Auditoría y Seguridad proactiva de datos.

Gabriel Murcia Roncancio

Director de Ventas y Servicios

R&C

PROTECCIÓN E INNOVACIÓN

En que piensa…

Control a Usuarios Privilegiados

Accesos no Autorizados

En que piensa cuando se trata de seguridad y protección de sus bases de datos?

Bloqueo

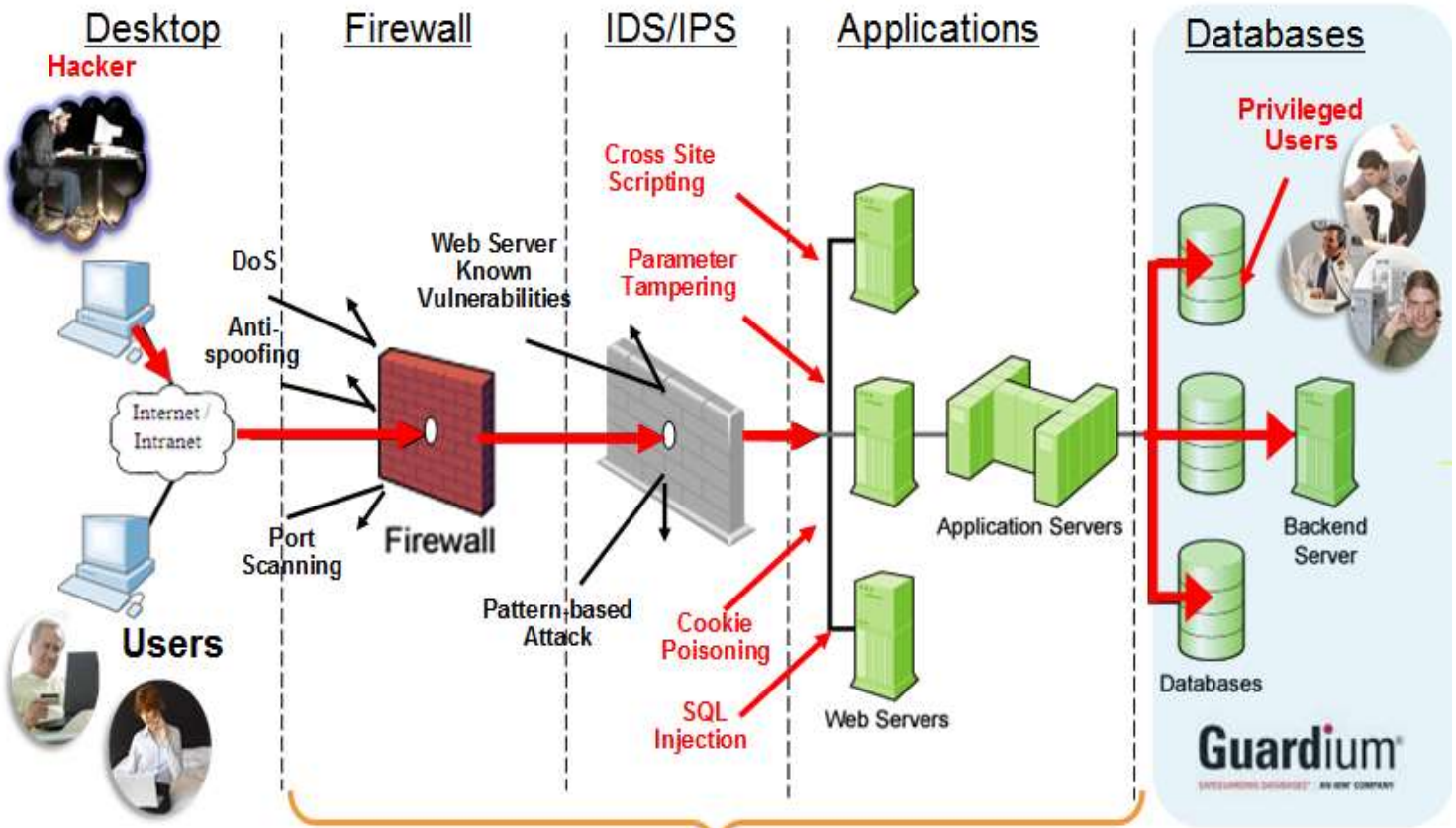
Auditoria

Cumplimiento

Controles Centralizados

PCI-DSS, SOX, Ley de protección de Datos, Circular 052

La seguridad perimetral no es suficiente



Reality: Most of the front end security layer protection cannot stop all the threat vectors → Need the last layer of protection at the data level

La Data es el principal objetivo

Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

WHY?

- Database servers contain your client's most valuable information
  - Financial records
  - Customer information
  - Credit card and other account records
  - Personally identifiable information
  - Patient records
- High volumes of structured data
- Easy to access

2012 Data Breach Report from Verizon Business RISK Team http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

"Go where the money is… and go there often."

- Willie Sutton

¿Cómo apoyamos?

Discovery
Classification

Assessment
Masking/Encryption

Identity & Access
Management

Activity
Monitoring

Blocking
Quarantine

Masking
Encryption

Discover | **Harden** | **Monitor** | **Block** | **Mask**

Where is the sensitive data?

How to secure the repository?

Who should have access?

What is actually happening?

How to prevent unauthorized activities?

How to protect sensitive data to reduce risk?

¿Cómo apoyamos?

Propuesta de Valor

1. **Prevención de brechas de seguridad**
   - Mitigar las amenazas internas y externas.
   - Asegurar la información sensible de la organización, es decir, información confidencial acerca de clientes, productos, estados financieros, entre otras.

2. **Gobernabilidad de los datos**
   - Prevenir los cambios no autorizados de los datos sensibles.

3. **Reduce costos operativos relacionados con el cumplimiento sin impactar el desempeño de las aplicaciones**
   - Automatizar y centralizar los controles y políticas.
   - Simplificar los procesos de cumplimiento y auditoria.

Propuesta de Valor

SECURITY OPERATIONS

CISO/CSO Director / VP of IT Security, Head of Sec Ops

- ✓ Real-time detection of breach
- ✓ Secure audit trail
- ✓ Forensic event analysis
- ✓ Data Access control
- ✓ Workflow and Reporting
- ✓ Vulnerability assessment

RISK, COMPLIANCE & Audit

CCO, CRO, CPO

- ✓ Separation of duties
- ✓ Best practices reports
- ✓ Automated & systematic controls
- ✓ Assurance monitoring
- ✓ Inappropriate access/use

APPLICATION AND DATABASE

CIO, IT Directors, IT Ops

- ✓ Minimal system impact
- ✓ Automated change reconciliation
- ✓ Audit logging
- ✓ Automated compliance workflow

Beneficios de nuestra solución

Risk Mitigation	System Core or MIPs Processor Savings	Disk Storage Savings	Violation Remediation
Real-time alerting of suspicious and abnormal activity Aggregated enterprise views, rollups & audit trails, correlation events	Overall savings of 10% on the core utilization for running Guardium over manual log scrapping process	94% savings in the disk storage for audit data. For every 100GB of audit data Guardium needs only 6GB	Estimated: 66% time savings in handling remediation violation due to automated workflows

Guardium Capability	Description	Stakeholder	Measure	Business Value
Prevent Data Breaches	Provide full controls on the cybercriminals and rouge insiders activities as well as protect customer data and corporate secret	Security Administrators, Executive Management	Improve Risk Mitigation	Cost take-out due to reduce risks, and operational costs
Assure Data Governance	Prevent unauthorized changes to sensitive data by privileged users	Compliance Team	Less # of compliance exposure Y2Y	Reduction in internal and external audit costs
Reduce Audit Costs	Provide an automated, and continuous control with simplified process	Database Administrators	Speed of audit	Cost take-out due to operational costs for managing a compliance process
Identify and Discover Sensitive Data	Be able to identify sensitive data such as credit card info in application databases	Compliance Team	Less breaches and compliance exposure	Proactive risk mitigation could save millions of $$

¡Gracias!

Gabriel Murcia Roncancio
Director de Ventas y Servicios
gmurcia@rycbc.com
301 568 6848
+57 1 - 621 7555 / 805 1122