



Security
TRENDS 2018



클라우드 환경에서 보안과 관리

Microsoft
이건복 이사



클라우드 확산으로 인한 새로운 이슈



Security
TRENDS 2018



PC 확산 (1995+)

디렉토리 서비스
보안 패치, 모바일 장치 관리
, 접근제어



서버의 증가 (2000+)

통합관리형 보안 모델
가상화, 모니터링, 백업
부하분산



클라우드 시대 (2015+)

SaaS 관리
보안 위협
모니터링, 백업과 신속한 복구

사고와 장애는 지속적으로 발생

Another big malware attack ripples across the world

by Alanna Petroff and Selena Larson @CNMONEY

🕒 June 28, 2017, 2:14 PM ET



The Scarily Common Screw-Up That Exposed 198 Million Voter Records

Database security continues to be a major pain point. Just ask the nearly 200 million people whose personal info got left exposed on the internet.

WIRED.COM



TechCrunch @TechCrunch · Feb 28

Amazon AWS S3 outage is breaking things for a lot of websites and apps
tcm.ch/2mpOdPd by @etherington

Ukrainians Say Petya Ransomware Hides State-Sponsored Attacks

And Western cybersecurity analysts are starting to believe them.

WIRED.COM



WIRED
@WIRED

Follow

Yahoo's breach is the biggest known hack of user data ever.

The Ransomware Meltdown Experts Warned About Is Here

It's not just British hospitals. A nasty strain of ransomware is sweeping the world.

WIRED.COM

4차산업 혁명과 Digital Transformation



Security
TRENDS 2018



IT조직의 역할 변화



사업부의 요구사항



개발자

클라우드 워크로드의 증가 | 보안은 IT부서만의 일이 아님 | 관리를 위한 보안이 아닌 업무를 위한 보안

안전하고 관리된 VM들의 필요



Security
TRENDS 2018



안전하고 위협감지

운영체제 보안 패치
설치
방화벽 포트의 차단
위협의 최소화



데이터 백업

가상머신 백업
개별적인 파일을 들의 접근
신속한 복구



로그분석을 통한 통찰력 확보

시스템 모니터링
(CPU, memory & 디스크)
응용프로그램의 오류처리
시스템 오류의 분석

모든 서비스에 대한 동일한 보안상태 유지

보안문제의 변화



Security
TRENDS 2018



사업부별 상이한 시스템 구성 및
다양한 솔루션 접근경로

위협에 대한 즉각적인 분석능력의
미흡

특정 목표를 대상으로한 위협의
지속적인 증가

보안의 대응

클라우드 자원에 대한 보안



Security
TRENDS 2018

통합보안 센터의 필요성



시각화 및 제어의 필요

Unified view of security
across your Azure resources

Central management of
security policies

Integrate with existing
processes and tools like SIEM



공격에 대한 보호조치

Remediate vulnerabilities
with ongoing assessment
and recommendations

Rapidly deploy built-in security
controls and integrated partner
solutions

Reduce attack surface with
predictive analytics



위협 분석과 즉각적인 대응

Identify real threats with
advanced analytics

Gain insight into attack campaign
with Intelligent Security Graph

Remediate quickly with prioritized
alerts and recommendations

Azure Security Center 제공

비즈니스의 연속성 유지



Security
TRENDS 2018



랜섬웨어의 증가

테스트가 되지 않은 시스템플랜은
무계획과 마찬가지

고객의 기대수준의 증가
24x7운영

보호정책

데이터의 보호



Security
TRENDS 2018

클라우드를 이용한 백업과 복구 솔루션 필요



비용의 절감

No need to purchase additional hardware

No secondary site resource costs

Pay for what you use



복잡도의 최소화

Faster onboarding with cloud services

Simpler execution for testing and failover

Integrated business continuity as a service



규제의 대응

Industry-leading certification portfolio

Deploy in one of Azure's 38 global datacenters

Increase your coverage of applications to meet your compliance requirements

시스템 모니터링



Security
TRENDS 2018



의미있는 데이터와 불필요한
데이터의 분리

응급대치과정에서 과도한
시간소모

전체 자산에 대한 시각화된
대시보드의 필요성

모니터링

모니터링 및 분석



Security
TRENDS 2018

모니터링, 로그분석 및 응용프로그램 분석



IT운영팀과 개발자간의
투명하고 통합된 정보공유

Get visibility into network,
infrastructure and application code
issues

Correlate data from multiple
sources on-premises and in cloud
Single pane view built directly into
Azure

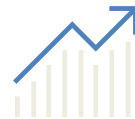


해결의 위한 평균시간의 절약

Use alerts and management
solution to accelerate resolution

Discover and map the app
and network connections

Search and query interactively at
cloud scale



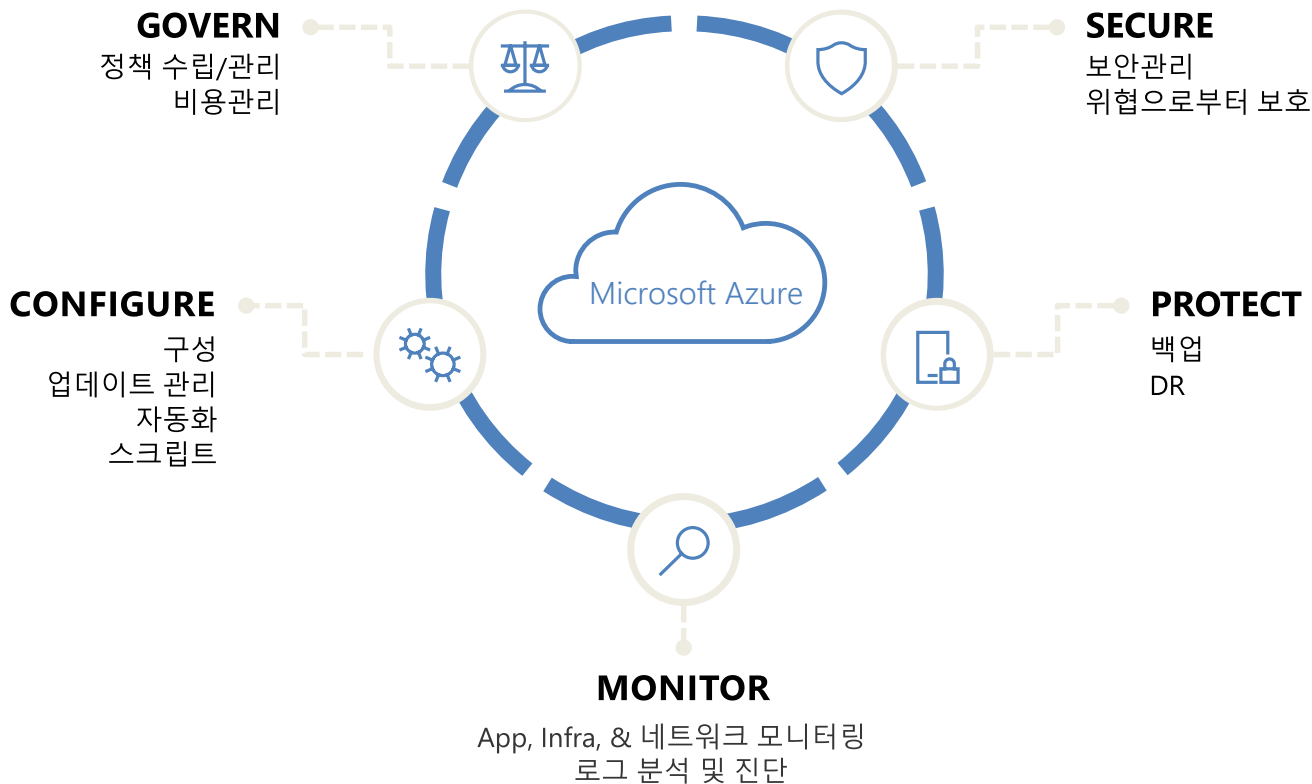
능동적인 대응을 통한
응답시간 단축

Respond to alerts immediately
using automation

Fine-tune applications based
on analytics from actual usage

Mitigate issues before they impact
users with machine learning

클라우드의기반의 보안 모델 구성



마이크로소프트 클라우드의 차이점





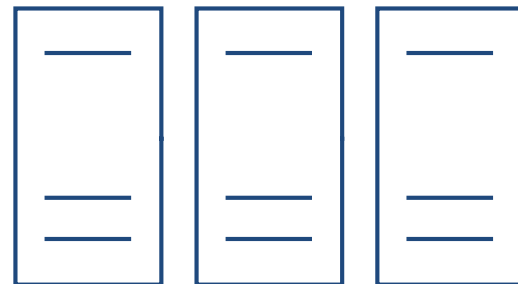
하이브리드 클라우드 시스템

클라우드와
하이브리드 환경



클라우드 전용 도구

On-premise 데이터센터



시스템센터



실시간 분석



빌트인 시스템을
통한 모니터링



유연한 시스템
통합



응용 프로그램과
연동하여 보안조치



응용 프로그램
인사이트



로그분석



모니터링

데이터유입관리서

프론트엔트



미들웨어



백엔드



운영체제



Windows Server



Linux

가상머신



네트워킹



Virtual
network



Load
balancer



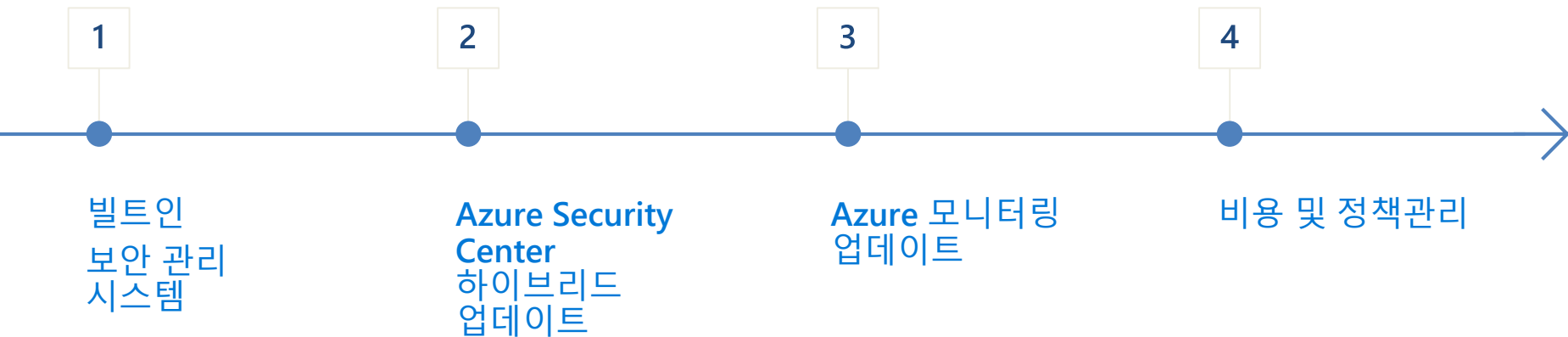
DNS



클라우드 보안관련 서비스 출시



Security
TRENDS 2018



클라우드와 통합된 경험 제공

- Quick access to Operations and Monitoring in the VM settings menu
- Scripting-based management with Cloud Shell (now with PowerShell support)
- Central monitoring services overview in Azure Monitor

The screenshot displays the Azure portal interface for a virtual machine named 'ContosoWeb'. The left-hand navigation pane includes options such as 'New', 'Dashboard', 'Virtual machines', 'Security Center', 'Log Analytics', 'Monitor', 'Application Insights', and 'Policy'. The main content area is divided into three sections: 'OPERATIONS', 'MONITORING', and 'SUPPORT + TROUBLESHOOTING'. The 'OPERATIONS' section lists actions like 'Auto-shutdown', 'Backup', 'Disaster recovery (Preview)', 'Update management (Preview)', 'Inventory (Preview)', and 'Change tracking (Preview)'. The 'MONITORING' section includes 'Metrics', 'Alert rules', 'Diagnostics settings', 'Advisor recommendations', and 'Diagram'. The 'SUPPORT + TROUBLESHOOTING' section features 'Resource health'. On the right side, the 'ContosoWeb' VM details are shown, including its status as 'Running', location as 'East US', and subscription information. Below this, a 'CPU (average)' graph is visible, showing a very low and stable CPU usage percentage over a period of time.

통합 모니터링 모델

- Secure workloads in Azure, on-premises and in other clouds now with Security Center
- Adaptive application controls (whitelisting)
- Interactive investigation mapping

The screenshot displays the Microsoft Azure Security Center interface. The top section is titled "Create application whitelisting rules" and includes a description of the process. Below this, there are two sections for selecting resources to whitelist:

- Select VMs to whitelist:** A table with columns for "VIRTUAL MACHINE", "STATE", and "SEVERITY". One VM, "res-azadsl1", is selected and its state is "Open".
- Select processes for whitelisting rules:** A table with columns for "NAME", "PROCESSES", "COMMON", and "EXPLOITABLE". Several process folders are listed, including "C:\Packages\Plugins", "C:\Windows\System32", "C:\Windows\azure\GuestAgent_2,7.1108.832", and "C:\Program Files".

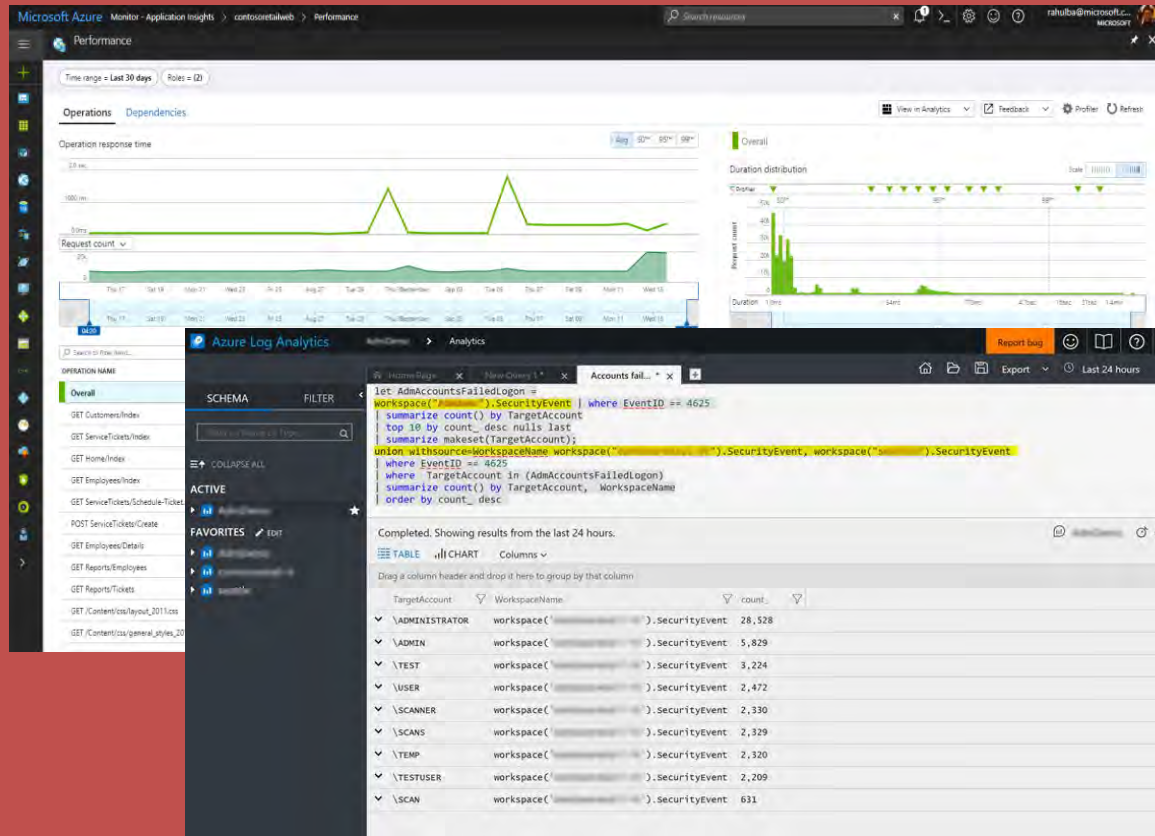
The bottom section is the "Investigation Dashboard (Preview)". It shows an "Investigation path" and a "Security incident detected" notification. The incident details include:

- Alert details:** The incident started on 09/19/2017 13:40:20 and was most recently detected on 09/19/2017 13:26:13. The description states that an attacker has attacked other resources from a virtual machine named "ContosoWebFE1".
- Alert ID:** 2518964759722139231_6649d222-8709-4b34-99dd-4e728759d441
- Time Generated:** 9/19/2017 7:09:52.000 AM
- Start Time (UTC):** 2017-09-19T13:40:20Z
- Detected Time (UTC):** 2017-09-19T13:26:13Z
- Compromised Host:** ContosoWebFE1
- Incident Stage:** attacked other resources from
- Severity:** High
- Reporting System:** (partially visible)

The dashboard also features an interactive investigation mapping diagram showing the flow of the incident, with nodes for "Successful ADP route for...", "Security Incident Detected", "Suspicious SVOHOST process...", "ContosoWebFE1", and "Apriori".

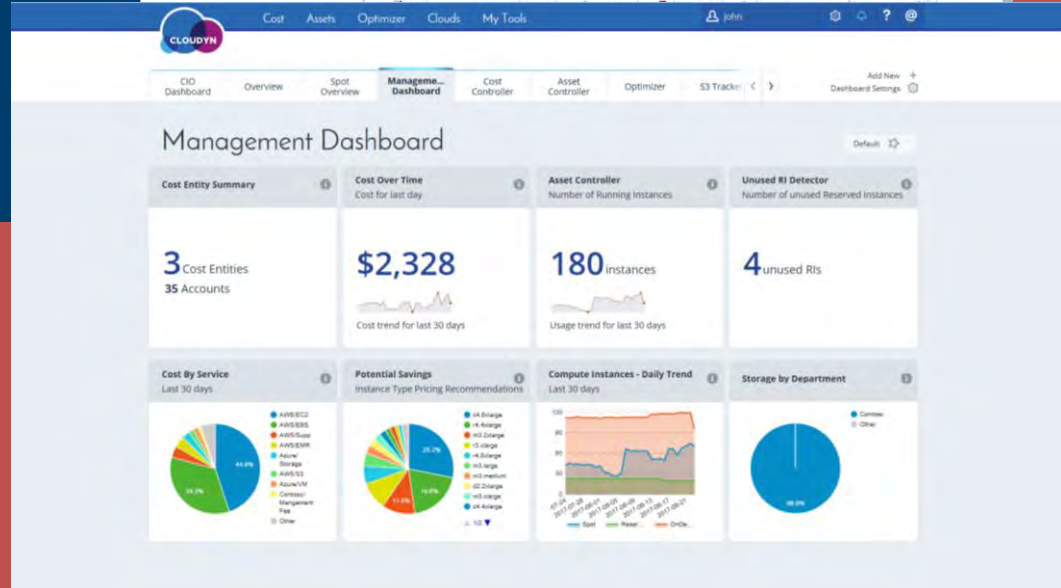
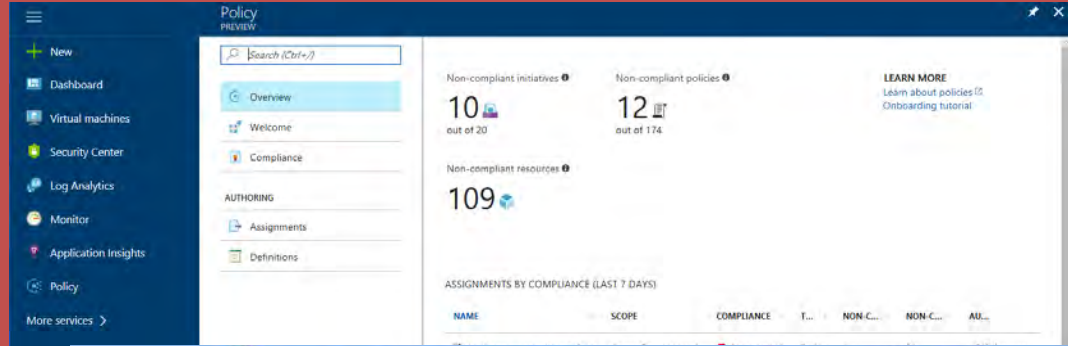
업데이트된 모니터링 도구

- Updated Application Insights performance monitoring and failure diagnostics experience
- Optimized Log Analytics experience using new query language
- Integrated Azure alerts with ITSM tools



비용의 모니터링

- Azure Cost Management by Cloudfy now available, free for Azure customers
- Limited preview of Azure Policy for enterprise-wide governance



신속한 보안 모델을 통한 혁신



Security
TRENDS 2018



모니터링

Log Analytics | Application Insights | Automation

- Custom Solutions (SDK)
- Azure Activity Logs
- OMS Gateway
- Service Map Preview
- Azure Monitor Preview
- Network Monitor (NPM)
- Service Map (GA)
- Network Performance monitor (GA)
- ITSM connector
- Azure Alert Remediation Integration
- Graphical runbook support for native PowerShell
- Integration with Azure Scheduler and Webhook
- Interactive Powershell in Azure portal



운영

Azure Backup | Azure Site Recovery | Configuration

- IaaS VM Backup for Premium Storage
- VMWare VM backup
- Azure SQL Native backup experience
- Backup of VMs encrypted with Azure Disk Encryption
- Exclude disk & Premium Storage support for recover to Azure
- Encryption at rest
- DR support for Azure IaaS
- Recover files/folders of IaaS VM backup
- Patch across Windows and Linux
- Windows File and Process change tracking



보안

Azure Security Center

- Vulnerability assessment
- Additional threat detections
- Enhanced security incidents
- Threat Intelligence Reports
- Symantec and Trend-Micro for Malware assessment solution
- Support for Common Event Format (CEF) logs
- JIT access to network ports & app whitelisting on Azure IaaS VMs

클라우드 기반 보안 모델 강화

고객 사례



Log Analytics, Security Center, Backup, Site Recovery

“

That was why Azure security and management services were chosen. It gave us that global view with a minimal amount of administrative effort.”

— Adeel Abbas,
Manager of Global Technology
Enterprise Systems, IHG

Azure Security Center

“

The prospect of having a single dashboard where we can prevent, detect, and respond to threats with increased visibility and control over our resources was very exciting... Today, our operations team saves at least 30 percent of its time by using Azure Security Center.”

— Monish Darda
Co-founder and
Chief Technology Officer

Azure Backup

“

We don't have to worry about managing space on expensive purpose-built backup storage systems. We have no tape costs, management costs, nothing. Backup is dramatically cheaper with Azure.”

— Sean DeLessio
Lead Engineer,
Distributed Infrastructure Team

자세한 고객 사례는 customers.microsoft.com

Q&A





Security
TRENDS 2018

감사합니다.

Microsoft
이건복

