VIRTUAL
GUARDIAN

# Unlock Organizational Security: A Three-Step Guide

## *Completing the Security Puzzle*

Governance & Protection

Identity Management,
Governance & Analytics

Automation

287 6th Street
E, Suite 500,
St. Paul, MN
55101

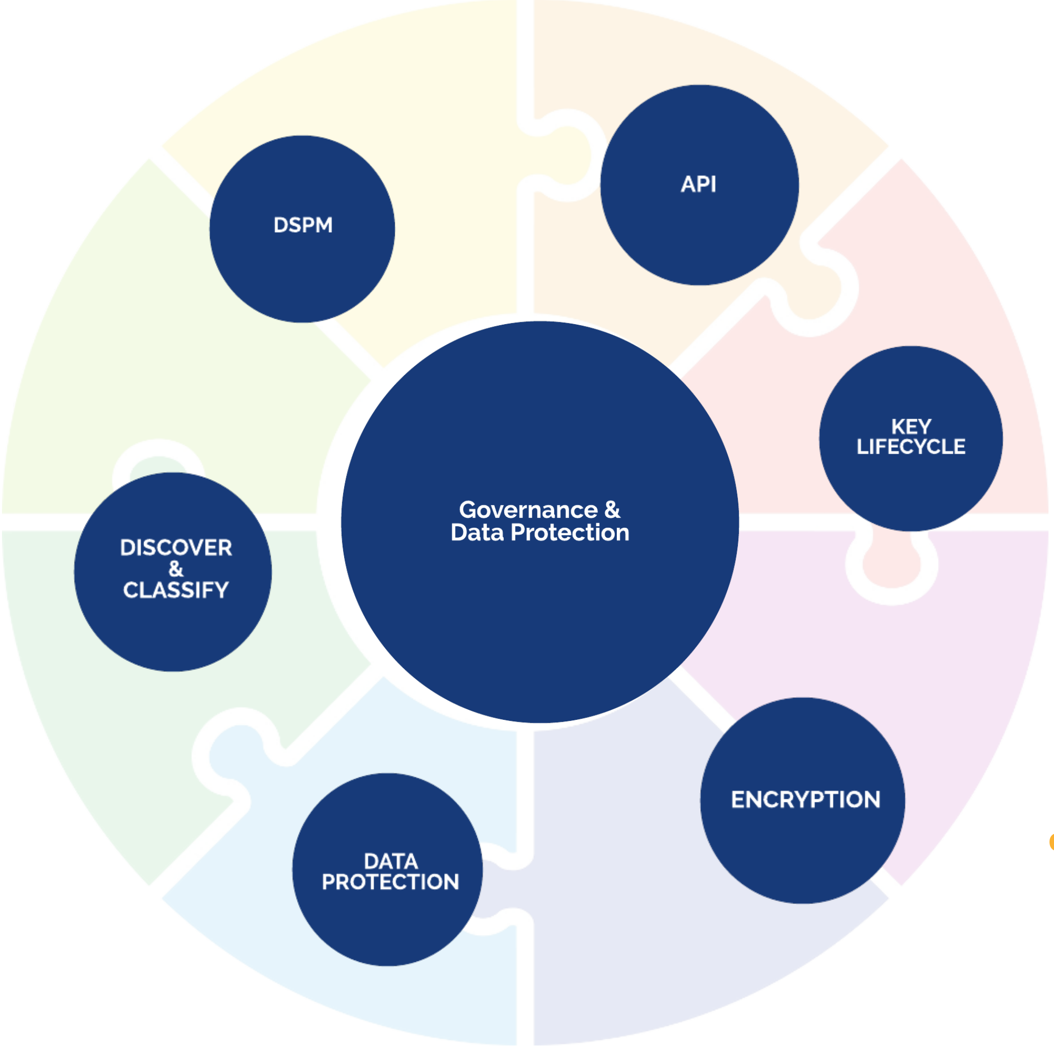
1550 Metcalfe
Street, Suite 1100,
Montréal, Québec
H3A 1X6

1255 Lebourgneuf
Blvd, Suite 270
Québec (Québec)
G2K 0M6

130 Adelaide St. W.,
Oxford Tower, Suite
No. 2202
Toronto, ON M5H 3P5

**+1-800-401-TECH (8324)**

**virtualguardian.com**



# 1 Essential Components for a Robust **Governance & Data Protection** Framework

## $1.04 M

**Average difference in cost of a breach** at organizations with high level vs. low level of compliance failure

*- IBM Security*

**Governance** ensures that data quality is maintained throughout its lifecycle and that appropriate controls are in place to support business objectives. **Protection** emphasizes the dependability of the data itself, rather than focusing solely on network, server, or application security.

Together, key aspects of data protection include:

- **Discovery:** Identifying and understanding the location and nature of sensitive data.
- **Management:** Defining and enforcing access policies to control who can view, edit, or access data.
- **Protection:** Implementing measures to prevent data loss, unauthorized use, and exposure to sensitive information.
- **Monitoring:** Continuously tracking data usage to detect anomalies that may indicate malicious activity.

API discovery and security are critical elements of a comprehensive governance and data protection program, providing visibility and control over data sets that traverse APIs to cloud, SaaS, and other external environments. By implementing robust governance, data protection measures, and leveraging technologies like API security, encryption, and data security posture management, organizations can significantly reduce their risk of data breaches and protect their valuable assets.

**SEE NEXT PAGE for detail on DSPM with IBM's Guardium**

# Virtual Guardian

## Your Partner in DSPM

DATA IS EXPLODING. Your organization is racing to keep up, especially in the cloud. The risks are real and rising. **Virtual Guardian's Data Governance and Protection cloud assessment** is your solution to gaining control.

### Powered by IBM's Guardium, we help you:

**Discover**

Uncover hidden data within your cloud environment.

**Automate**

Simplify data management.

**Analyze**

Understand data flow to detect vulnerabilities.

**Identify**

Pinpoint sensitive information like PHI and PII.

**Uncover**

Find and fix weaknesses in your data stores.

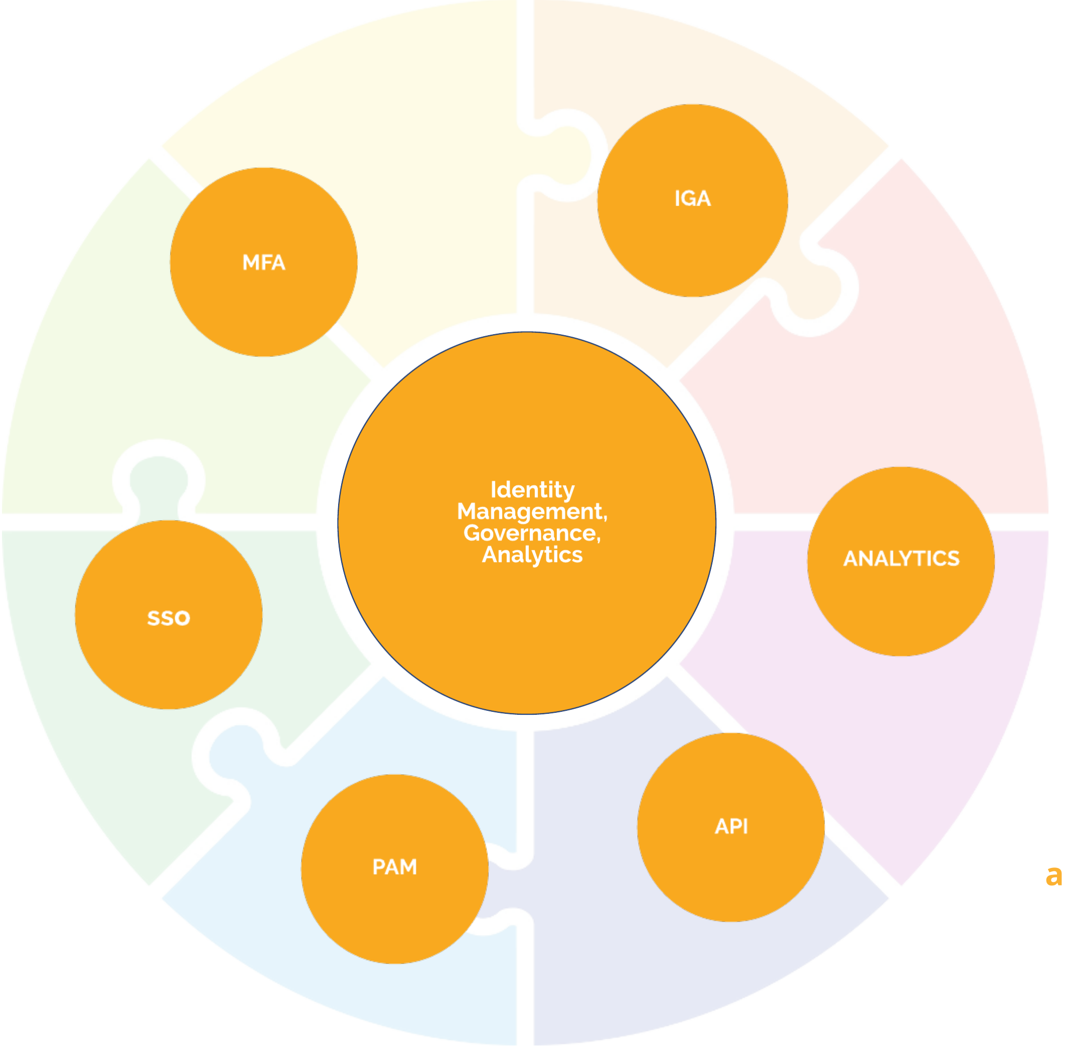
**Comply**

Ensure regulatory compliance with clear visibility reports.

Our agentless solution connects directly to your SaaS data repositories, providing **continuous monitoring** and peace of mind.

**Protect your organization's future with Virtual Guardian.**

*UNMATCHED CYBERSECURITY EXPERTISE, FUELED BY TRUST*



# 2 Essential Components for a Robust **Identity Management, Governance, and Analytics** Framework

## 277 Days

**Average time to identify and contain** a data breach.

*- IBM Security*

**Identity Management** ensures user identities are properly managed. **Governance** establishes policies for managing identities and access rights. **Analytics** provides insights into user behavior and helps identify threats.

**Identity Governance** focuses on:

- Access control
- Role-Based Access Control (RBAC)
- Entitlement management
- Segregation of duties (SoD)

**Identity Analytics** involves:

- User behavior analysis
- Risk assessment
- Identity threat detection

**Identity Management** involves:

- Lifecycle management
- Provisioning and de-provisioning
- Single Sign-On (SSO)

**Benefits of effective identity management** include:

- Enhanced security
- Improved efficiency
- Compliance
- Productivity

**SEE NEXT PAGE for detail on Virtual Guardian's API Security**

# Virtual Guardian

## Your Partner in API Security

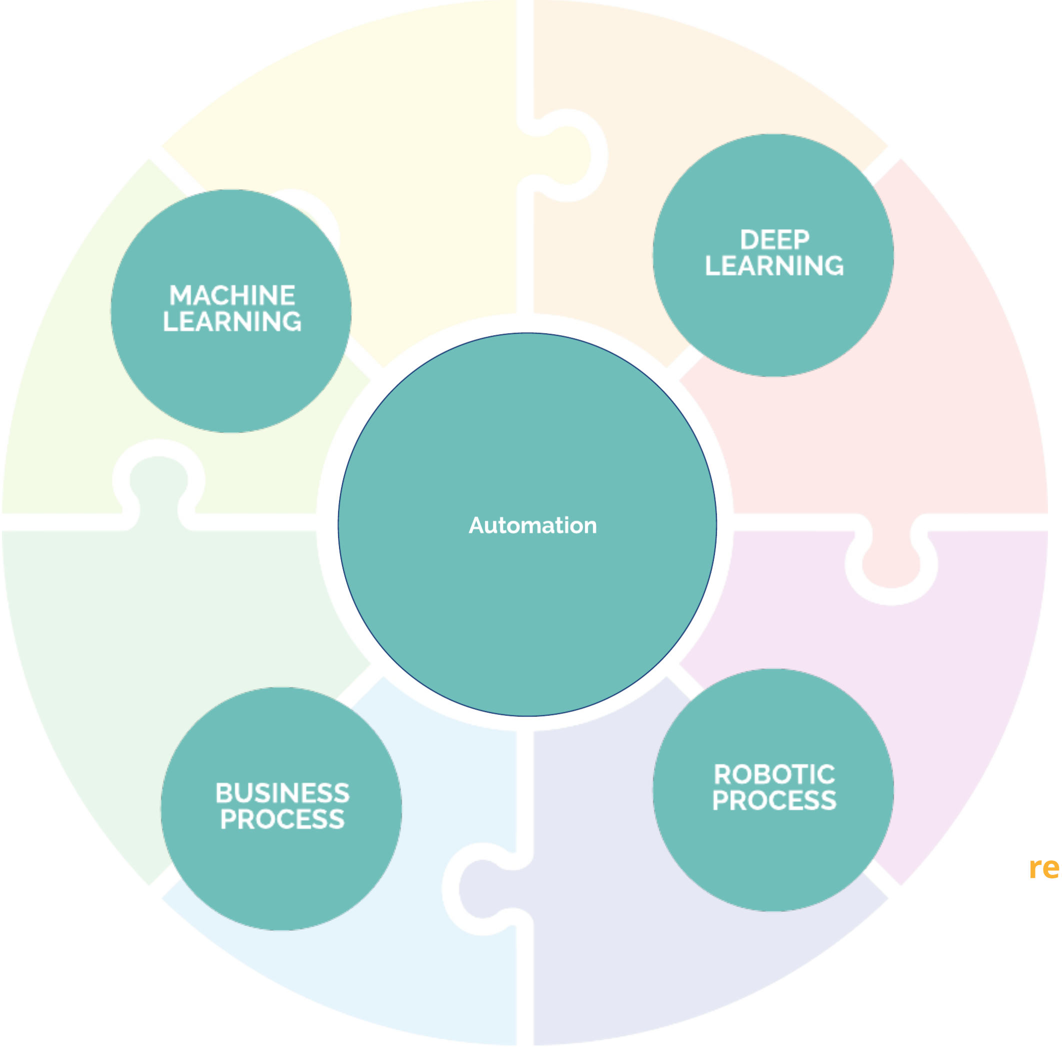
Virtual Guardian combines **Offensive API Penetration Testing** and **API Gateway with Continuous API monitoring** for a "pay and forget", all-around API security service offering.

- Baseline penetration testing of client’s API
- API Gateway with Continuous API monitoring (“API SOC”)
- Securing CI/CD
- Static code security testing
- External recurrent security scans (once per x)
- Extensive penetration test in collaboration with DevSecOps team.

Studies suggest a high prevalence of API-related breaches.

A survey by Traceable AI found that **74% of organizations reported experiencing at least 3 API breaches in the past two years**, with some facing even more (*Traceable AI, State of API Security 2023*).

DDoS attacks are a common method for exploiting API vulnerabilities,with one report indicating **38% of respondents experiencing a DDoS attack that resulted in a breach** (*Imperva, Denial-of-Service Attacks Report 2023*).



# 3 Essential Components for a Robust **Security Automation** Framework

## Automate

**Manual and reactive response** = too little, too late.

*- IBM Security*

**Automation** involves using technology to streamline processes, reduce manual labor, and improve efficiency. When combined with **Machine Learning** and **Deep Learning**, automation can unlock even greater potential.

By automating tasks, organizations:

- **Improve efficiency:** Reduce manual errors and increase productivity.
- **Reduce costs:** Lower operational expenses and optimize resource allocation.
- **Enhance scalability:** Handle increased workloads without significant additional resources.
- **Drive innovation:** Free up employees to focus on more strategic and creative tasks.

**Machine Learning** enables automation systems to learn from data and improve. **Deep Learning** uses neural networks to model complex patterns. **RPA** automates repetitive tasks using software bots.

Key areas where automation can be applied include:

- **Business processes:** Automating repetitive and time-consuming tasks, such as data entry, report generation, and customer service.
- **IT operations:** Automating infrastructure management, security tasks, and software deployment.
- **Decision-making:** Using machine learning to automate decision-making processes based on data analysis.

# Take Action

## Address Your Security Blind Spots

### Effective Security requires a trusted partner:

- **Risk Assessment:** We'll conduct a thorough risk assessment to identify potential vulnerabilities. We'll consider factors like the likelihood of an attack, the potential impact of a breach (financial, reputational), and existing security controls - placing focus on High-Risk APIs.

- **SOC & Ongoing Monitoring:** Security is an ongoing process. We'll capture critical security logs, including for API transactions, for enhanced operational awareness and continuously monitor for threats to business, watching for bad actors, and indicators of compromise. Our 24/7 SOC, powered by IBM's Qradar, manages your security so that you can focus on what matters - running your business.

VIRTUAL GUARDIAN

VIRTUAL
GUARDIAN

# Unmatched Cybersecurity Expertise, Fueled by Trust

Contact Us to Get Started Today.

+1-800-401-TECH (8324)

f in X

virtualguardian.com

287 6th Street
E, Suite 500,
St. Paul, MN
55101

1550 Metcalfe
Street, Suite 1100,
Montréal, Québec
H3A 1X6

1255 Lebourgneuf
Blvd, Suite 270
Québec (Québec)
G2K 0M6

130 Adelaide St. W.,
Oxford Tower, Suite
No. 2202
Toronto, ON M5H 3P5