security. Often the costs are associated with the capacity size of the drive, along with the level of encryption you are looking for. For example, a commercially-designed encrypted drive with 16GB capacity will be much less expensive than a 128GB capacity encrypted drive that is FIPS 140-2 Certified for military grade security with built in brute-force protection.

Kanguru Defender® AES 256-Bit Hardware Encrypted USB Drives

AES 256-bit
Hardware
Encryption
KANGURU DEFENDER 3000™ USB 3.0 AES Hardware Encryption
KANGURU DEFENDER 2000™ AES Hardware Encryption
KANGURU DEFENDER ELITE300™ USB 3.0 AES Hardware Encryption
KANGURU DEFENDER ELITE30™ USB3.0 AES Hardware Encryption
KANGURU DEFENDER ELITE200™ AES Hardware Encryption
KANGURU DEFENDER HDD300™ USB 3.0 AES Hardware Encryption

A great solution to augment the security of your organization is to create a company-wide policy committed to the exclusive use of secure, hardware encrypted USB devices. **Kanguru Defender secure USB drives** provide a variety of encryption flexibility and operate with AES 256-Bit hardware encryption built inherently into the drives. All Defender devices plug in conveniently as any typical USB device. A password window opens on the computer screen with hidden characters, allowing the user to enter the password privately. There is also an option to use the dropdown virtual keyboard if a threat of keylogging software is suspected on the host computer.

Kanguru Defender hardware encrypted USB drives have select features which provide flexibility, and the best options can be determined by the specific needs of your organization:

- **Rugged, high-quality alloy housings and tamper-proof features**
- **Physical write protect switch - perfect for using read-only configuration to assess a possible virus-infected computer**
- **FIPS 140-2 and Common Criteria encrypted drives for full compliance with security regulations in high-security environments**

Kanguru Defender secure USB drives help organizations easily comply with high-security regulations, maintain automatic encryption for data and provide convenience for staff to work without cumbersome, time-consuming security procedures getting in the way.

They are manufactured with the highest-quality components and are **TAA Compliant**, yet their prices are comparable or even less expensive to similar security products on the market.

Exhibit B: Built-in Safety Features of Kanguru Defender® drives:

MULTIPLE PASSWORD ATTEMPT DISABLING	With Multiple Password Attempt Disabling, if an attempt were made by a third-party to try to gain access to the drive by entering multiple password attempts, the drive would be disabled after a certain amount of tries. These settings can be changed by the owner as desired.
AES 256-BIT HARDWARE ENCRYPTION Learn More	AES 256-Bit Hardware Encryption provides the highest level of security. AES stands for Advanced Encryption Standard and is a specification standard by the National Institute of Standards and Technology (NIST) for the security of data. AES is a widely recognized and adapted cryptographic module used in the U.S., Canada and worldwide by military, government, financial institutions, and organizations all around the world as the standard for encrypting and decrypting of data.
ON-BOARD ANTI-VIRUS PROTECTION Learn More	Every Kanguru Defender flash drive, hard drive or solid state drive comes with fully-integrated, on-board Anti-Virus Protection to protect from potential viruses on the host computer. The anti-virus consistently scans the drive in the background, adding a layer of defense to protect your files from viruses, malware or spyware.
TAMPER PROOF PROTECTION	Most Kanguru Defender secure USB drives have a tamper-proof design to prevent the drive itself from being compromised. Access to the cryptographic chip through the casing is protected with an epoxy compound that is water resistant and prevents physical access to the chip. Any subversive attempt to remove the epoxy compound destroys the flash chip, rendering it unusable and inaccessible.
SELF-SERVICE PASSWORD MANAGEMENT Learn More	Self-Service Password Management is a great new feature by Kanguru, providing users with the ability to securely reset their password in the event it is ever forgotten.
CUSTOMIZATION/ ENGRAVING Learn More	All Kanguru Defender drives can be customized with engraving features for logos, serial numbers, contact information, etc. In addition, unique electronic identifiers read-only configuration and pre-loaded data features are some of the other customization options available for Defender secure USB drives.

3 Remotely Manage Your Organization’s Secure USB Drives Around the World

Remotely managing actions and data assets of the organization is an administrator’s ultimate tool for ensuring data security and protecting information. Whether your secure USB drives are across the globe, or the next room over, remote management can ensure that the drives are doing the job they were intended to do, and manage compromising situations if they arise. IT Administrators can manage actions and company data property from a central cloud console location in case something goes wrong, and take immediate action to prevent and report on potential risks.

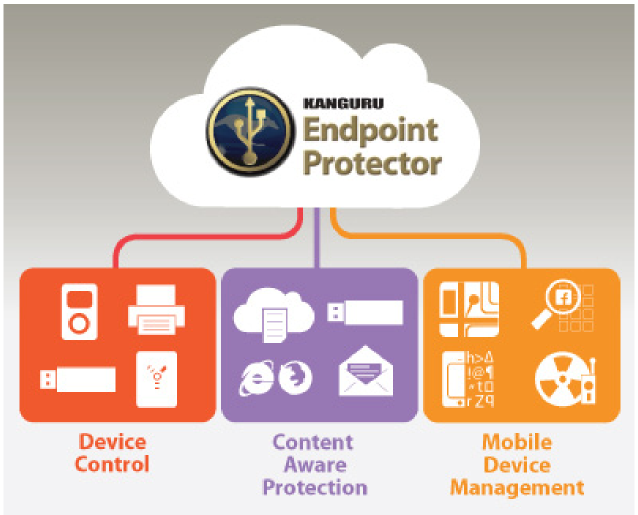
Kanguru Remote Management is a great tool for any organization that wishes to oversee the whereabouts of their important information, and can ensure that the data is protected on secure, hardware encrypted USB drives. The built in AES 256-Bit hardware encryption protects the data from being accessed without the consent of the owner, and remote management of the secure USB drives prevent the owner from becoming an agent for a data breach.

Exhibit C: Kanguru has several great remote management tools available for administrators, depending upon their specific needs:

KRMC CLOUD Learn More	KRMC-Cloud™ (Kanguru Remote Management Console™) is the perfect, easy-to-use solution for organizations that need a single administrator to watch over the company's secure, encrypted USB assets around the world. KRMC Cloud can be implemented without delay to immediately start reaping security benefits. KRMC Cloud is hosted by Kanguru's Enterprise-level, international cloud-hosting platform.
KRMC CLOUD PRO Learn More	KRMC-Cloud PRO is for larger organizations who may require more administrators to monitor certain assets. Organizations with KRMC-Cloud Pro can delegate certain tasks to several other administrators under one-super administrator, and restrict certain permissions as needed. KRMC Cloud is hosted by Kanguru's Enterprise-level, international cloud-hosting platform.
KRMC ENTERPRISE Learn More	KRMC-Enterprise is a self-hosted platform for enterprise organizations who wish to remotely manage secure USB assets from their own server.

Since no data on the drives can be seen by the KRMC management interface, IT Administrators can concentrate on simply managing the assets, while the staff in possession of the individual secure drives can work securely with the data under strict security policies. This provides organizations with a perfect balance of security between the user and the administrator.

4 Protect Your Network Infrastructure from Malware, Viruses and Data Breach with Cloud-Based Endpoint Security



Having an exclusionary security policy in place of only allowing hardware encrypted USB drives is a great start, but if just one curious staff member finds a rogue flash drive on the street and plugs it into your unguarded network, the potential for a malware attack could be disastrous. That's where Endpoint Security comes in.

With Endpoint Security, organizations can further protect their network infrastructure with strict policies that actually prevent certain devices or actions from taking place which could be harmful to the company.

One only has to go so far as to review the story of Edward Snowden, who leaked classified information from the NSA, allegedly with the use of sneaking in a thumb drive and pulling off sensitive information. Just one rogue memory stick could leak years of historical data, secrets, or the personal information of your biggest clients, and haunt the organization for years.

A well organized Endpoint Security structure will enforce strong security policies, by forcing users automatically to use only specific product types, or even brands of devices that you allow, maintaining full compliance with security regulations. By locking down the network and creating usage scenario restrictions, you as the administrator take back control once again over USB devices, mobile devices, internet content traffic, and content awareness across your network. There are multiple parts to Endpoint, but they essentially all do the same thing:

- **Develop strong security rules and policies as the administrator**
- **create restrictions for what can and cannot be plugged into the network**
- **Monitor, stealth reporting or halt specific actions based on your security criteria**

Kanguru Endpoint Protector

Kanguru Endpoint Protector is a 100% cloud-based endpoint security solution, so it can be immediately implemented by organizations large or small without the need for an expensive centralized server installation. Endpoint Protection is the perfect solution to securing the company's infrastructure. With Kanguru Endpoint Protector, there are three powerful modules to choose from, which can either be used independently of each other, or together to form a dynamic, comprehensive solution.

DEVICE CONTROL Learn More	Manage the activity of USB and other portable storage devices and enforce strong security policies to protect vital data and the health of the network.
CONTENT AWARE PROTECTION Learn More	Ensure sensitive data does not leave the network whether copied on devices, through applications, online services, email, the clipboard or even as screen captures.
MOBILE DEVICE MANAGEMENT Learn More	Gain full control and detailed monitoring of mobile devices and make sure data is safe at any time and at any place it is carried, while keeping pace with the BYOD trend.

Endpoint Protection provides today's system administrators of BYOD environments, a strong, all around security solution to protect their managed environment from all kinds of threats. The rapid adoption of portable storage devices, easy-to-upload Cloud based storage services like Google Drive, Dropbox and Microsoft OneDrive, and the variety of smartphones being used in corporate environments make for a highly-complex environment for a system administrator to protect, making it difficult to keep confidential data from getting lost or stolen in the shuffle.

Using the easily deployable Kanguru Endpoint Protector, administrators can minimize potential risks of data loss and data theft, conveniently managing the mobile device fleet from a single centralized online console from anywhere, at any time.

- **Easily lockdown computers to support only authorized devices**
- **Scan MS Word files, PDF files, emails, web links, clipboard, screen captures and other common content types for sensitive information**
- **Prevent copying of corporate IP out of your network**
- **Enforce smartphone and tablet policies for all employees using their own handheld devices in the corporate environment**
- **Centrally monitor and audit managed devices for any rule violations**
- **Choose from options like stealth monitoring or outright denying any violations based on perceived threat level**
- **Create and apply policies at organization (company) level, group level, computer level, or user level**
- **Support remote employees with Offline Code to temporarily allow rule bypass in cases where an Internet connection is not available**
- **Easily export audit logs to .csv files for import into Excel or your own corporate auditing system for further processing**

5 Enforce Only Trusted Secure Firmware USB Devices to Protect Infrastructure from Potential Third-Party Malware Attacks

Part of migrating a culture to that of more awareness of data security culture means understanding and preparing for the next level of attacks. The next potential arsenal in a hacker's quest is using people's curiosity or the convenience of USB to infiltrate an organization with malware. For instance, experts have seen that thieves may find a way to manipulate the firmware of a standard USB device to introduce destructive malware and bring down the grid of an organization. They call this phenomena "badUSB".

In August of 2014, security researchers revealed a potential threat to USB technology known as "badUSB" at a Black Hat event, arguing that any USB device including a webcam, a computer mouse, a keyboard or a flash drive from an untrusted source could potentially be tampered and manipulated by a savvy hacker that could then be used to deliver harmful malware to a computer network. Although it would be a very difficult thing for a hacker to do, organizations might choose to be proactive in implementing solutions that will help prevent this potential threat.

Most particularly vulnerable are organizations whose infrastructure are vital to a vast number of people, such as energy, transportation, and utility companies. Hackers need only to leave a standard USB device which they have manipulated with this malware “lying around” an organization, on a sidewalk or in a hallway, and wait for a curious employee to pick it up and plug it into a piece of equipment within the organization. Once introduced, the malware can wreak havoc on the entire organization’s infrastructure.

The Kanguru Defender® line of hardware encrypted USB drives automatically protect you from this harmful new trick from third-party hackers, with **digitally-signed, RSA-2048 secure firmware,** and are immune to such risks. The secure firmware is verified with a self-test on start-up. If a hacker ever tried to use a Kanguru Defender USB stick to infiltrate an organization, say an energy or utility company by tampering with the firmware to introduce malware, the drive would immediately shut down, preventing any chance of a risk to the organization.

Kanguru FlashTrust™

The **Kanguru FlashTrust Secure Firmware flash drive** is designed for those customers and organizations that, while still concerned about security and quality storage, may not require the specific usage scenarios or additional costs of hardware encrypted solutions, but want a trusted USB flash drive encryption alternative. Kanguru is the first to provide this non-encrypted version to organizations as a trusted, secure firmware device.

Though the FlashTrust should not be used for sensitive information, it is a perfect solution for organizations transferring non-sensitive information, who still want to protect their organization from malware. The Kanguru FlashTrust contains the same digitally-signed firmware security implementation as our Kanguru Defender encrypted counterparts.

Used in conjunction with Endpoint Security, the Kanguru FlashTrust provides assurance that the network is protected from malware attacks by third-party hackers. Employees can work as they normally would with the convenience USB flash drives bring to business, while administrators can be confident that the infrastructure is safe and protected.

Energy companies, transportation, medical facilities and utilities are finding it important to use secure firmware drives throughout the organization to prevent potential hackers from infiltrating and bringing down the infrastructure with devious malware.

Conclusion

In conclusion, the sooner you begin incorporating good data security policies, the sooner your organization can be protected from the potential threats that are out there. When you enforce strong security policies that monitor, prevent, discern and encrypt automatically, you also lighten the load as an administrator and security tasks become easier. With the right security measures in place, organizations will immediately see results that greatly reduce the risks.

Secure.

Anytime.

Anywhere.

KANGURU™

Secure. Anytime. Anywhere.

1360 Main Street
Millis Massachusetts 02054
888-KANGURU
508.376.4245
sales@kanguru.com

www.kanguru.com