# Encryption: A Mandatory Privacy & Financial Risk Reduction Tool

Cybersecurity – " A business that ONLY ENCRYPTS its data, is more secure than a business that only does EVERYTHING ELSE"

**Bob Adhar,** BE, MBA, CISSP
CEO and Founder
Randtronics

# 1 Small and large businesses are more vulnerable than ever

## Information is power

Enterprises are collecting more information about their customers, employees, suppliers and competitors. Examples of sensitive data - tax file number, passport ID, bank account number, name, credit card number, social security number, health details, salary, etc.

## Data breaches are increasing

Refer to David McCandless on “information is beautiful” [http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/](http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/) . Unemployment, remote workers, professional criminals, shared cloud, outsourced workers and big data analytics increase breach risk

→ 2022

## Old way of stealing money

Robbing a bank

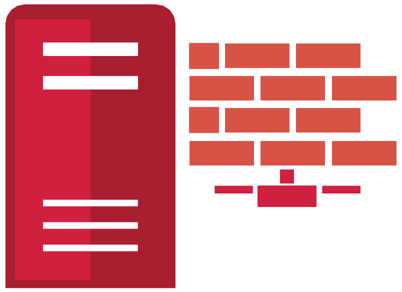
## New way of stealing money

Professional hacking

# 2 Cybersecurity is a question of priority

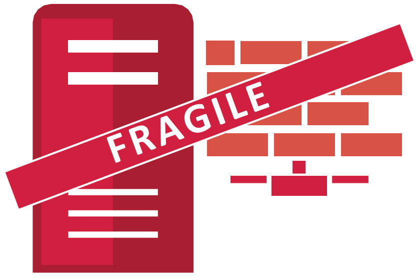
## IT Security focuses on the wrong areas

Organizational resources are mostly invested in protecting the perimeter – not your data!



## Only encryption protects the data

While perimeter security is important, it is a misguided priority when protecting data. "Encryption is your last line of defense when all other measures fail" ~ PCI Security Standards Council (Visa, Mastercard, Amex, JCB & Discover)



## Breaking through firewall is easy

Professional hackers can penetrate most firewalls easily

## Encryption is hard to crack

Using 256-bit length keys, AES has $2^{255}$ possible key combinations that could take 3 x $10^{51}$ years to break

## If your aim is to protect data, encryption should be your top priority

To determine your organization's priority, ask the question – Do we secure systems or data? Your answer determines your starting point

# 3 Encryption of data eliminates legal liability and stops breaches

randtronics

## Regulators mandate encryption

PCI DSS, HIPAA, GDPR and international privacy equivalents, legally mandate the protection of citizen's personal data. You won't get fined if your firewall is hacked or IT systems suffer ransomware attack, but fines and criminal charges may apply if you lose personal data. Only encryption removes the GDPR fine of 4% or €20M. "Encryption is your last line of defense when all other measures fail" ~ PCI Security Standards Council (Visa, Mastercard, Amex, JCB & Discover)

## Long delays discovering data breaches

Average time taken to identify malicious attacks is more than six months (IBM Ponemon Report) , which can lead to irreparable brand damage, financial loss, customer churn, share price drop or closure of your business forever. Only encryption removes the health records breach risk per HIPAA

## C-Level executives are liable

Data breaches are no longer just an IT problem. "Board members and the C-suite can no longer ignore the drastic impact a data breach has on company reputation" (Experian). Usage of encryption before a breach, demonstrates utmost care of customer's sensitive data. After a breach, if you can report to regulators that you have used encryption, it removes financial liability, protects reputation, and maintains customer loyalty

# 4 Ubiquitous Patented Encryption from Randtronics

## Performance

*Will systems run slower after encryption?*

Randtronics DPM uses proven methods and systems of Windows, Linux, database, cloud and hardware accelerators where user experience before and after encryption is the same

## Deployment

*Will we need to change software code for applications to use encryption? What about ROI?*

Randtronics DPM deployment is transparent and reduces scope of compliance and business risk

## Availability

*Is my data lost forever if encryption fails? What safeguards are available? What about reliability and availability?*

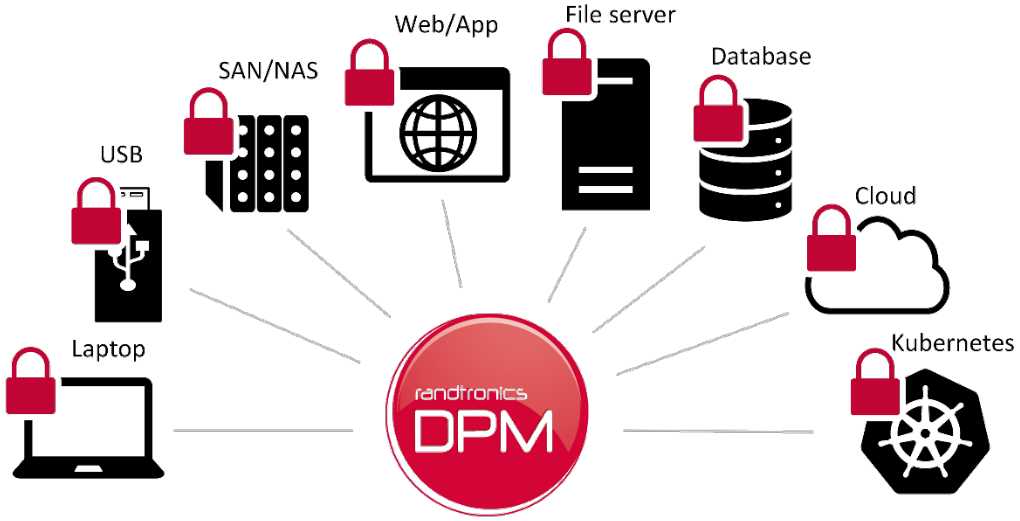
Randtronics DPM uses familiar proven systems and methods of load balancers, disk mirroring and database clustering for automated backups and redundancy used by businesses for decades

## Usability

*Will encryption require retraining due to changed business processes? What about ease of use?*

DPM is easy to use and requires no business process changes, as it uses familiar Windows/Linux/database technologies and transparent encryption integration

# 5 | Randtronics DPM simplifies encryption for everyday use

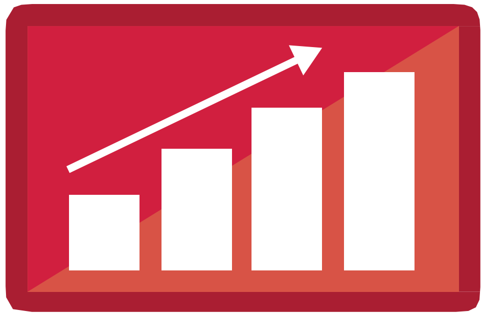


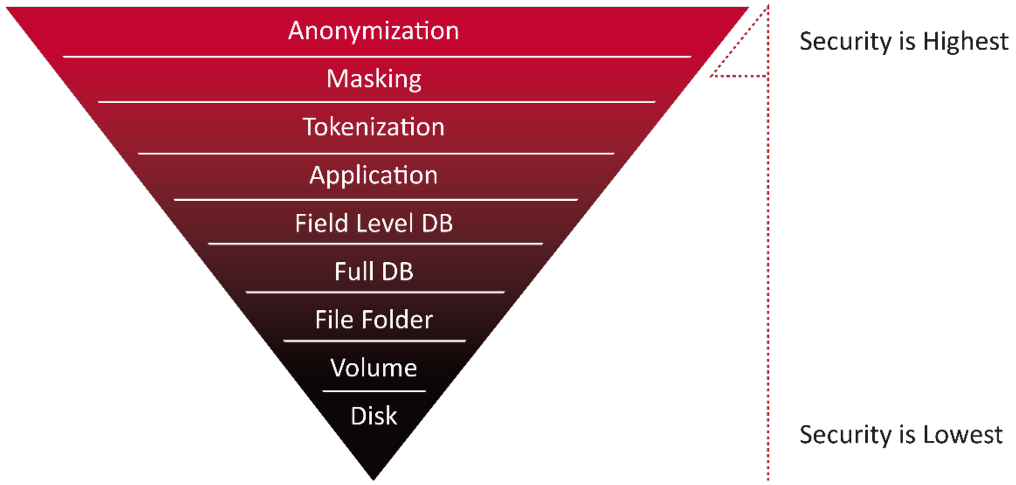
## DPM is easy to deploy and use

DPM transparent data encryption and spoofing requires no software code changes and supports laptops, servers, any application, multi-vendor databases, Kubernetes containers, on-prem and multi-vendor clouds. DPM SaaS offering enables outsourcing all to Randtronics

## Rapid Return-on-Investment

DPM enables reduced compliance scope and lower operational costs, through better management of risks associated with privacy, compliance, employees, contractors, outsourced workers, remote workers and public cloud usage



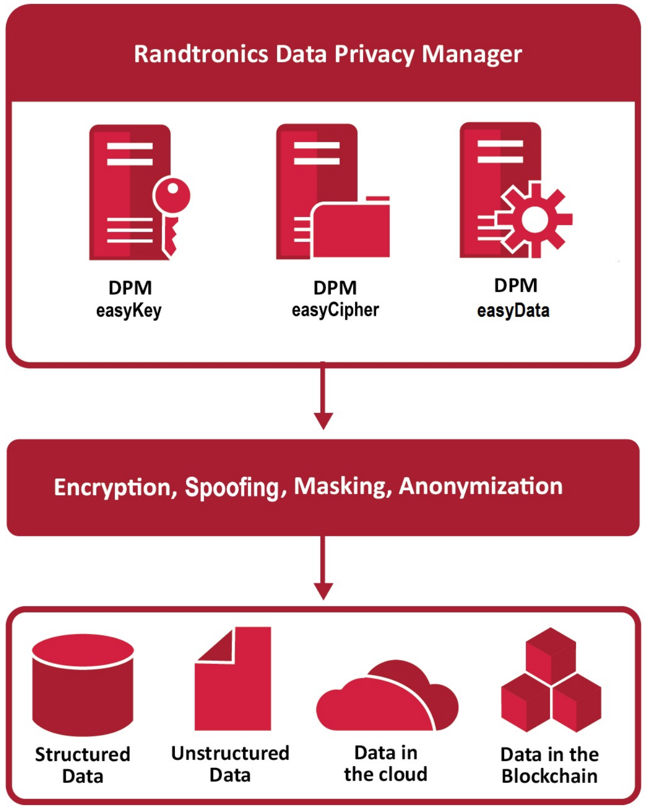


Data Privacy Application Points & Security Levels

## Flexible security levels

Data spoofing, encryption, masking, tokenization, anonymization, pseudonymization, ACL, application white listing, FIPS140-2 L3 & CC EAL4+ HSM support support

# 6 Randtronics DPM - comprehensive data protection



## DPM works on-premise or in the cloud

DPM provides comprehensive data protection for sensitive information to facilitate data privacy and compliance on premises, in the cloud, or hybrid cloud and on-premise infrastructures

## DPM uses innovative data spoofing

The Randtronics DPM solution uses data encryption, tokenization, anonymization, pseudonymization and masking technologies to protect your data in Kubernetes containers and across multi-vendor clouds and in-house systems

## DPM leverages current staff and skillsets

Randtronics DPM uses methods and standard components of Windows/Linux operating systems and MySQL/Microsoft SQL Server databases. This lets you use the same technical support staff, skillsets, methods, hardware and software vendors and contractors, rather than acquiring new systems and specialist staff to deploy and maintain encryption. DPM easyEaaS enables outsourcing encryption and key management to Randtronics

## DPM deploys quickly and easily, with a rapid ROI

DPM’s transparent data encryption deploys into existing IT systems and applications without requiring any software code changes, business process re-engineering or user re-training. Format-preserving Tokenization further reduces the scope of compliance. This directly reduces resources, effort and costs, providing a more rapid Return on Investment

# 7 Request demonstration or trial software

## Please either phone the number below or send an email request to enquiry@randtronics.com

### Americas

Redwood City, CA

### Australia

North Ryde, NSW

**Sales Americas:** Julian Suarez +720 244 7987

**Founder & CEO:** Bob Adhar +650 241 2671 or global roaming +614 18 226 234

### United Kingdom

London, England
**Sales Director**: Neil Woodley +44 7825 448310

### Korea

Seoul, South Korea
**Sales Director:** Jeong Yun Lee +61 400 451 490

Email: enquiry@randtronics.com | www.randtronics.com | ABN: 99 101 584 329