

Cloud Security: Focusing on Automation and Thwarting APTs

Derek Tumulak
VP Product Management
June 5th 2013

Stark Reality of Security Industry Today: Perimeter Security is Failing

100%

of victims have up-to-date
antivirus software



94%

of breaches are reported
by third parties



416

median number of days
advanced attackers are
on the network before
being detected



100%

of breaches involved
stolen credentials



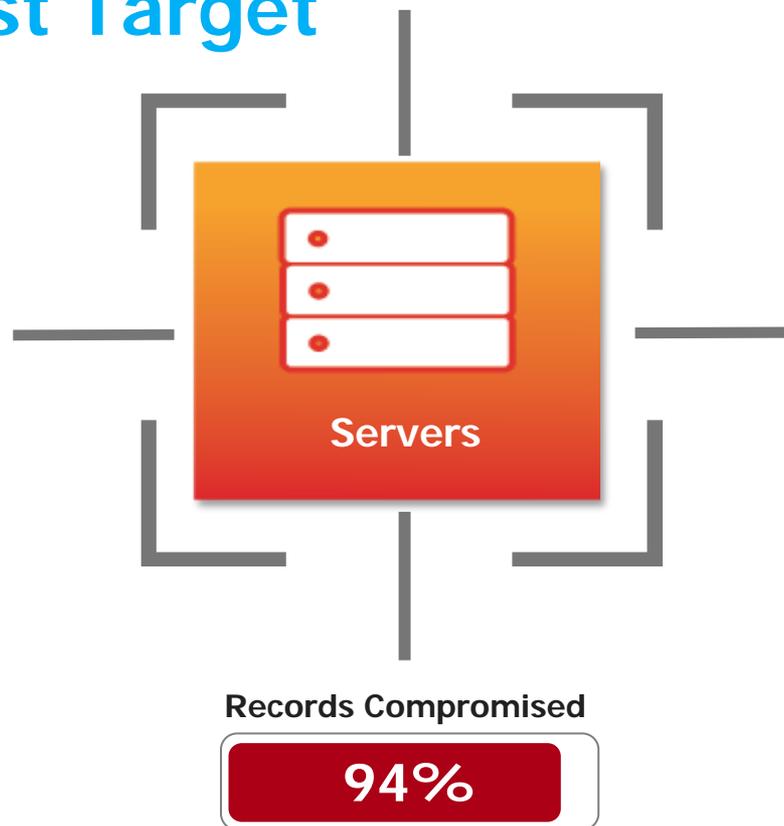
MANDIANT Source: mandiant.com/threat-landscape/

“We must accept the fact that no barrier is impenetrable, and detection/response represents an extremely critical line of defense. Let’s stop treating it like a backup plan if things go wrong, and start making it a core part of the plan.”

Verizon Data Breach Report 2013

Data is the Target ...

Server Data = Biggest Target



2012 DATA BREACH INVESTIGATION REPORT



Data is the New Currency ...

Protect What Matters – Your Sensitive Data



In the underground market economy, **data is money**, and much like any other market economy, principles of supply and demand drive it.



Forrester Research, Inc.

Measure the Effectiveness of Your Data Privacy Program - January 2013



FORRESTER®

Sensitive Data is the Target ... and No One is Immune

LinkedIn Password Hack: Check To See If Yours Was One Of The 6.5 Million Leaked

The Huffington Post | By Sara Gates  
Posted: 06/07/2012 11:25 am Updated: 06/07/2012 12:20 pm

New York Times, Wall Street Journal say Chinese hackers broke into computers

By Jethro Mullen, CNN
updated 5:59 PM EST, Thu January 31, 2013 |

50 million customers hit in LivingSocial hack

By Julianne Pepitone @julpepitone April 26, 2013: 5:47 PM ET

 Recommend 722  Tweet 260  Share 30  +1 39  Email  Print



CNNMoney

China Tied To 3-Year Hack Of Defense Contractor



Mathew J. Schwartz

[See more from Mathew](#)

Connect directly with Mathew:  Bio | [Contact](#)

U.S. defense contractor QinetiQ ignored persistent attack warning signs, lost terabytes of secret information, say investigators.

Plus There Are Insider Threats

"At the bureau, about 24 percent of the incidents we track on a yearly basis have to do with just accidental insiders — people being a knucklehead. We spend about 35 percent of our incident response time [on them]."

Patrick Reidy, CISO for the FBI

http://www.darkreading.com/insider-threat/167801100/security/news/240150554/over-privileged-well-meaning-and-dangerous.html?cid=nl_DR_daily_2013-03-12_html

Market Drivers For Enhancing Security

Global Compliance, Cloud Adoption, Big Data, Data Breaches



GLOBAL COMPLIANCE
Aggressive New Regulations



CLOUD ADOPTION
Enterprise Security
#1 Inhibitor¹



BIG DATA
Big Data is a
Big Target

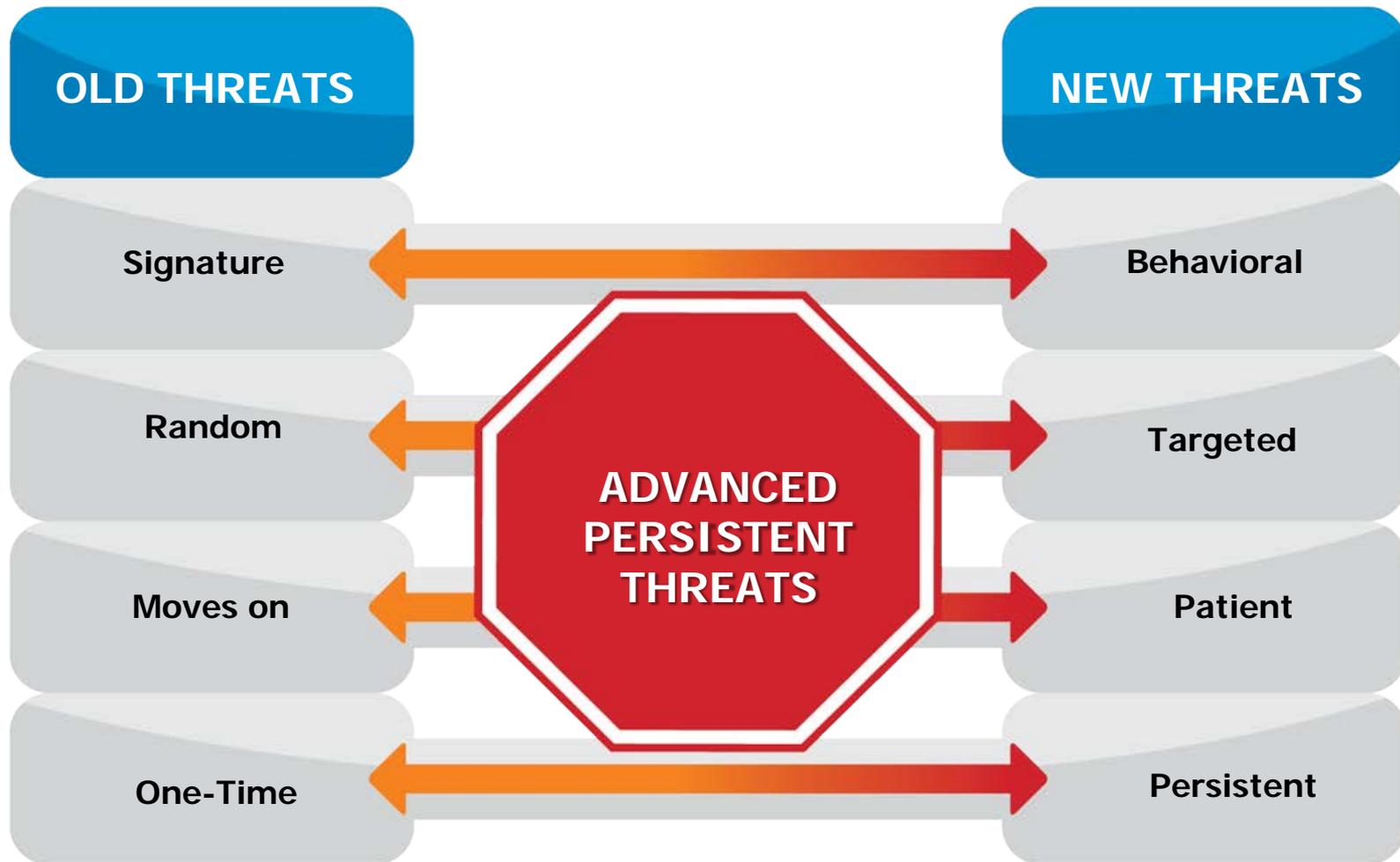


**APT
DATA BREACHES**
98% Stolen Records
From Large Orgs²

**PROTECT
WHAT MATTERS**

1. Global State of Information Security® Survey by PwC, CIO magazine, and CSO magazine – October 2012
2. Verizon Data Breach Investigation Report – March 2012

Threats Behave Very Differently Today



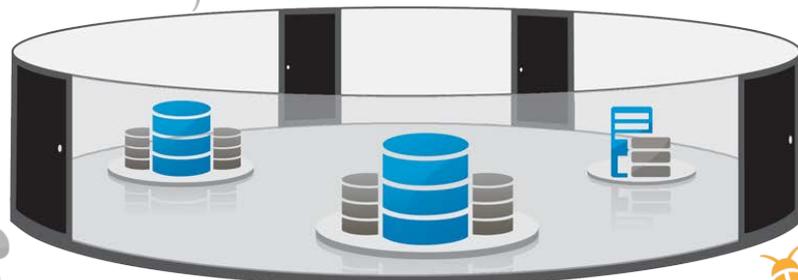
Old Model is Weak Against New Threats — A Data-Centric Security Model is Required

Signature-Based Known Old Threats / Old Model

Anti-Virus



Firewalls



Worms, Virus, Spyware, Bots
One-Time Events

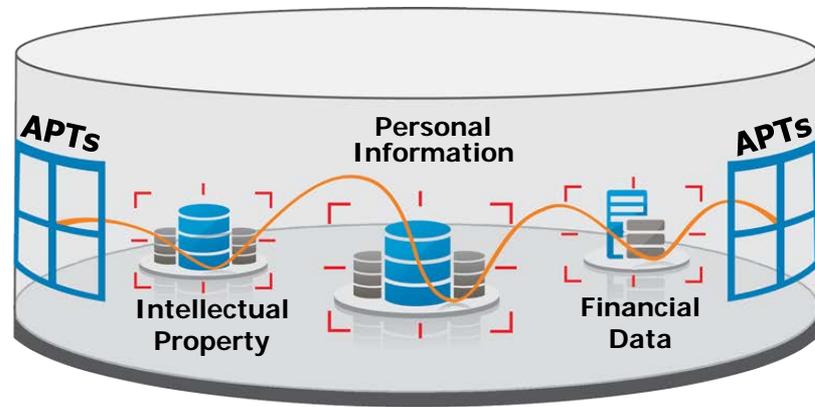


Web
Gateways



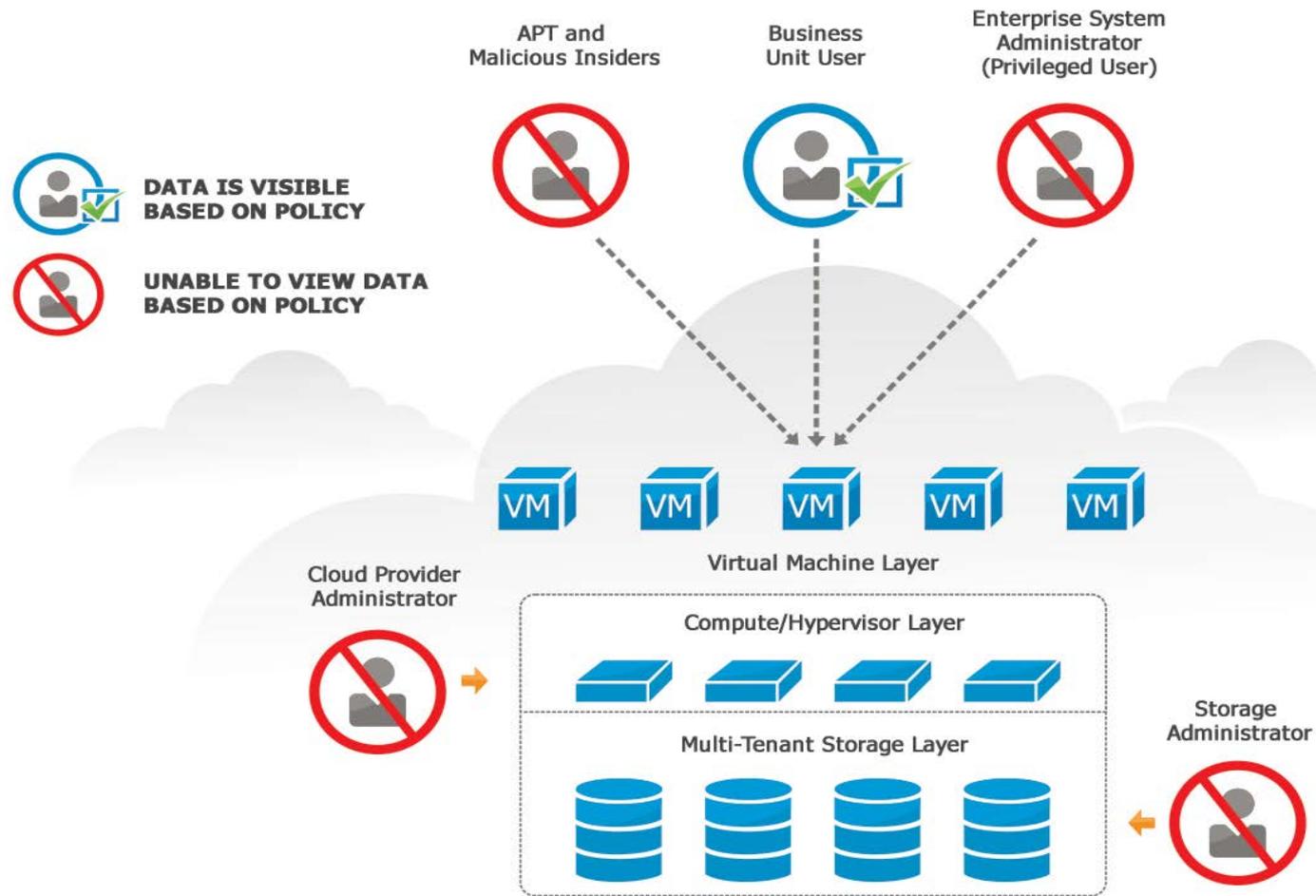
Intrusion
Prevention
Systems

Advanced Persistent Threats APT's/New Threats



Advanced Malware

Reducing the Attack Surface by Restricting Access to Data in the Cloud



Essential Data-Centric Security Measures



Access Policies

- Block privileged users like root from viewing data and thwart APTs
- Provide fine-grained control to determine who can view specific data



Encryption & Key Management

- Lock down the data using strong industry approved algorithms
- Centralized and hardened key management appliance



Security Intelligence

- Log all access to what matters → the protected data
- Provide valuable real-time intelligence on who is accessing protected data where and when



Multi-Tenancy

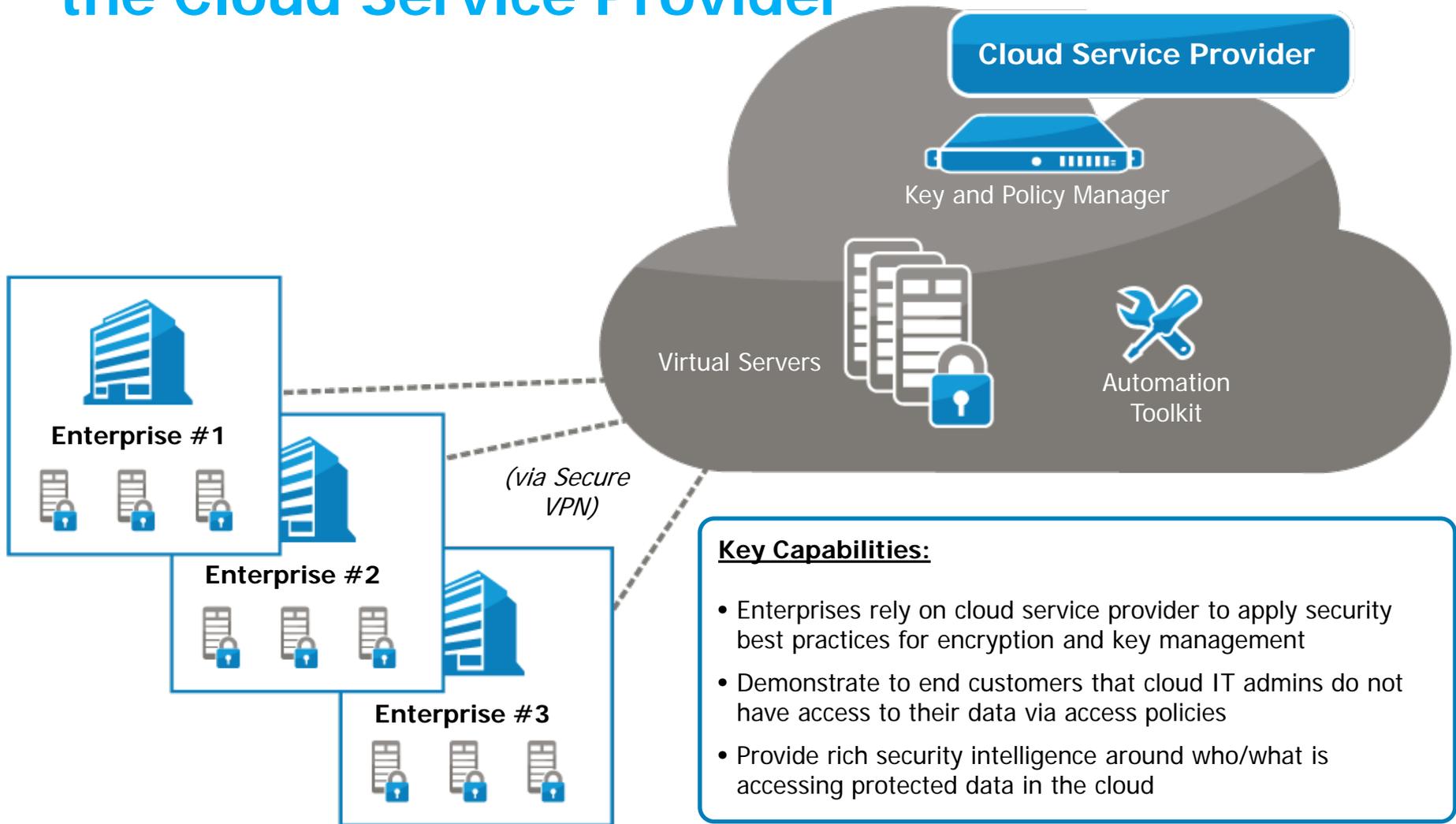
- Secure cloud data in commingled and multi-tenant environments
- Enable end customers to control policies specific to their own data



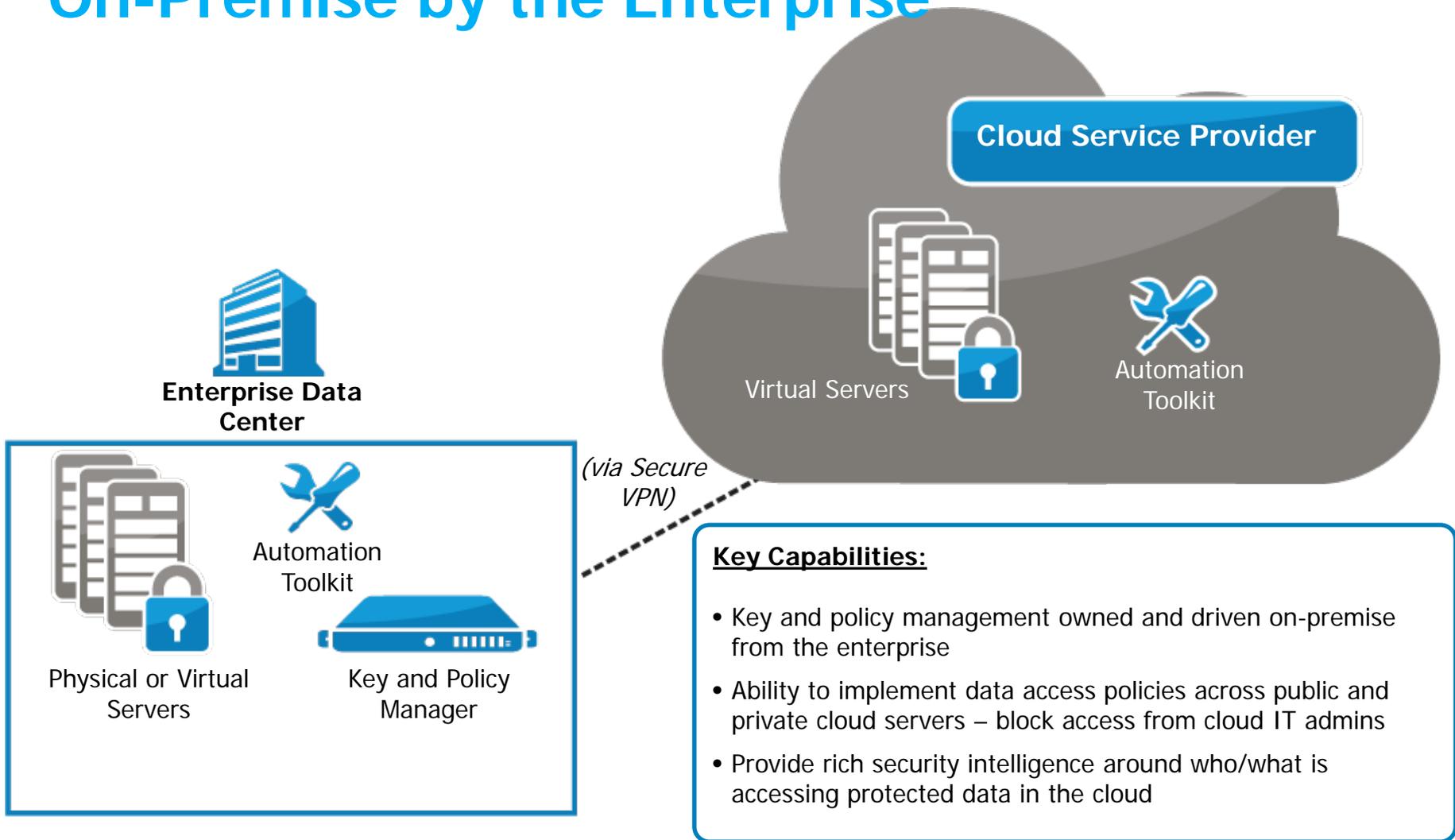
Automation

- Automatic installation, configuration, and dynamic policy enhancements based on real-time threats
- Instant protection during new customer onboarding

Use Case 1: Security Controls Managed by the Cloud Service Provider



Use Case 2: Security Controls Managed On-Premise by the Enterprise



Data-Centric Security Must Be...



▶ Transparent

- ▶ Transparent to Business Process
- ▶ Transparent to Apps / Users
- ▶ Protect All Data



▶ Strong

- ▶ Firewall Your Data
- ▶ Protect Privileged User Access
- ▶ Most Demanding

▶ Automated

- ▶ Cost Savings
- ▶ Avoid Error Prone Manual Steps
- ▶ Dynamic Real-Time Responsiveness

▶ Easy

- ▶ Easy to Manage
- ▶ Easy to Monitor & Automate
- ▶ Easy to Understand



- ▶ Minimal Performance Impact
- ▶ Support Existing SLAs
- ▶ Low Administrative Support



Benefits of Automation



Cost Savings

- With fewer manual steps time and money is saved
- Apply the 80/20 rule and automate the most common tasks



Avoid Errors

- Manual steps often lead to mistakes
- This can be costly for your business



Real-Time Responsiveness

- Dynamic action can be taken based on events
- Security can be enhanced by increasing auditing or by even blocking access to data for certain users and processes

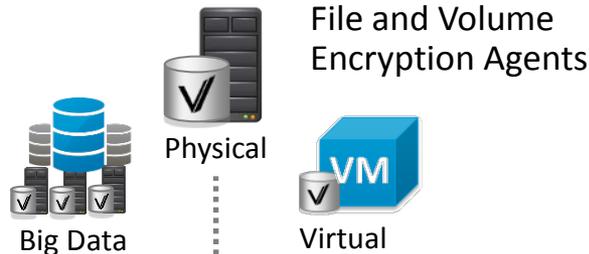
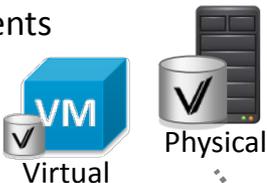
Data-Centric Security Elements

Advanced Encryption

Key Management

Application Agents

- Oracle and SQL Server TDE Keys
- Application Encryption API



Secure Vaulting

(Certificates, Keys)

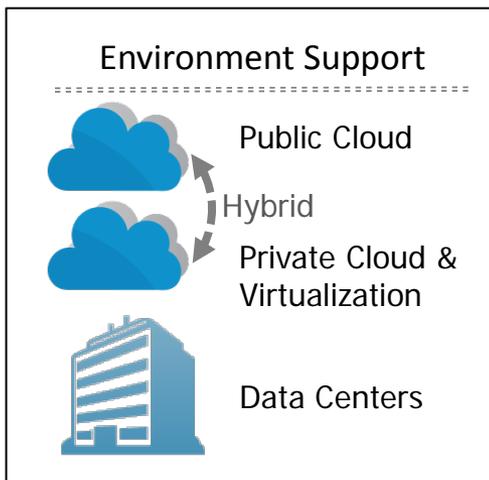


Automated Toolkits

API

- Automate Deployment
- Key & Encryption Management

Data Security Manager

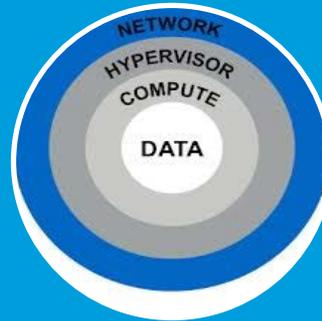


Conclusion



Get Ready for the Cloud

- Invest in security solutions that provide for a smooth transition from physical to virtual to cloud



Be Data-Centric

- Thwart APTs and malicious cloud administrators by bringing controls closer to the data and reducing the attack surface



Automate

- Drive additional cost savings and dynamically adjust security policy in real-time



Protect What Matters