Presidio Cloud Solutions

Azure OMS – Planning, Design & Best Practices

PRESIDIO®

Future. Built.

OMS – Summary

- Envisioning and Design
- Planning, Guidance and Architecture
- Discussion Points
  - **OMS: Dashboards**
  - **Audit & Regulatory Compliance: Getting Started**

PRESIDIO®
Future. Built.

Microsoft Operations Management Suite

Common challenges of IT operations

Siloed infrastructure and operations

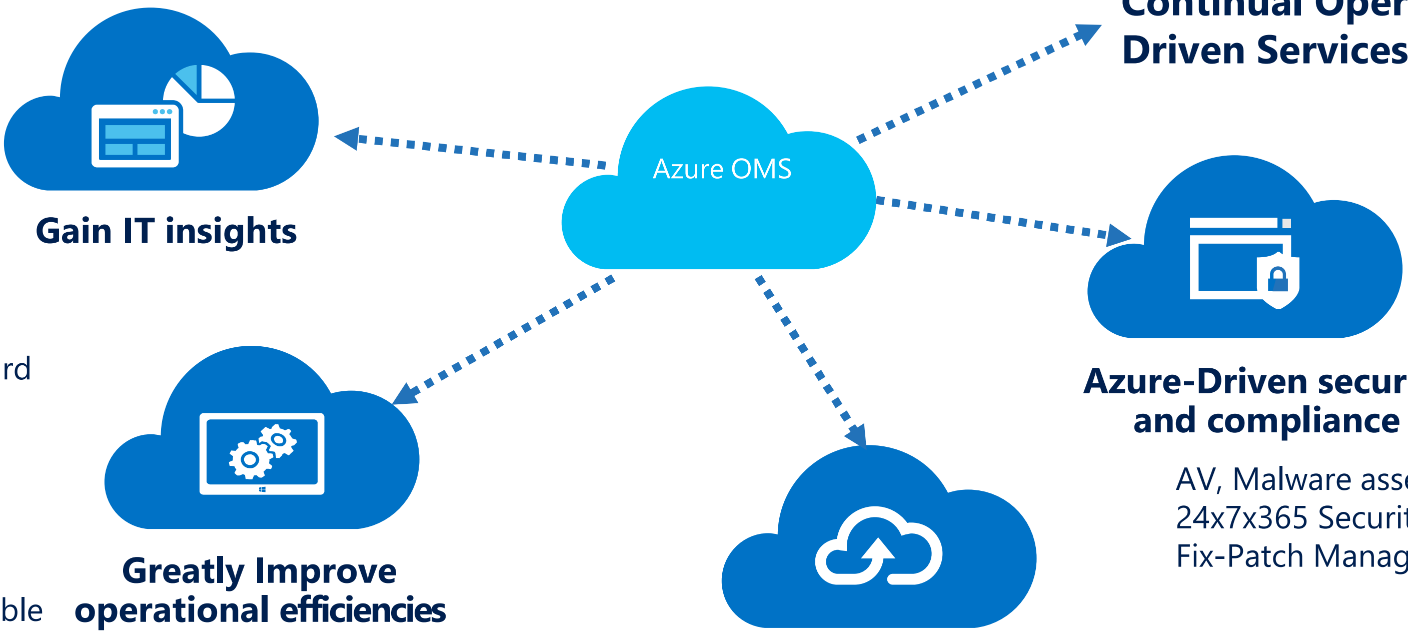
Slow and reactive responses

Sprawling environments and disparate views

PRESIDIO®
Future. Built.

Azure OMS

Integrating On-Premise with Azure Resource Management



Gain IT insights

Log analytics
Fast integrated search
Custom dashboard

Greatly Improve operational efficiencies

Workflow Capable
Template-Graphical &
PowerShell resource creation

"Knowing When" to Increase availability on demand

Continual Operations Driven Services....

Azure-Driven security and compliance

AV, Malware assessment
24x7x365 Security Awareness
Fix-Patch Management

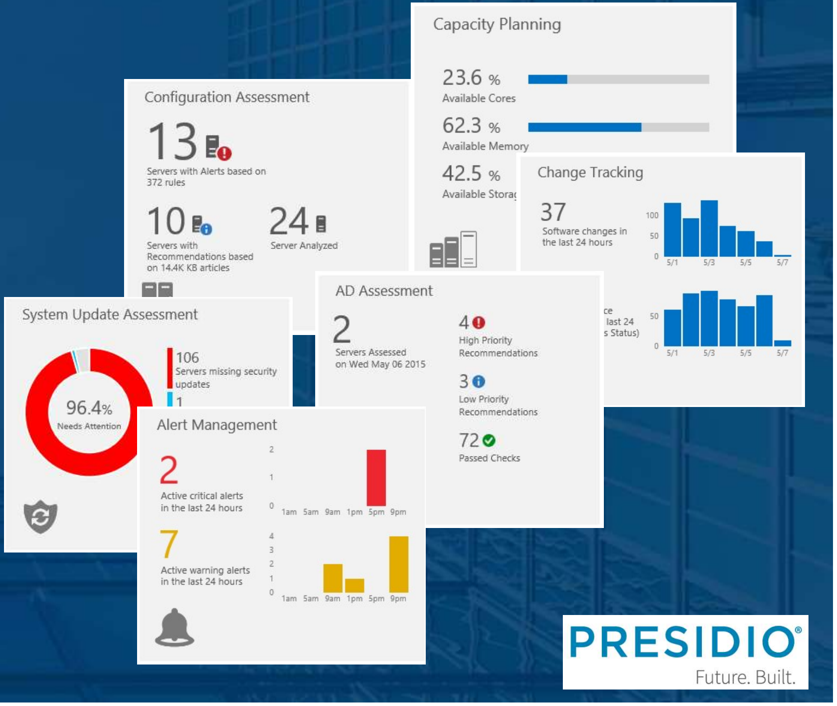
PRESIDIO®
Future. Built.

Deliver IT insights

With Log Analytics

- Combine and correlate any machine data from multiple sources with
  - Integrated search and
  - Custom dashboards

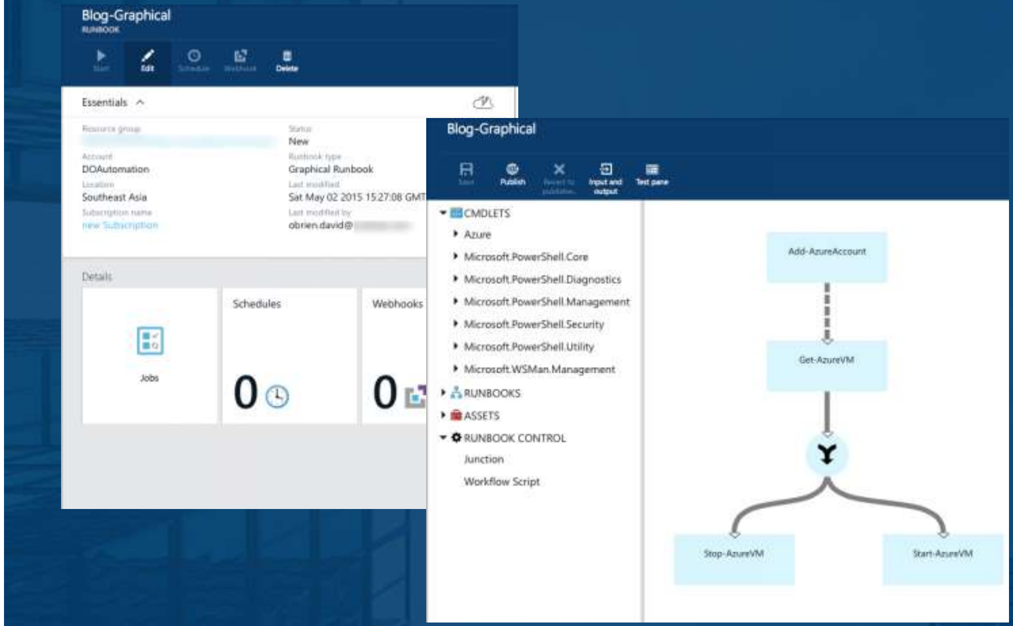
- Faster investigation and resolution of operational issues through various solution packs including:
  - Alert management,
  - Active Directory assessment,
  - Capacity planning,
  - Change tracking,
  - System update assessment, etc.,


Capacity Planning
23.6 %
Available Cores
62.3 %
Available Memory
42.5 %
Available Storag
Configuration Assessment
13
Servers with Alerts based on 372 rules
10
Servers with Recommendations based on 14.4K KB articles
24
Server Analyzed
Change Tracking
37
Software changes in the last 24 hours
100
50
0
5/1
5/3
5/5
5/7
ce
last 24
s Status)
50
0
5/1
5/3
5/5
5/7
AD Assessment
2
Servers Assessed on Wed May 06 2015
4
High Priority Recommendations
3
Low Priority Recommendations
72
Passed Checks
System Update Assessment
96.4%
Needs Attention
106
Servers missing security updates
1
Alert Management
2
Active critical alerts in the last 24 hours
2
1
0
1am
5am
9am
1pm
5pm
9pm
7
Active warning alerts in the last 24 hours
4
3
2
1
0
1am
5am
9am
1pm
5pm
9pm

PRESIDIO®
Future. Built.

Improve operational efficiency

With Automation



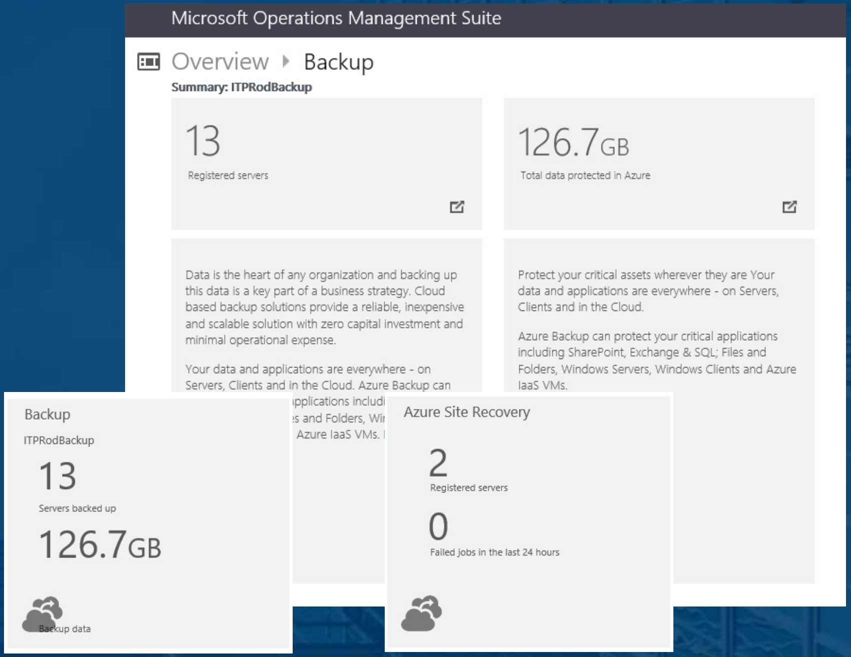
Resource group: [redacted]
Status: New
Account: DOAutomation
Runbook type: Graphical Runbook
Location: Southeast Asia
Last modified: Sat May 02 2015 15:27:08 GMT
Subscription name: new Subscription
Last modified by: obrien.david@[redacted]

- Works across clouds, on-premises systems and PowerShell DSC nodes
- Graphical workflow-authoring tool
- Integrated workflow and runbook management
- Ready-to-use runbooks from a centralized library

Increase availability on demand

With Azure Site Recovery and Backup

- Automated virtual machine replication
- Protect your critical systems and applications
- Customize recovery plans with easy-to-manage recovery points
- Migrate from physical and virtual to Azure
- Access new scenarios including cloud bursting and dev/test



Microsoft Operations Management Suite

Overview ▸ Backup

Summary: ITPRodBackup

13

Registered servers

126.7GB

Total data protected in Azure

Data is the heart of any organization and backing up this data is a key part of a business strategy. Cloud based backup solutions provide a reliable, inexpensive and scalable solution with zero capital investment and minimal operational expense.

Your data and applications are everywhere - on Servers, Clients and in the Cloud. Azure Backup can

pplications includi

s and Folders, Wir

Azure IaaS VMs.

Protect your critical assets wherever they are Your data and applications are everywhere - on Servers, Clients and in the Cloud.

Azure Backup can protect your critical applications including SharePoint, Exchange & SQL; Files and Folders, Windows Servers, Windows Clients and Azure IaaS VMs.

Backup

ITPRodBackup

13

Servers backed up

126.7GB

Backup data

Azure Site Recovery

2

Registered servers

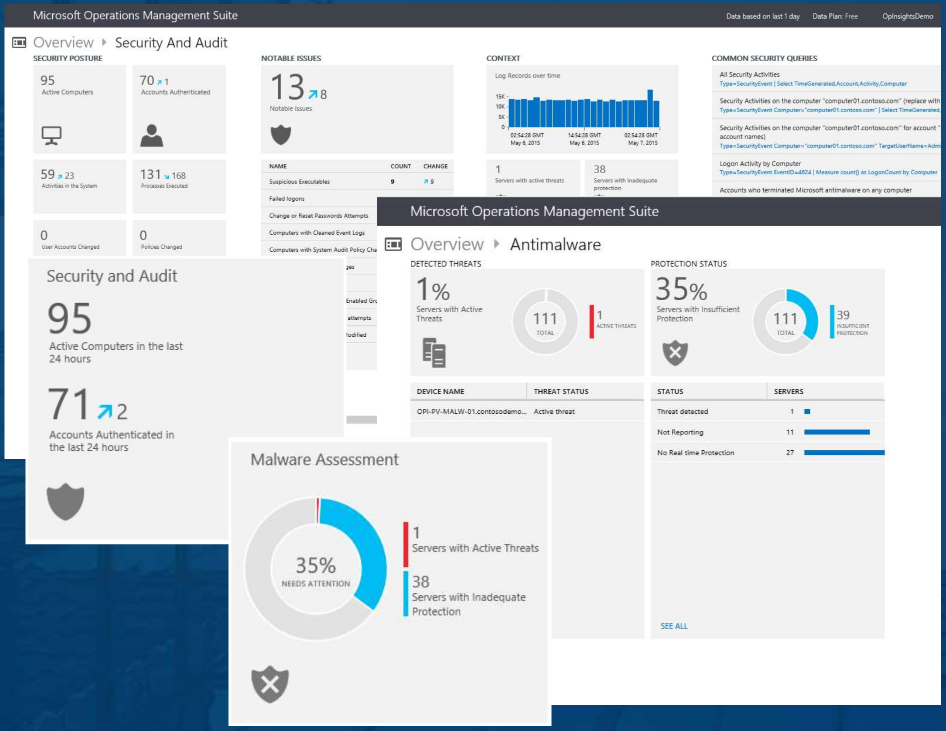
0

Failed jobs in the last 24 hours

PRESIDIO®
Future. Built.

Champion security and compliance

With events analysis and assessments



NAME	COUNT	CHANGE
Suspicious Executables	9	↗ 9
Failed logons		
Change or Reset Passwords Attempts		
Computers with Cleaned Event Logs		
Computers with System Audit Policy Cha		

All Security Activities
Type=SecurityEvent \| Select TimeGenerated,Account,Activity,Computer

Security Activities on the computer "computer01.contoso.com" (replace with
Type=SecurityEvent Computer="computer01.contoso.com" \| Select TimeGenerated,

Security Activities on the computer "computer01.contoso.com" for account "
account names)
Type=SecurityEvent Computer="computer01.contoso.com" TargetUserName=Adm

Logon Activity by Computer
Type=SecurityEvent EventID=4624 \| Measure count() as LogonCount by Computer

Accounts who terminated Microsoft antimalware on any computer

DEVICE NAME	THREAT STATUS
OPI-PV-MALW-01.contosodemo...	Active threat

STATUS	SERVERS
Threat detected	1
Not Reporting	11
No Real time Protection	27

- Collect security related events and perform forensic and audit analysis
- Comprehensive updates assessment across datacenters and public clouds
- Detection of breaches and threats with malware assessment

PRESIDIO®
Future. Built.

Azure OMS – Presidio Paving the way…

Monitoring

Provisioning

Protection

- ✓ Web based alert management
- ✓ Efficient server discovery and agent deployment
- ✓ Centralized log repository
- ✓ VM capacity planning and management
- ✓ Integrated recovery for VM workloads
- ✓ Cloud backup and long-term retention

PRESIDIO®
Future. Built.

Audit & Regulatory Compliance

Why Measuring Your InfoSec Program Matters

InfoSec Program Measurement and KPI Analysis

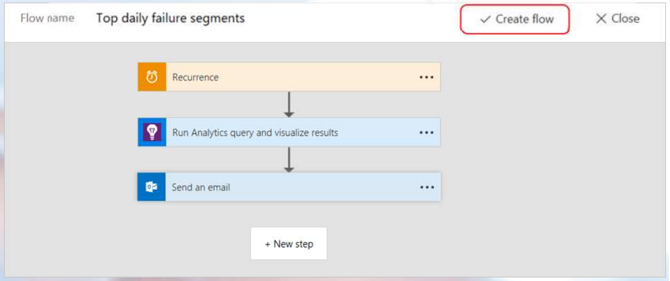
Simple Measurement & Analysis Example

Analysis Target	What does it Measure	Customer Measures	Source	Quantifiable	Repeatable	Derived Cost
Mean time to patch application	Exposure window	On time (SLO)	Patching System	Yes	Yes	$$
Content filtering event counts	Effectiveness	Cost	SOC	Yes		$
Percent of un-patched systems to asset inventory	Risk index		Patching System	Yes	Yes	
AV events detected and cleaned	Effectiveness	Reliability	AV service	Yes	Yes	$$
Mean time to AV control file update	Exposure window	On time (SLO)	AV Service	Yes	Yes	$
Average historical spend per InfoSec Incident			Historical records	Yes	No	$$$$
IDS incident reporting rate			IDS system	Yes		$
SPAM messages suppressed	Effectiveness	Customer Sat	Service Records			$$

Key Focus

- Analysis Actions
- Reporting Actions
- Rationalization Actions
- Prioritization Actions
- Reassessment Actions
- **<u>Repeatable Action</u>**

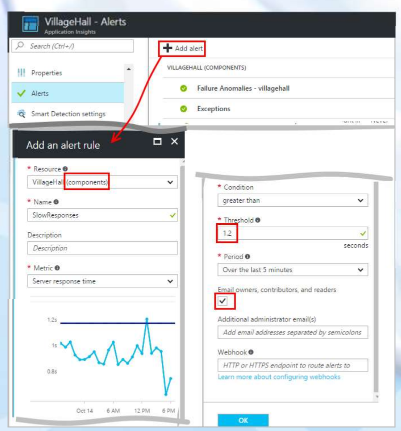
Azure Flow - Repeatable


Flow name: Top daily failure segments

Assess

"A" →

Rationalization


VillageHall - Alerts
Application Insights

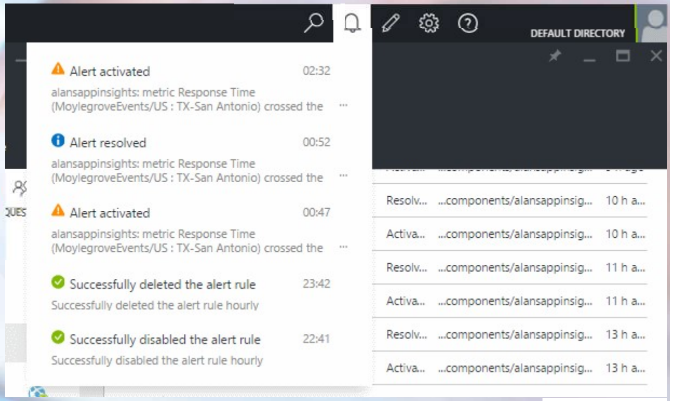
VILLAGEHALL (COMPONENTS)
- ✓ Failure Anomalies - villagehall
- ✓ Exceptions

Add an alert rule

- * Resource: VillageHall (components)
- * Name: SlowResponses
- Description: Description
- * Metric: Server response time
- * Condition: greater than
- * Threshold: 1.2 seconds
- * Period: Over the last 5 minutes
- Email owners, contributors, and readers ☑
- Additional administrator email(s): Add email addresses separated by semicolons
- Webhook: HTTP or HTTPS endpoint to route alerts to

"B" →

"C" ↑ Prioritization



- Alert activated 02:32
  alansappinsights: metric Response Time (MoylegroveEvents/US : TX-San Antonio) crossed the …
- Alert resolved 00:52
  alansappinsights: metric Response Time (MoylegroveEvents/US : TX-San Antonio) crossed the …
- Alert activated 00:47
  alansappinsights: metric Response Time (MoylegroveEvents/US : TX-San Antonio) crossed the …
- Successfully deleted the alert rule 23:42
  Successfully deleted the alert rule hourly
- Successfully disabled the alert rule 22:41
  Successfully disabled the alert rule hourly

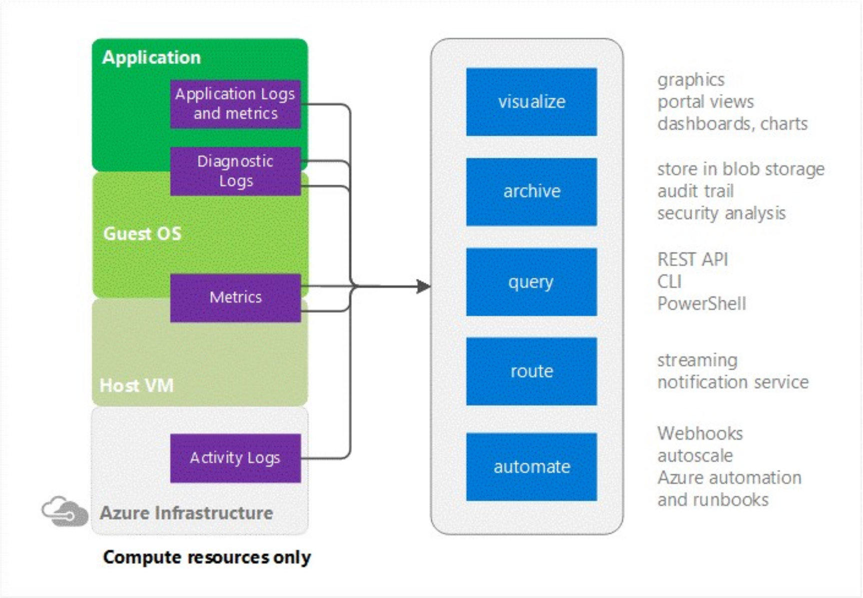
Resolv...	...components/alansappinsig...	10 h a...
Activa...	...components/alansappinsig...	10 h a...
Resolv...	...components/alansappinsig...	11 h a...
Activa...	...components/alansappinsig...	11 h a...
Resolv...	...components/alansappinsig...	13 h a...
Activa...	...components/alansappinsig...	13 h a...

PRESIDIO
Future. Built.

Assessing Meaningful Metrics to Report

InfoSec Program Measurement and KPI Analysis

"Azure Monitor enables you to consume telemetry to gain visibility into the performance and health of your workloads on Azure. The most important type of Azure telemetry data is the metrics (also called performance counters) emitted by most Azure resources. Azure Monitor provides several ways to configure and consume these metrics for monitoring and troubleshooting. Metrics are a valuable source of telemetry and enable you to do the following tasks…" – Microsoft, 2017

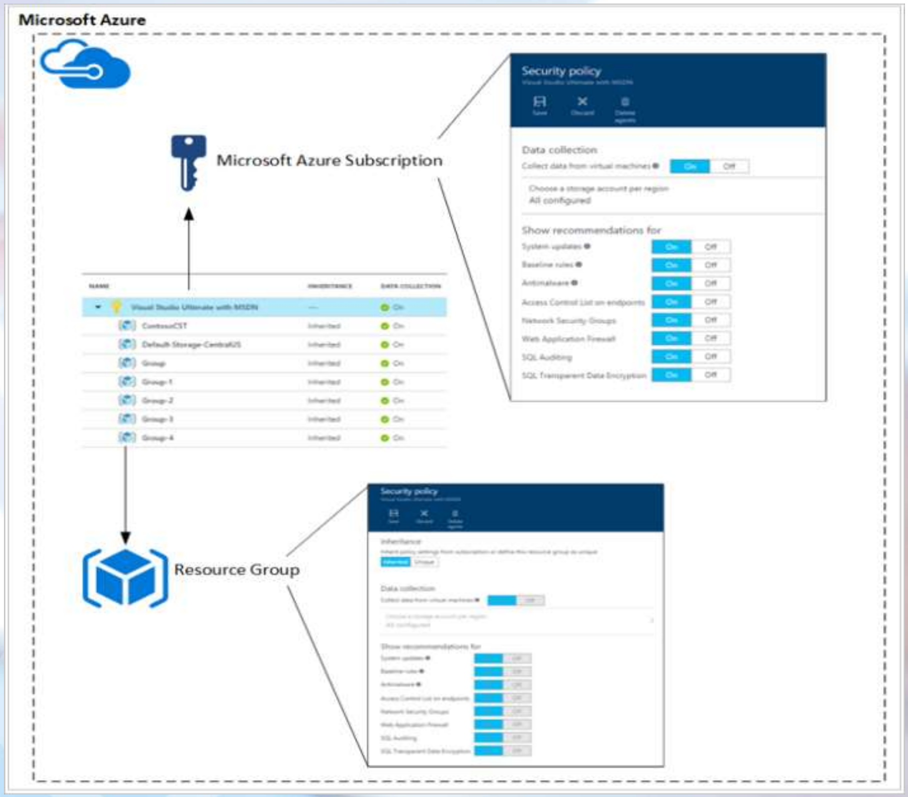


- **Track the performance** of your resource (such as a VM, website, or logic app) by plotting its metrics on a portal chart and pinning that chart to a dashboard.
- **Get notified of an issue** that impacts the performance of your resource when a metric crosses a certain threshold.
- **Configure automated actions**, such as auto scaling a resource or firing a runbook when a metric crosses a certain threshold.
- **Perform advanced analytics** or reporting on performance or usage trends of your resource.
- **Archive** the performance or health history of your resource for compliance or auditing purposes.

Measurements and Metrics

Controlled and Uncontrolled Events – Policy Driven Approach

- Azure Security Center analyzes data from the following sources to provide visibility into your security state, identify vulnerabilities and recommend mitigations, and detect active threats:
- Azure Services: Uses information about the configuration of Azure services you have deployed by communicating with that service's resource provider.
- Network Traffic: Uses sampled network traffic metadata from Microsoft's infrastructure, such as source/destination IP/port, packet size, and network protocol.
- Partner Solutions: Uses security alerts from integrated partner solutions, such as firewalls and antimalware solutions.
- Your Virtual Machines: Uses configuration information and information about security events, such as Windows event and audit logs, IIS logs, syslog messages, and crash dump files from your virtual machines.



NAME	INHERITANCE	DATA COLLECTION
Visual Studio Ultimate with MSDN	—	On
ContosoCST	Inherited	On
Default-Storage-CentralUS	Inherited	On
Group	Inherited	On
Group-1	Inherited	On
Group-2	Inherited	On
Group-3	Inherited	On
Group-4	Inherited	On

Security policy

Data collection

Collect data from virtual machines: On

Choose a storage account per region
All configured

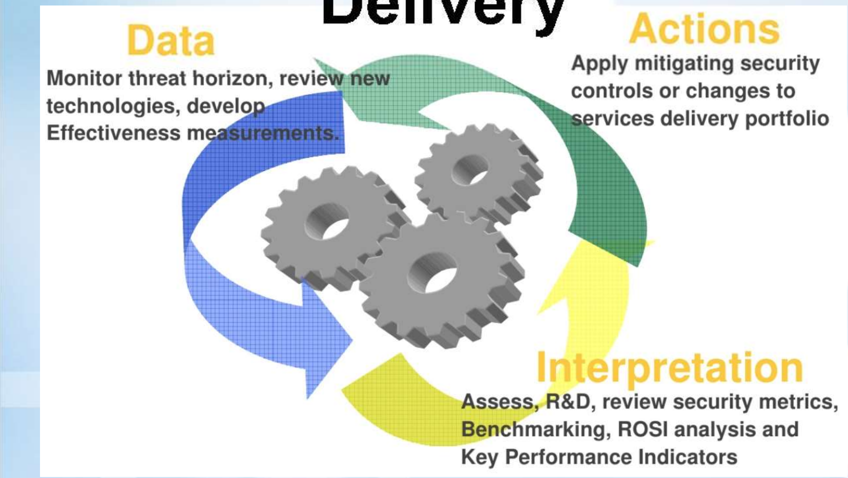
Show recommendations for

System updates	On
Baseline rules	On
Antimalware	On
Access Control List on endpoints	On
Network Security Groups	On
Web Application Firewall	On
SQL Auditing	On
SQL Transparent Data Encryption	On

How Presidio Brings Cybersecurity Programs Together

InfoSec Program Measurement and KPI Analysis

Discovery, Design, Delivery



Data

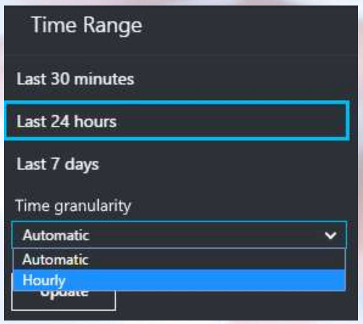
Monitor threat horizon, review new technologies, develop Effectiveness measurements.

Actions

Apply mitigating security controls or changes to services delivery portfolio

Interpretation

Assess, R&D, review security metrics, Benchmarking, ROSI analysis and Key Performance Indicators



Time Range

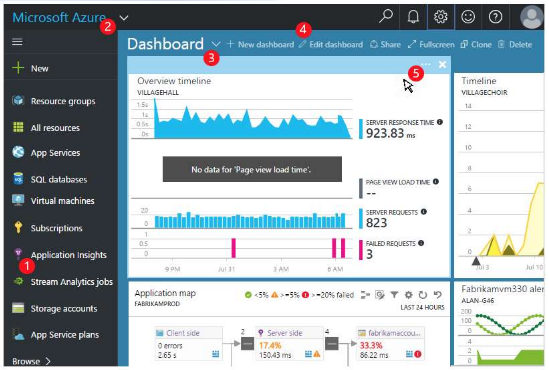
Last 30 minutes

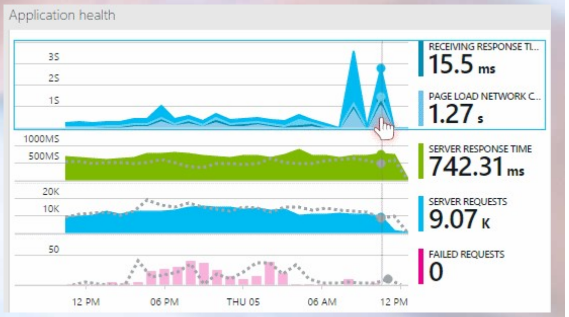
Last 24 hours

Last 7 days

Time granularity

Automatic

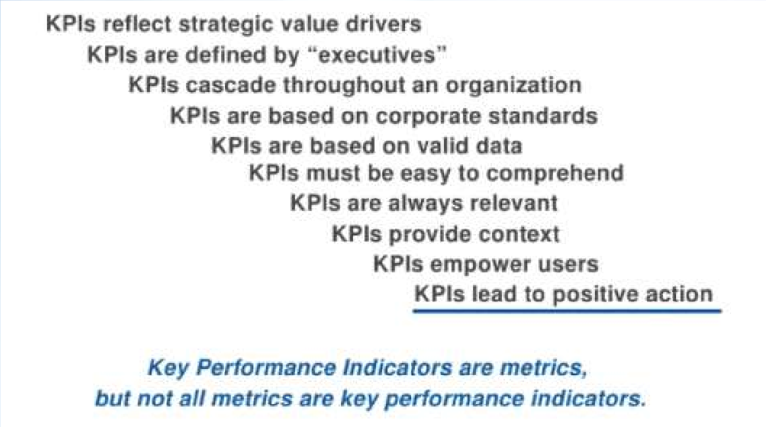




- **Discovery** through Data Collection
- **Design** of security solution based upon Interpretation of findings
- **Delivery** with specific targeted technologies and action

Security Program KPIs

10 Critical Characteristics

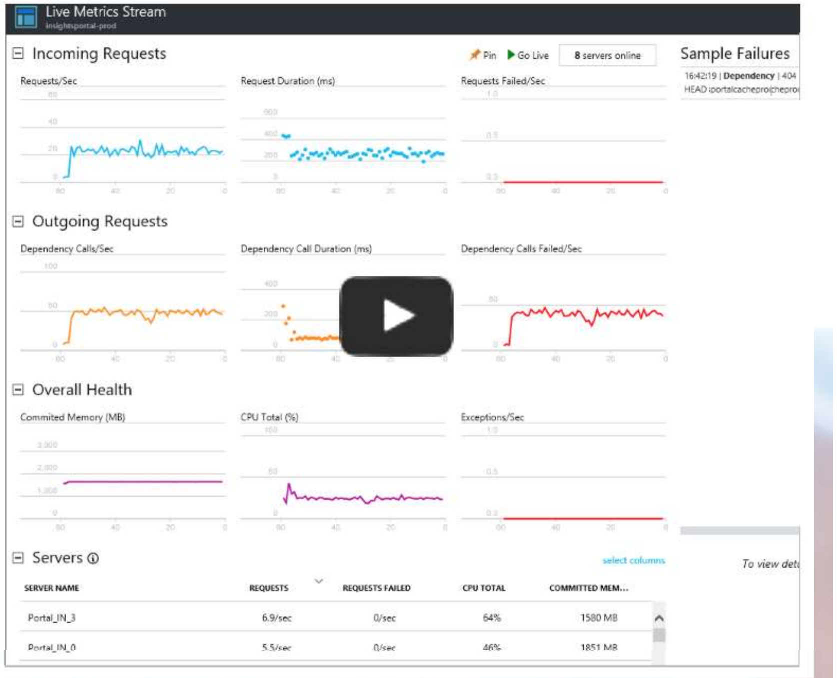


KPIs reflect strategic value drivers
KPIs are defined by “executives”
KPIs cascade throughout an organization
KPIs are based on corporate standards
KPIs are based on valid data
KPIs must be easy to comprehend
KPIs are always relevant
KPIs provide context
KPIs empower users
KPIs lead to positive action

Key Performance Indicators are metrics, but not all metrics are key performance indicators.

With Azure Live Metrics Stream, you can:

- Validate a fix while it is released, by watching performance and failure counts.
- Watch the effect of test loads, and diagnose issues live.
- Focus on particular test sessions or filter out known issues, by selecting and filtering the metrics you want to watch.
- Get exception traces as they happen.
- Experiment with filters to find the most relevant KPIs.
- Monitor any Windows performance counter live.
- Easily identify a server that is having issues, and filter all the KPI/live feed to just that server.



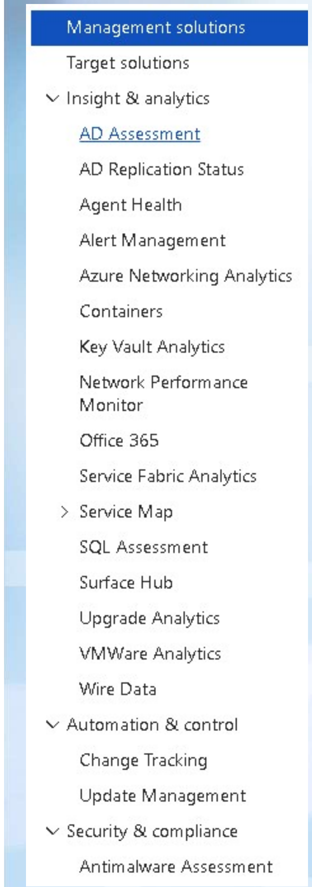
16:42:19 | **Dependency** | 404
HEAD iportalcacheprodchepro

SERVER NAME	REQUESTS	REQUESTS FAILED	CPU TOTAL	COMMITTED MEM...
Portal_IN_3	6.9/sec	0/sec	64%	1580 MB
Portal_IN_0	5.5/sec	0/sec	46%	1851 MB

Match **Biz-KPI’s** with Azure

How Presidio Brings It Together - Automation Mapping

Automation Mapping for Security Metric Development



Management solutions

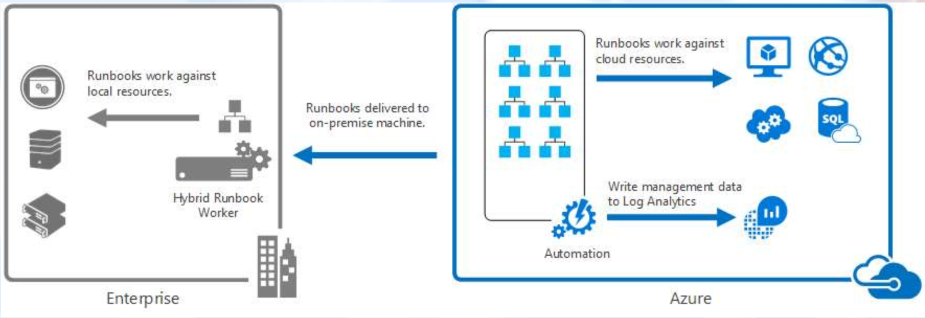
Target solutions

- Insight & analytics
  - AD Assessment
  - AD Replication Status
  - Agent Health
  - Alert Management
  - Azure Networking Analytics
  - Containers
  - Key Vault Analytics
  - Network Performance Monitor
  - Office 365
  - Service Fabric Analytics
  - Service Map
  - SQL Assessment
  - Surface Hub
  - Upgrade Analytics
  - VMWare Analytics
  - Wire Data
- Automation & control
  - Change Tracking
  - Update Management
- Security & compliance
  - Antimalware Assessment

Azure Management Solutions:

- Are prepackaged sets of logic that implement a particular management scenario leveraging one or more OMS services. Different solutions are available from Microsoft and from partners that you can easily add to your Azure subscription to increase the value of your investment in OMS. As a partner you can create your own solutions to support your applications and services and provide them to users through the Azure Marketplace or Quickstart Templates.

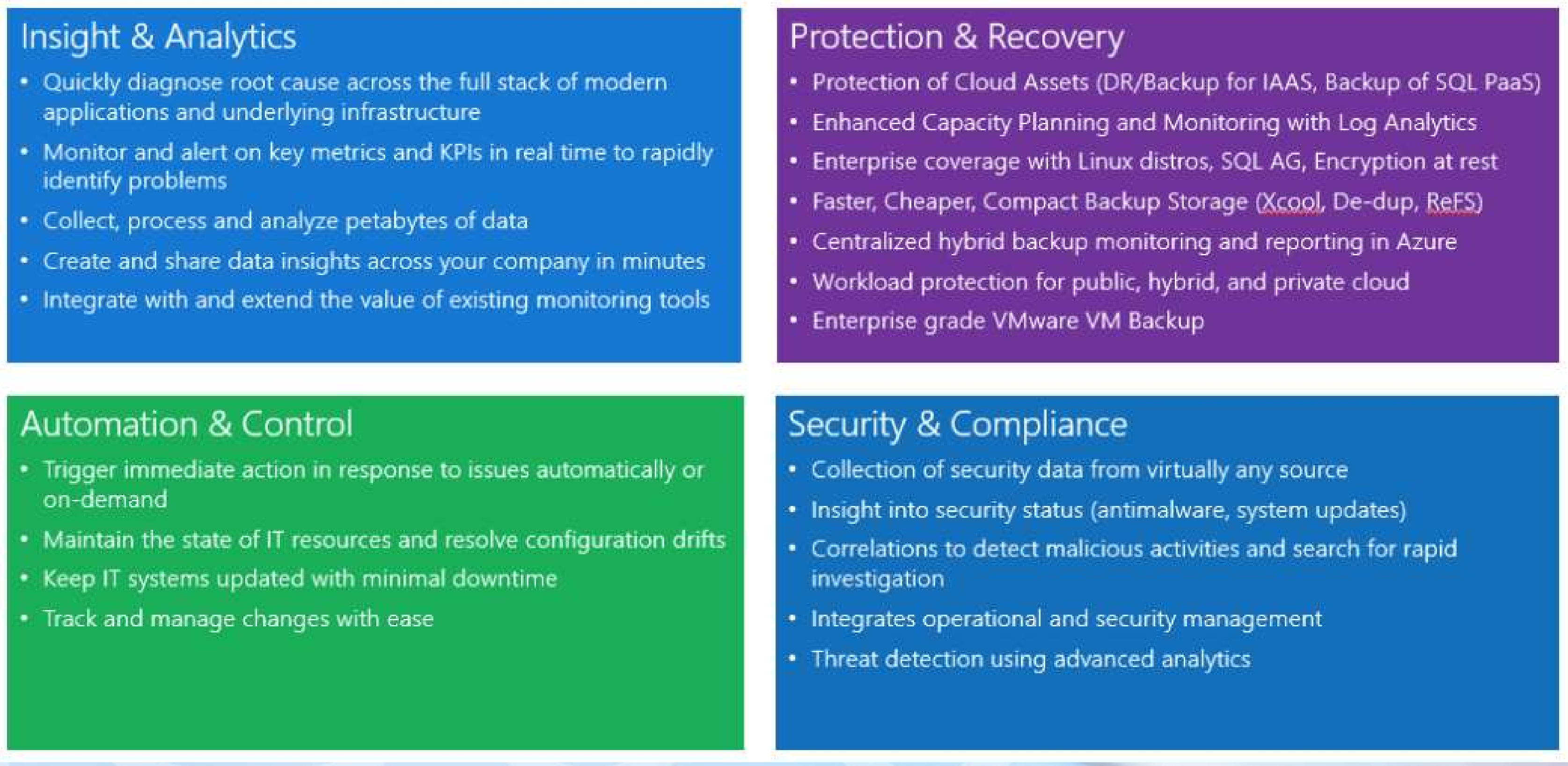
- A good example of a solution that leverages multiple services to provide additional functionality is the Update Management solution. This solution uses the Log Analytics agent for Windows and Linux to collect information about required updates on each agent. It writes this data to the Log Analytics repository where you can analyze it with an included dashboard. When you create a deployment, runbooks in Azure Automation are used to install required updates. You manage this entire process in the portal and don't need to worry about the underlying details.



Runbooks work against local resources.
Hybrid Runbook Worker
Enterprise
Runbooks delivered to on-premise machine.
Runbooks work against cloud resources.
SQL
Write management data to Log Analytics
Automation
Azure

Measurement and Analysis - Examples

Assessing the viability of your target measurements with criteria



Insight & Analytics

- Quickly diagnose root cause across the full stack of modern applications and underlying infrastructure
- Monitor and alert on key metrics and KPIs in real time to rapidly identify problems
- Collect, process and analyze petabytes of data
- Create and share data insights across your company in minutes
- Integrate with and extend the value of existing monitoring tools

Protection & Recovery

- Protection of Cloud Assets (DR/Backup for IAAS, Backup of SQL PaaS)
- Enhanced Capacity Planning and Monitoring with Log Analytics
- Enterprise coverage with Linux distros, SQL AG, Encryption at rest
- Faster, Cheaper, Compact Backup Storage (Xcool, De-dup, ReFS)
- Centralized hybrid backup monitoring and reporting in Azure
- Workload protection for public, hybrid, and private cloud
- Enterprise grade VMware VM Backup

Automation & Control

- Trigger immediate action in response to issues automatically or on-demand
- Maintain the state of IT resources and resolve configuration drifts
- Keep IT systems updated with minimal downtime
- Track and manage changes with ease

Security & Compliance

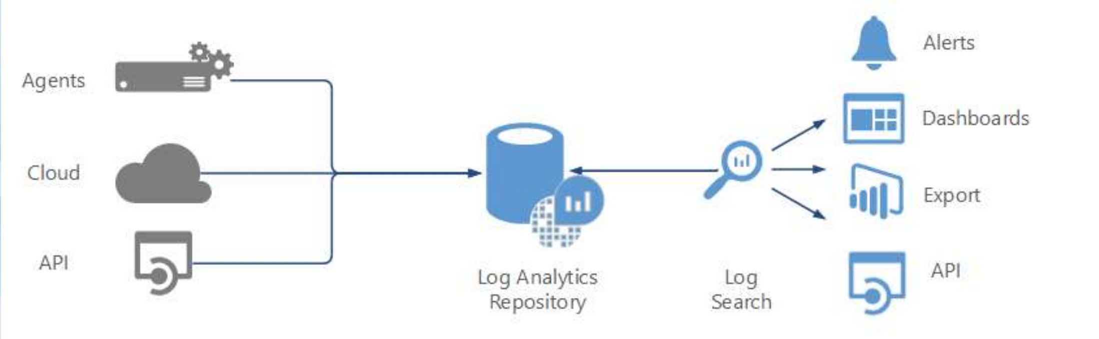
- Collection of security data from virtually any source
- Insight into security status (antimalware, system updates)
- Correlations to detect malicious activities and search for rapid investigation
- Integrates operational and security management
- Threat detection using advanced analytics

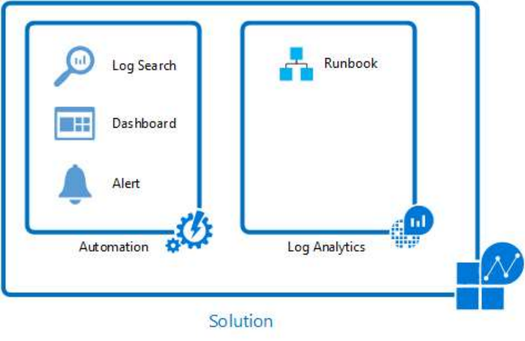
Presidio – Developing a Security Program Scorecard

Converged Reporting for Hybrid-Cloud

Automation of Azure Log Analytics service manages your cloud-based data securely by using the following methods:

- data segregation
- data retention
- physical security
- incident management
- compliance
- security standards certifications





THANK YOU

FIND OUT MORE

PRESIDIO®

Future. Built.