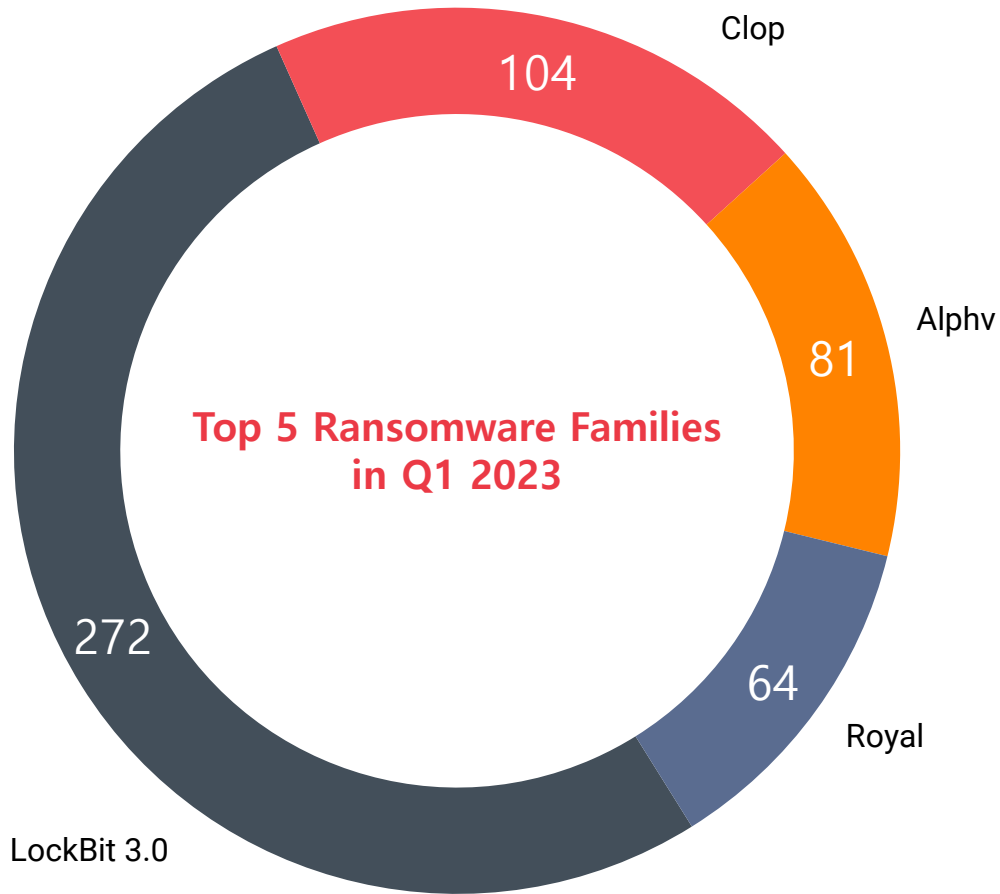


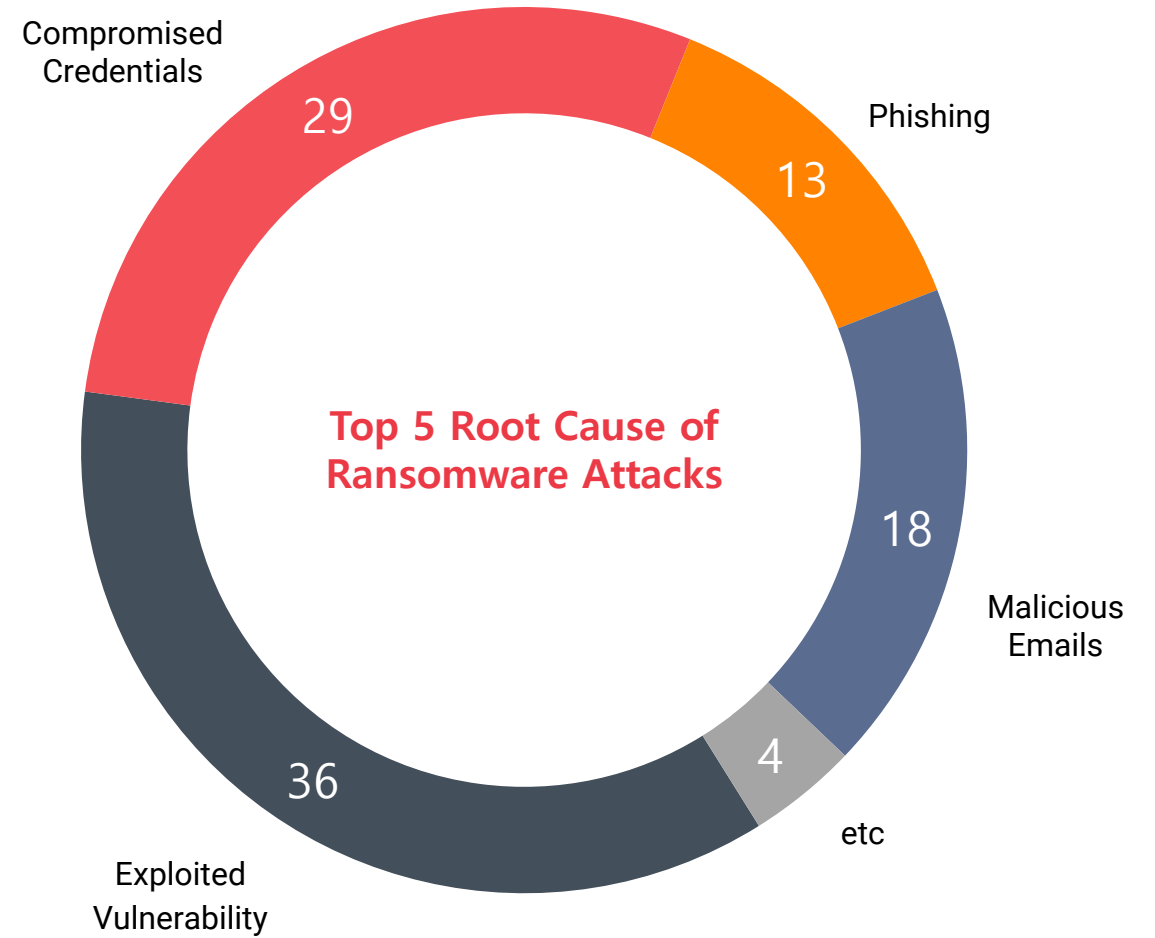
VMware가 제시하는 랜섬웨어 방어 및 복구 전략

VMware의 내재화된 보안을 통한 랜섬웨어 대응

랜섬웨어 위협 동향



Cyberint : Top 10 ransomware Families in Q1



Sophos : The State of Ransomware 2023

랜섬웨어 공격 절차



탐색/정찰:
공격대상
시스템 취약점 스캔



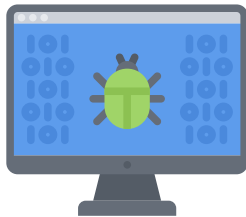
권한 상승:
더 높은 권한을 가진 도메인, 시스템
관리자 계정 확보/생성



데이터 유출:
데이터 도용/
C&C 서버 전송



랜섬웨어 배포:
데이터 암호화/
금전 요구



공격 기반 구축:
해킹툴 등을 활용한 계정 정보 탈취 및
초기진입 경로 확보



파일 실행:
악성 프로세스 실행, 지속적인
접근을 위한 악성 소프트웨어 설치

랜섬웨어 공격 전술

Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Phishing (0/3)	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/7)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (0/2)
Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Trusted Relationship	Scheduled Task/Job (1/5)	Create or Modify System Process (0/4)	Escape to Host	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Exfiltration Over Web Service (0/3)	Firmware Corruption
Valid Accounts (0/4)	Serverless Execution	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Network Denial of Service (0/2)	Inhibit System Recovery
	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (0/2)
	Software Deployment Tools	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
	System Services (0/2)	Implant Internal Image	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery	Network Service Discovery	Data from Removable Media	Protocol Tunneling		Service Stop
	User Execution (0/3)	Modify Authentication Process (0/8)	Scheduled Task/Job (1/5)	Hide Artifacts (0/10)	Steal Application Access Token	Group Policy Discovery	Network Share Discovery	Data from Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
	Windows Management Instrumentation	Office Application Startup (0/6)	Valid Accounts (0/4)	Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	Network Sniffing	Network Sniffing	Email Collection (0/3)	Remote Access Software		
		Pre-OS Boot (0/5)		Hijack Execution Flow (0/12)	Steal or Forge Kerberos Tickets (0/4)	Password Policy Discovery	Network Sniffing	Input Capture (0/4)	Traffic Signaling (0/2)		
		Scheduled Task/Job (1/5)		Impair Defenses (0/10)	Steal Web Session Cookie	Peripheral Device Discovery	OS Credential Dumping (0/8)	Screen Capture	Web Service (0/3)		
		Server Software Component (0/5)		Indicator Removal (0/8)	Unsecured Credentials (0/8)	Permission Groups Discovery (0/3)	Steal Application Access Token	Video Capture			
		Traffic Signaling (0/2)		Indirect Command Execution		Process Discovery	Steal or Forge Authentication Certificates				
		Valid Accounts (0/4)		Masquerading (0/8)		Query Registry	Steal or Forge Kerberos Tickets (0/4)				
				Modify Authentication Process (0/8)		Remote System Discovery	Steal Web Session Cookie				
				Modify Cloud Compute Infrastructure (0/4)		Software Discovery (0/1)	Unsecured Credentials (0/8)				
				Modify Registry		System Information Discovery					
				Modify System Image (0/2)		System Location Discovery (0/1)					
				Network Boundary Bridging (0/1)		System Network Configuration Discovery (0/1)					
				Obfuscated Files or Information (0/11)		System Network Connections Discovery					
				Plist File Modification							

NIST 사이버 보안 프레임워크

RECOVER - 복구

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RESPOND - 대응

- Recovery Planning
- Improvements
- Communications



DETECT - 탐지

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

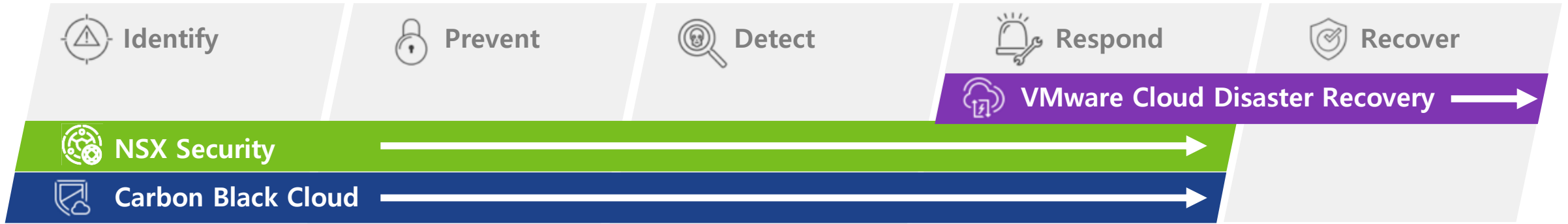
IDENTIFY - 식별





























- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT - 보호

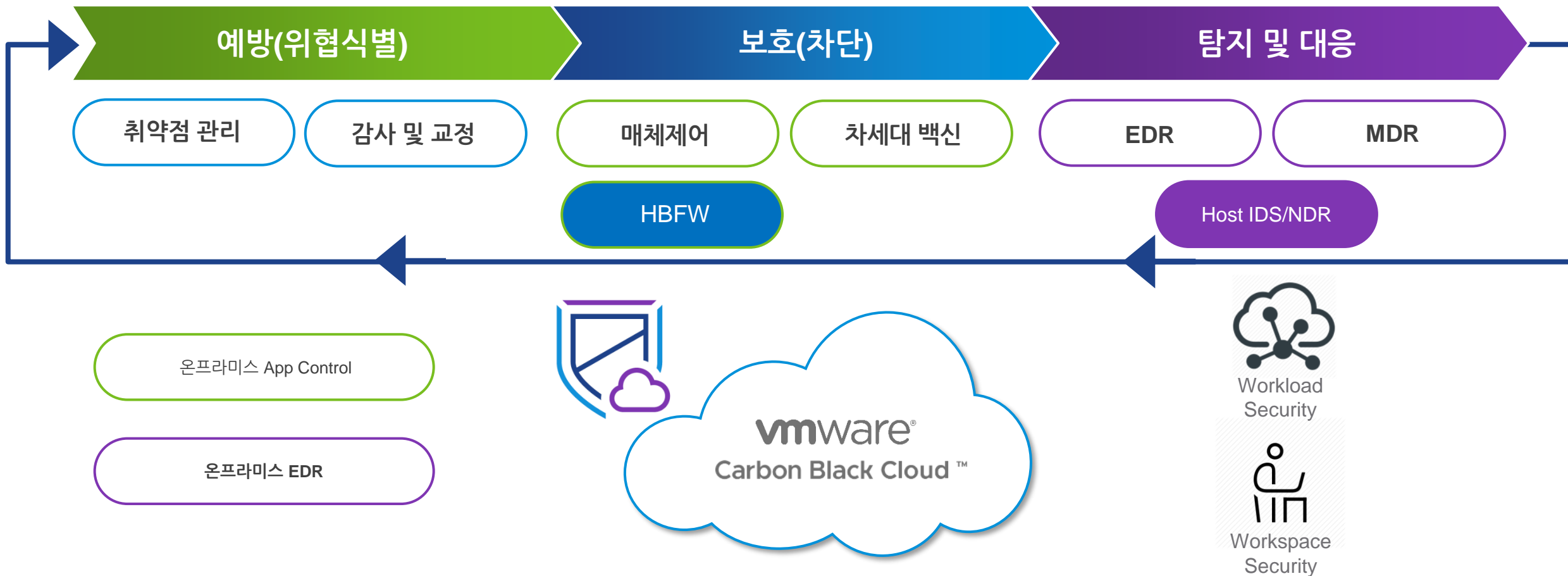
- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

VMware 랜섬웨어 대응 솔루션



- | | | | | |
|---|---|--|--|---|
|  Vulnerability Assessment |  Next Gen Anti-Virus Prevention Capabilities |  Forensic Investigations |  SOAR Integration |  Delta-based Fallback |
|  Audit & Remediation |  Network Segmentations |  Endpoint Detection & Response |  Remote Response Capabilities |  Review, Audit & Remediate |
|  Baseline Network Environment |  IDS/IPS/Deep Packet Inspection |  Signature-based & Behavior-based Detection |  Network Quarantine | |
|  High Value Assets Tagging |  Attack Surface Reduction |  Signature-based & Behavior-based detection (Network) |  Network Resets | |
|  Flow Visualization |  Micro-segmentation |  Micro-segmentation |  Allow/Deny | |
|  DR Plan Config, Test, Check |  Malware Prevention |  Malware Prevention |  Failover to Recovery Site | |
|  Application Dependency Mapping | | |  Identify VM Snapshot | |

VMware Carbon Black 엔드포인트 보안 플랫폼



Windows



Mac



Linux



Azure



GCP



AWS



vSphere



Container

Carbon Black – 식별 (Identify)

랜섬웨어를 포함한 다양한 공격에 활용되는 취약점 관리 및 운영 환경 점검



취약점 평가

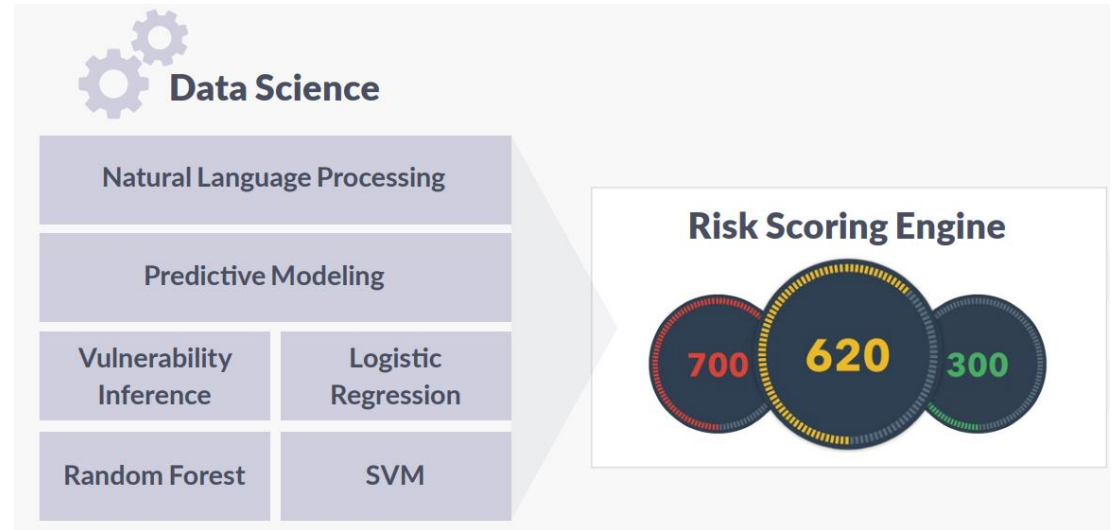
워크로드, 엔드포인트 및 컨테이너 운영 환경의 취약점 검색 및 진단
랜섬웨어를 포함한 다양한 사이버 보안 위협에 노출될 수 있는 취약점 우선순위 선정



감사 및 조치

워크로드, 엔드포인트 및 컨테이너 운영 환경의 취약점 검색 및 진단
랜섬웨어를 포함한 다양한 사이버 보안 위협에 노출될 수 있는 취약점 우선순위 선정

KENNA
Security



Carbon Black – 식별 (취약점 평가)

vm Carbon Black Cloud

Notifications > Help > Sungyoon Cho (vmw-internal-se-asia.com) >

3h 1d 1w 2w 1m All Custom All policies [Filter Icon]

vmw-internal-se-asi... Add Widget [Download Icon]

Endpoint Status

TOTAL 897

- Active: 59
- Inactive: 830
- Quarantined: 1
- Bypass: 7

Time frame not applied

Prevented Malware

TOTAL 248

- Known Malware: 55
- Suspect Malware: 6
- Non-Malware: 172
- PUPs: 15

Alert severity not applied

VM Workloads Overview

Enabled	303
Not enabled	409
VMware Tools update required	76
Not supported	86

VMs with Critical Vulnerabilities

TOTAL 110

- Windows OS: 110
- Linux OS: 0

Filters not applied

Critical Vulnerabilities on Endpoints

TOTAL 39

- Windows OS: 11
- Linux OS: 0
- Windows App: 28
- Linux App: 0

Filters not applied

Top Alerted Applications

APPLICATION	ALERTS
explorer.exe	80
chrome.exe	57
setup.exe	36
powershell.exe	29
repmgr.exe	28
msedge.exe	27
cmd.exe	20
msiexec.exe	17
7z.exe	16

Carbon Black – 식별 (취약점 평가)

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

9,720 Total Vulnerabilities

VULNERABILITIES

🔒 CVE-2023-2033 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.


Description

Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 NIST: NVD Base Score: **8.8 HIGH** Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-2033

NVD Published Date:
04/14/2023

NVD Last Modified:
05/01/2023

Source:
Chrome

CVE ID	App	Product	Version	Severity	Published	Affected Endpoints
CVE-2023-21716	App	Microsoft Windows Server 2019	10.0.17763	Critical (10)	Feb 15, 2023	1
CVE-2023-2033	App	Microsoft Office Professional Plus 2019	16.0.10394.20022	Critical (10)	Feb 15, 2023	1

Carbon Black – 보호/탐지 (Protect/Detect)

알려진/알려지지 않은 랜섬웨어/멀웨어 차단



Cloud Reputation

시그니처 기반 차단

차세대 백신,
클라우드
머신 러닝을 통한
시그니처/평판
실시간 업데이트



AMSI 차단

악성 스크립트 자동 분석 및 차단

PowerShell 스크립트,
오피스 매크로 등에
대해 Anti-Malware
Scanning Interface)
방지 기능 사용



정책 기반 차단 룰

알려지지 않은
Zero-day
악성코드 차단

사용자 정책 적용을
통한 다양한 사용자
운영 환경 적용



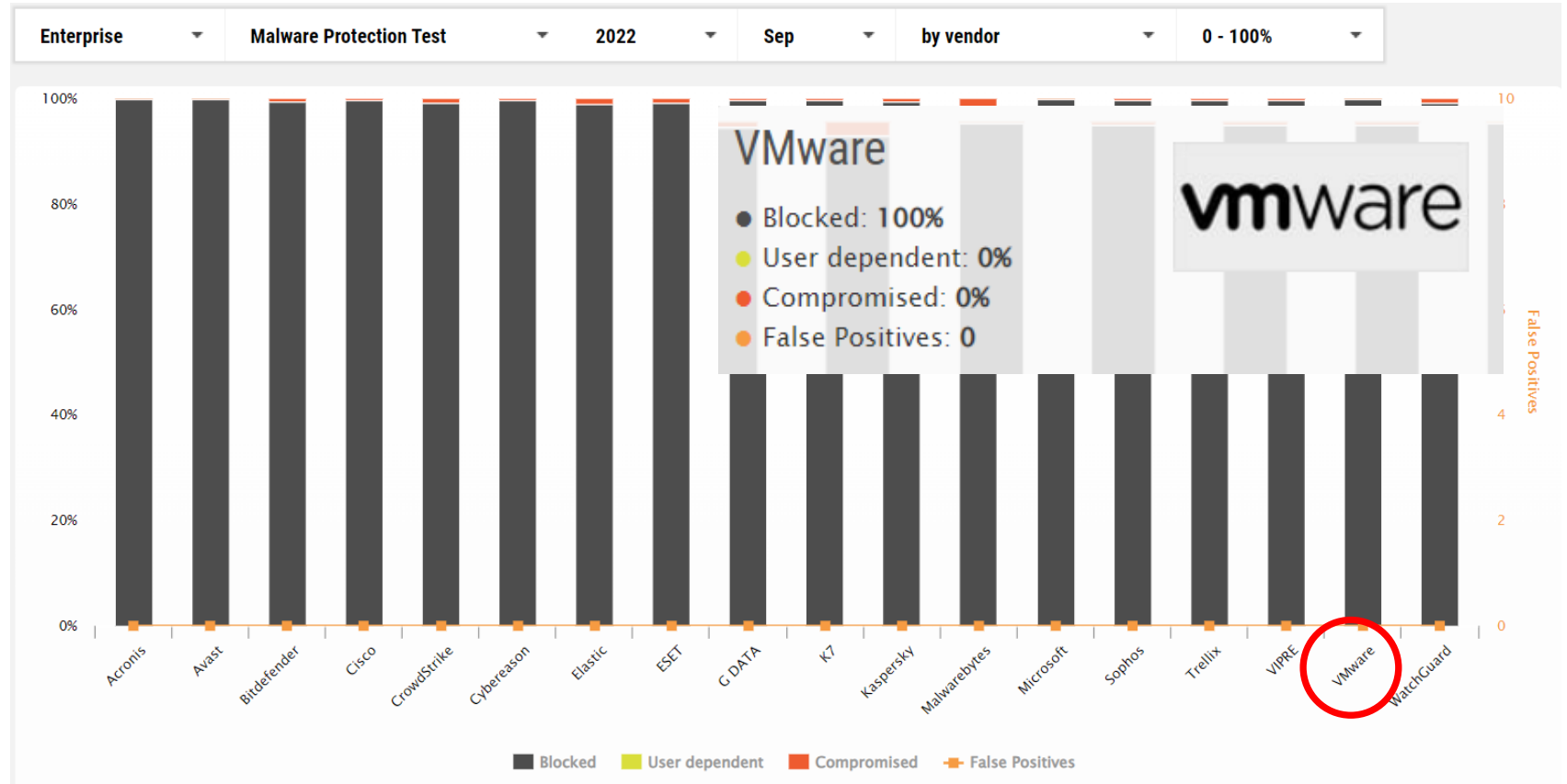
Canary 파일

암호화 방지 위한
Decoy 파일 생성

VSS 복사본 및
MBR 액세스 차단

Carbon Black – 보호/탐지 (Protect/Detect)

업계 최고의 NGAV 기능



Carbon Black – 보호/탐지 (Protect/Detect)

20개 이상의 위협 인텔리전스 정보를 수집된 정보와 매핑 제공

Carbon Black Cloud

클라우드 및 엔드포인트 환경의
카본블랙 센서



Carbon Black Cloud

위협 인텔리전스



컨텍스트 기반 위협 대응



Carbon Black TAU 위협 인텔리전스 피드

- Reputation Threat
- Advanced Threats
- Early Access
- Endpoint Visibility
- Endpoint Suspicious Indicators
- Banning Events
- EMET Protection
- AMSI Threat Intelligence
- CBLK Community
- Known IOC FEED
- CB Inspection
- Bit9+Carbon Black

3rd 파티 벤더 위협 인텔리전스 피드



Carbon Black – 대응 (Respond)

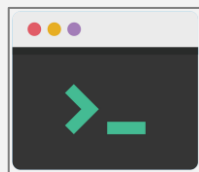
알려진/알려지지 않은 랜섬웨어/멀웨어 차단



Quarantine

원격 네트워크 격리

랜섬웨어 혹은 위협에 노출된 시스템을 내부 확산 방지를 위해 원격 격리



Live Response

전용 리모트 셸 명령

- 상세 조사를 위한 추가 정보 검색
- 악성코드 제거 / 복구 작업
- 표준 구현된 다수의 명령어 활용



File Deletion

원격 파일 제어

랜섬웨어 원본, 악성 행위에 사용된 파일을 원격지에서 원클릭으로 삭제



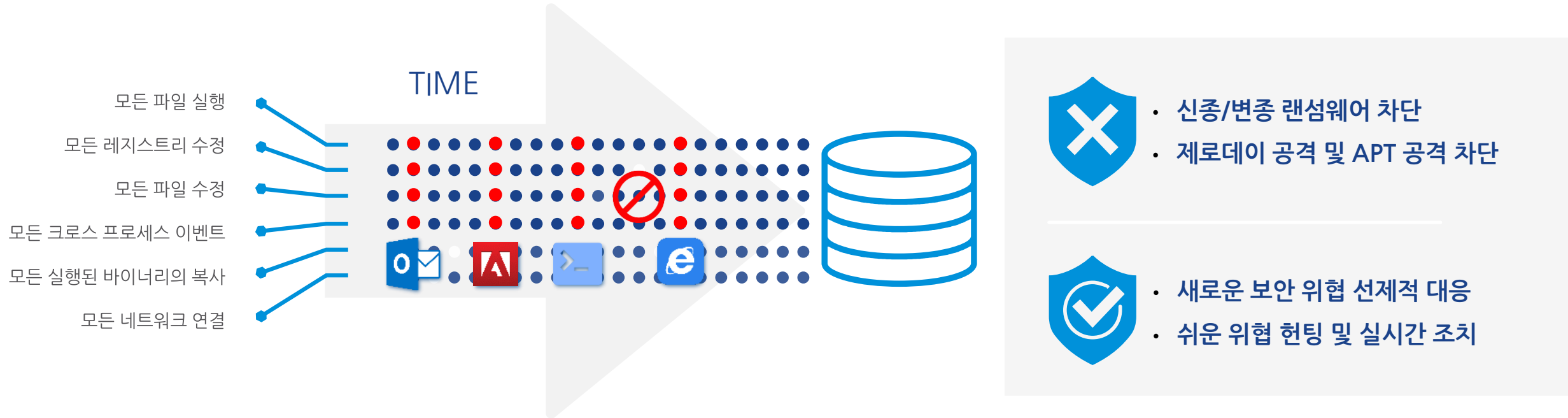
Ban/Approval

금지/허용 관리

파일 Hash, 실행 경로, 인증서, 신뢰 수준 등 다양한 시스템 항목에 대한 적용

Carbon Black – 대응 (Respond)

필터링 없는 Unfiltered Data 모든 프로세스 및 네트워크 행위 수집



모든 데이터를 지속적으로 수집해서 중앙 저장하여 킬체인
기반 공격 대응과 포렌식 수준 데이터

Carbon Black – Respond

랜섬웨어 모든 행위 가시화 및 TTP 등 추가 인텔리전스 정보 제공

PROCESS ANALYSIS

Primary Process Selected Process 9:13:55 pm Jul 2, 2023
powershell.exe

DEVELOPER DETAILS:
Group by hash

ALERT BEHAVIORS BASED ON SEVERITY

All Behaviors

- network_access
- unknown_app
- active_client
- run_malware_app
- detected_malware_app
- run_another_app
- modify_memory_protection
- malware_app
- code_drop
- run_cmd_shell
- run_unknown_app
- malware_drop
- run_system_utility
- run_system_app
- fileless
- mitre_t1106_native_api
- mitre_t1059_003_win_cmd_shell
- mitre_t1059_cmd_line_or_script_inter

Includes all behaviors associated with alert d80c5baf-c3ba-4ecf-8925-82f85a3cec90

ALERT NOTES & TAGS

Add note (0/255)

Add tag

Take Action

More

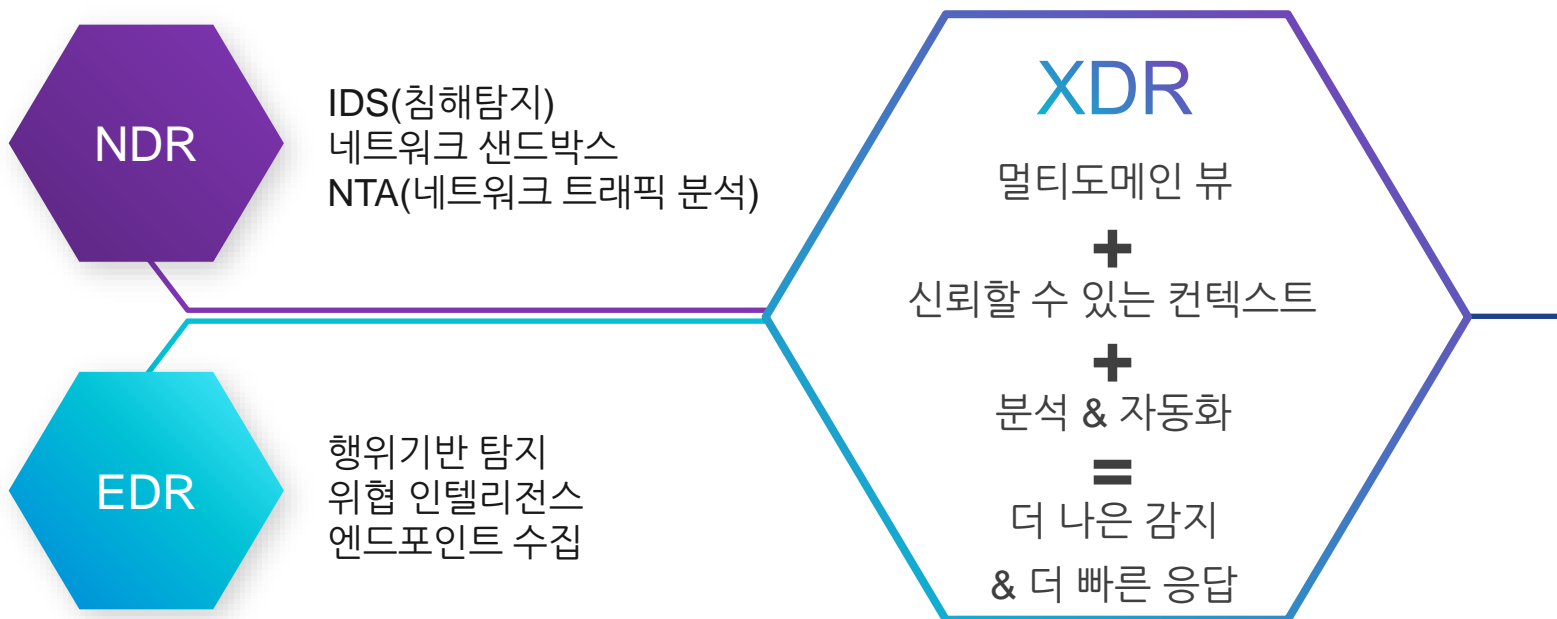
Binary Details

Privileges: Elevated True, Integrity System, Privileges SeBackupPrivilege

VMware Carbon Black – XDR

EDR + NDR 기능 통합

단일 콘솔에서 EDR, NDR 적용 및 양방향 위협 정보 분석/통합



- 풍부하고 상세한 네트워크 원격 측정 가시성(NDR)
- 네트워크 공격 경보를 위한 **Lastline Analytics**

APPLICATION LAYER DETAILS

Webrequest

Method GET

URL /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ff2f0571a1dc886a

Headers Host:ctldl.windowsupdate.com
Accept:/*/*
Connection:Keep-Alive
User-Agent:Microsoft-CryptoAPI/10.0
If-None-Match:"08f5ab0361ad71:0"
If-Modified-Since:Tue, 16 Mar 2021 07:33:42 GMT

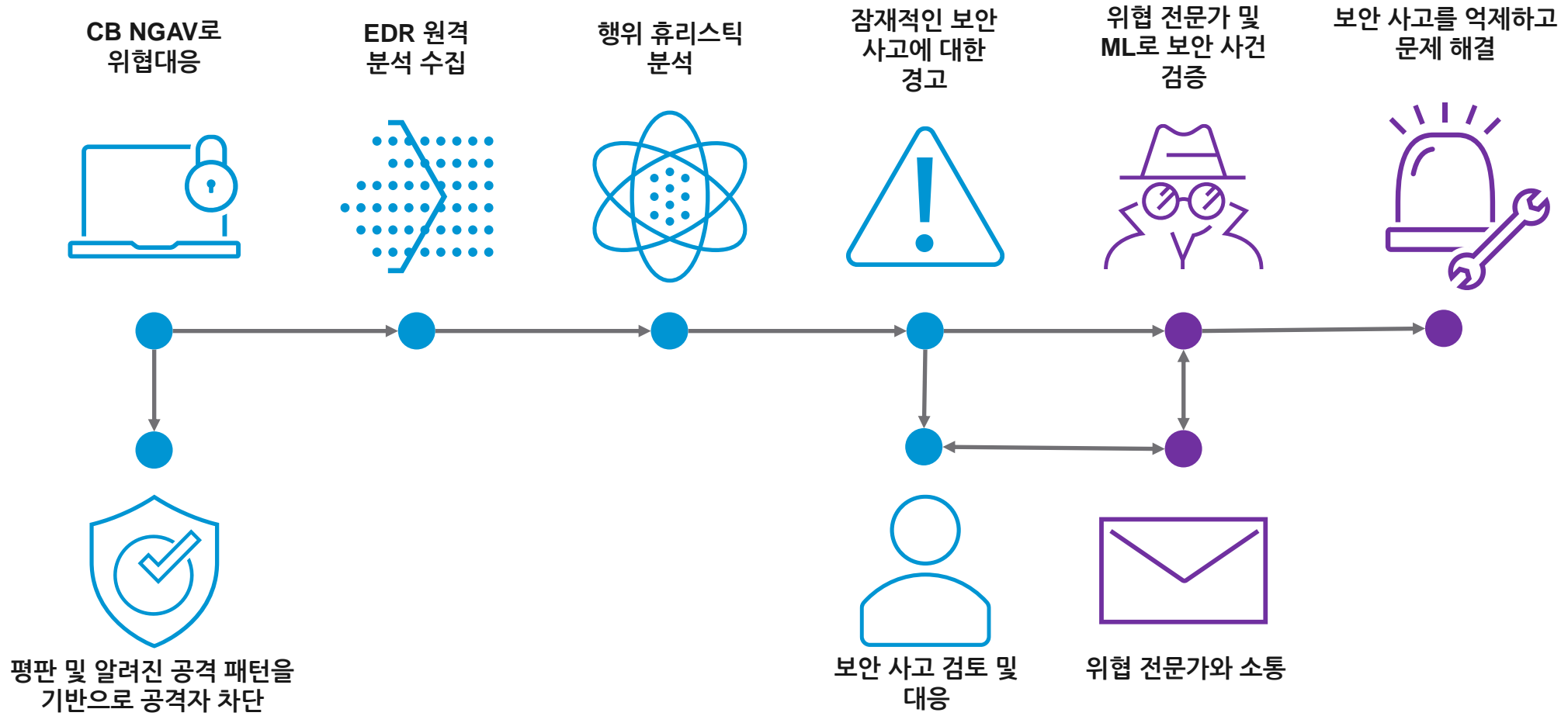
Response

Status Code 304

Headers Date:Fri, 16 Sep 2022 17:25:20 GMT
ETag:"08f5ab0361ad71:0"
X-CCC:US
X-CID:2
Connection:keep-alive
Content-Type:application/vnd.ms-cab-compressed
Cache-Control:public,max-age=900
Last-Modified:Tue, 16 Mar 2021 07:33:42 GMT

Carbon Black – MDR (Managed Detection & Response)

고객 환경의 위협에 대한 24/7 통찰력 및 대응 & PoC 지원



차세대 안티바이러스(NGAV)

Managed Detection and Response

» 가상 클라우드 네트워크 및 보안 솔루션

네트워크, 보안 관리, 자동화

클라우드 기반의 관리	워크로드 자동화	블루프린트 / 템플릿	통찰력 / 파악	가시성
<p>Aria Operations for Network 네트워크 디스커버리 및 통찰력 제공</p>		<p>Aria Automation 엔드 투 엔드 워크로드 자동화</p>		

네트워크, 보안 가상화

보안	통합	확장성	자동화	유연성
<p>NSX 데이터센터 데이터센터 워크로드를 위한 네트워킹 및 보안 풀 패키지</p>	<p>NSX 클라우드 퍼블릭 클라우드 워크로드를 위한 네트워킹 및 보안 풀 패키지</p>	<p>NSX 인텔리전스 보안 가시성, 정책 관리, 고급 분석 & 컴플라이언스 준수</p>	<p>NSX 분산 IDS/IPS 위협 보호와 컴플라이언스 준수를 위한 컨텍스트 기반의 분산 IDPS</p>	
<p>NSX 고급 로드밸런서 (ALB) 멀티 클라우드 SW 로드밸런서, WAF 및 애플리케이션 성능 분석</p>	<p>NSX 서비스 메시 클라우드 네이티브 워크로드를 위한 네트워킹과 보안</p>	<p>NSX 하이브리드 커넥트 (HCX) 데이터센터 및 클라우드 워크로드 마이그레이션 도구</p>	<p>NSX VeloCloud SD-WAN 원격 지점의 비즈니스 연속성과 보안을 보장하는 에지 네트워크</p>	

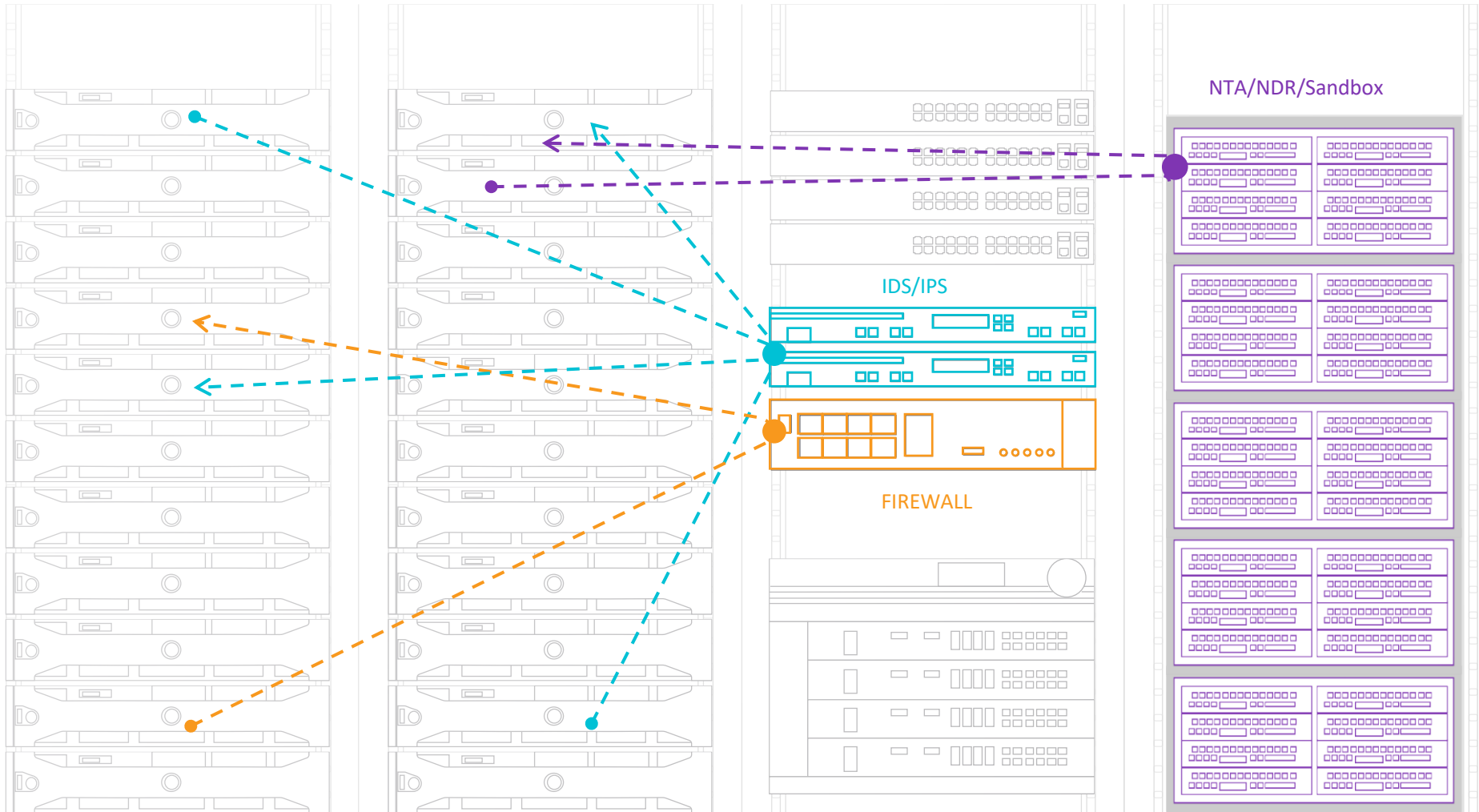
» 내재된 보안



탄력적 규모 | 애플리케이션 인식 | 네트워크 변경 없음 | 정책 자동화

East-West 보안을 위한 전통적인 아키텍처

» 랜섬웨어 대응에 취약한 비효율적인 구조



현실

네트워크에 복잡하게 삽입 필요

동적 확장 / 축소 불가

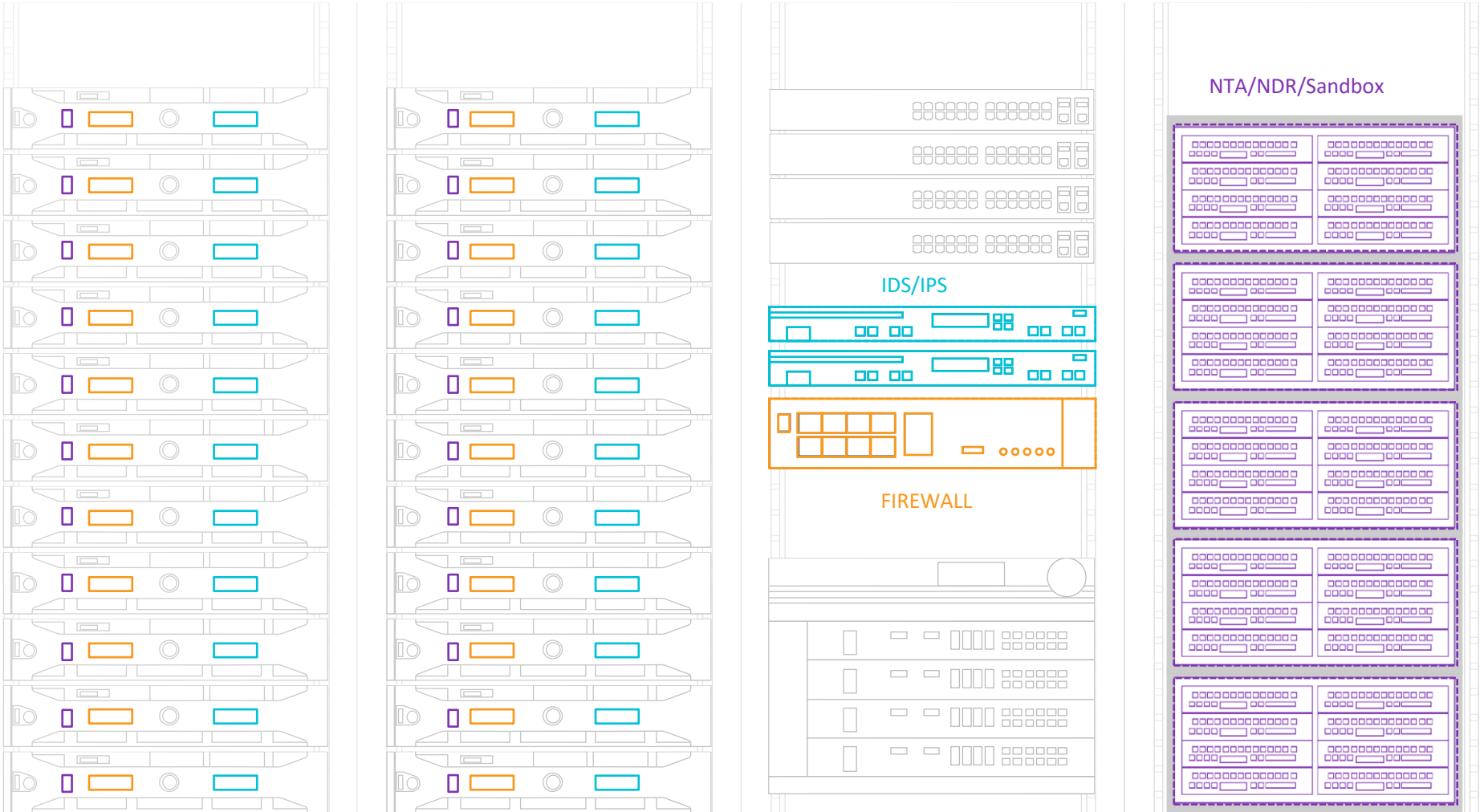
사각지대 존재 및 컨트롤 부족

정책의 일관성 부재

고비용 구조 (HW, SW,
유지보수, 전력, 쿨링, 케이블링,
랙 상면 등)

East-West 보안을 위한 현대화된 NSX 분산 아키텍처

» 랜섬웨어 대응에 최적화



솔루션

고급 위협 방지 기능을 갖춘 커널 기반 L4-7 방화벽

분산 아키텍처로 트래픽 헤어핀 제거

단일 관리 콘솔

간편한 구현 - 물리적 환경 변경 필요 없음

민첩성(자동 정책 프로비저닝/프로비저닝 해제)

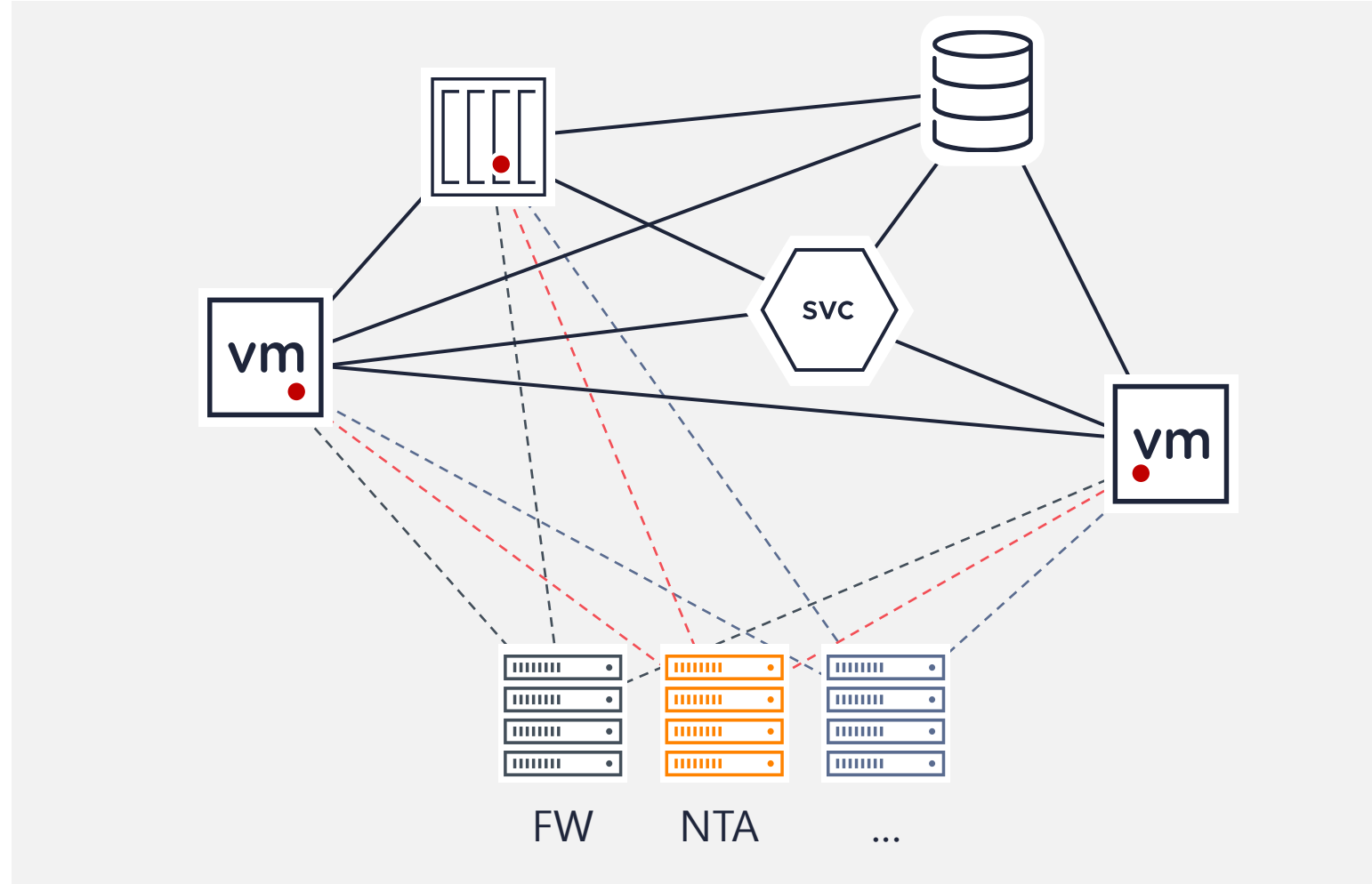
모든 워크로드 및 멀티 클라우드에서 일관된 정책 제공
비용 효율성 향상(최대 70% 이상 절감)

NSX Security – 식별 (Identify)

» 모든 흐름 수집/시각화, 기준 설정 및 세분화 정책 권장

분석에 대한 전통적인 접근 방식

- 대형 중앙집중식 어플라이언스
- 중복된 트래픽
- 네트워크 저하
- 운영 복잡성
- 제한된 컨텍스트 및 샘플링



NSX Security – 식별 (Identify)

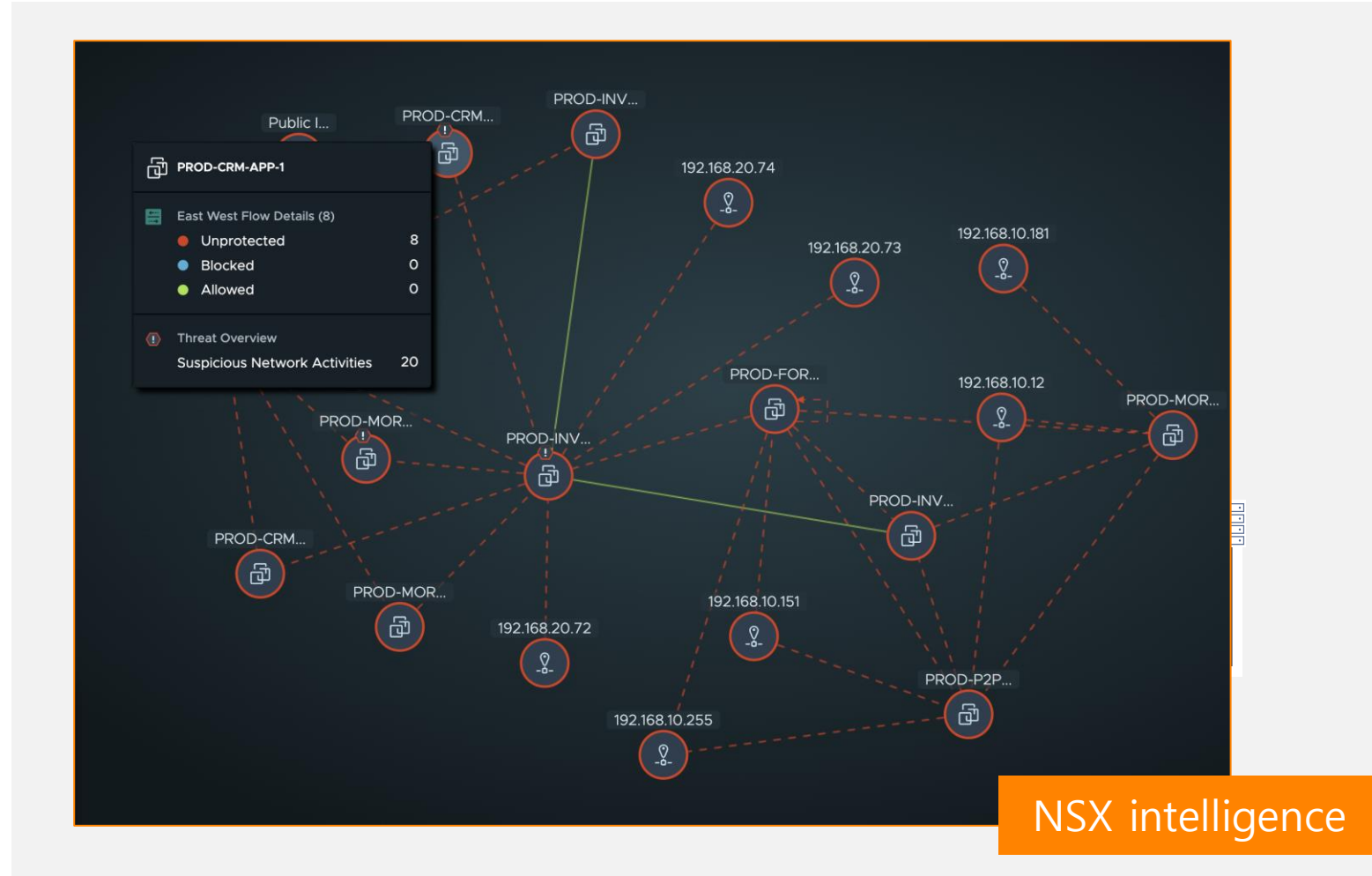
» 모든 흐름 수집/시각화, 기준 설정 및 세분화 정책 권장

분석에 대한 전통적인 접근 방식

대형 중앙집중식 어플라이언스
중복된 트래픽
네트워크 저하
운영 복잡성
제한된 컨텍스트 및 샘플링

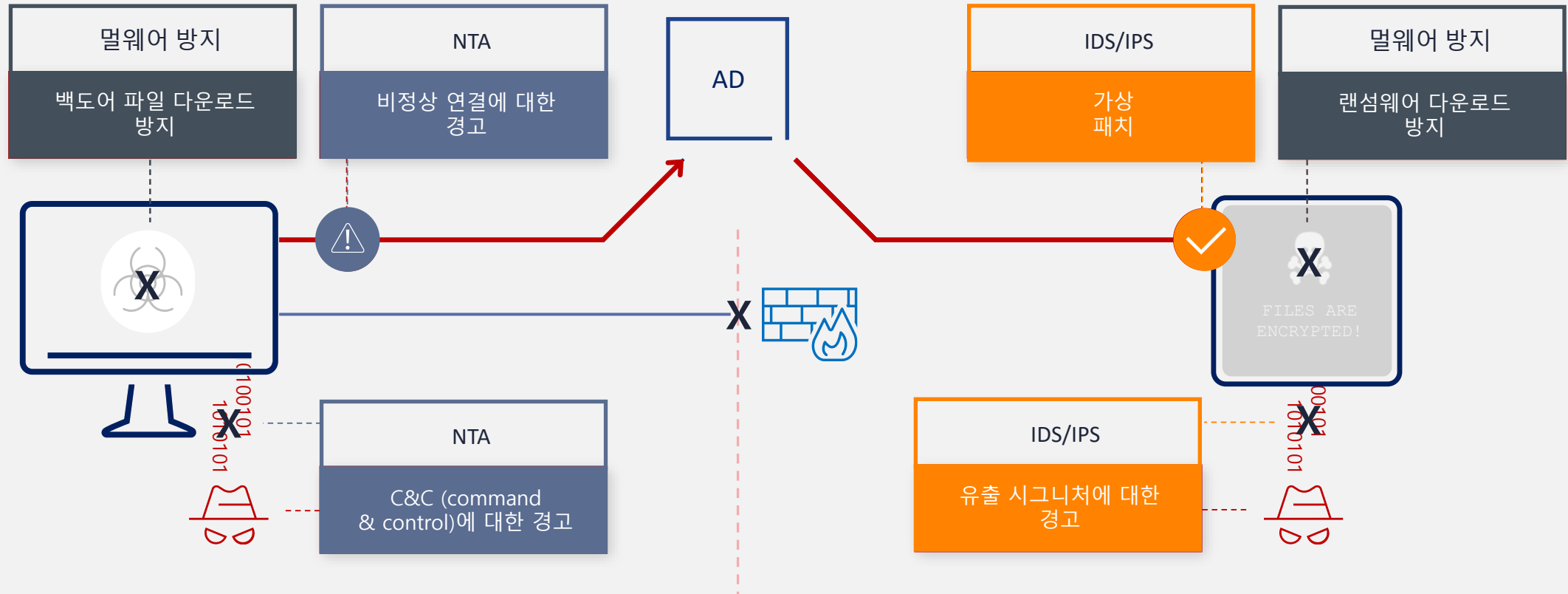
NSX 접근 방식

분산 처리 아키텍처
경량화된 중앙 어플라이언스
운영 모델 단순화
전체에 대한 커버리지



NSX Security – 보호/탐지 (Protect/Detect)

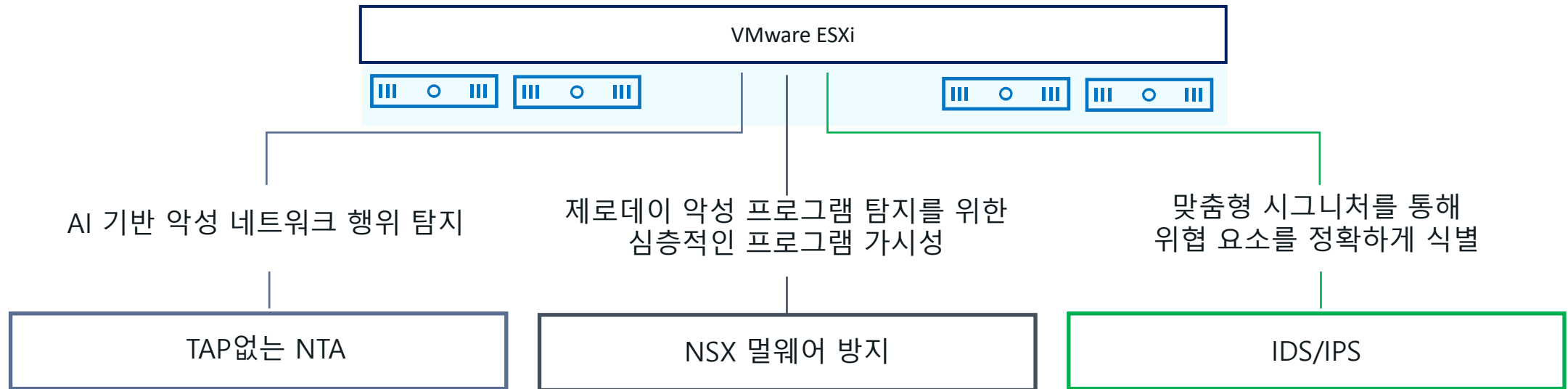
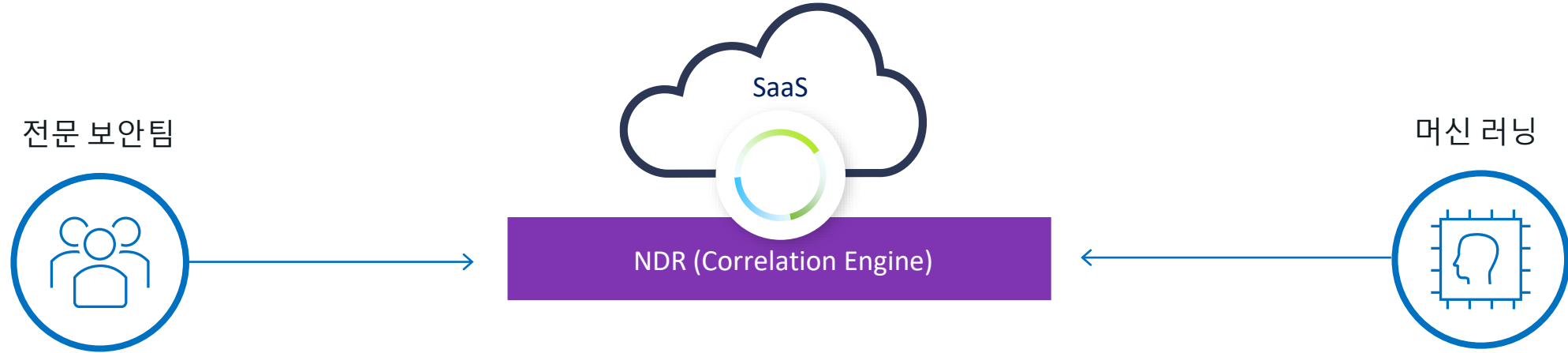
» 전체 공격 체인에 대한 가시성 및 적용



포괄적인 접근 제어 + 위협 탐지/예방

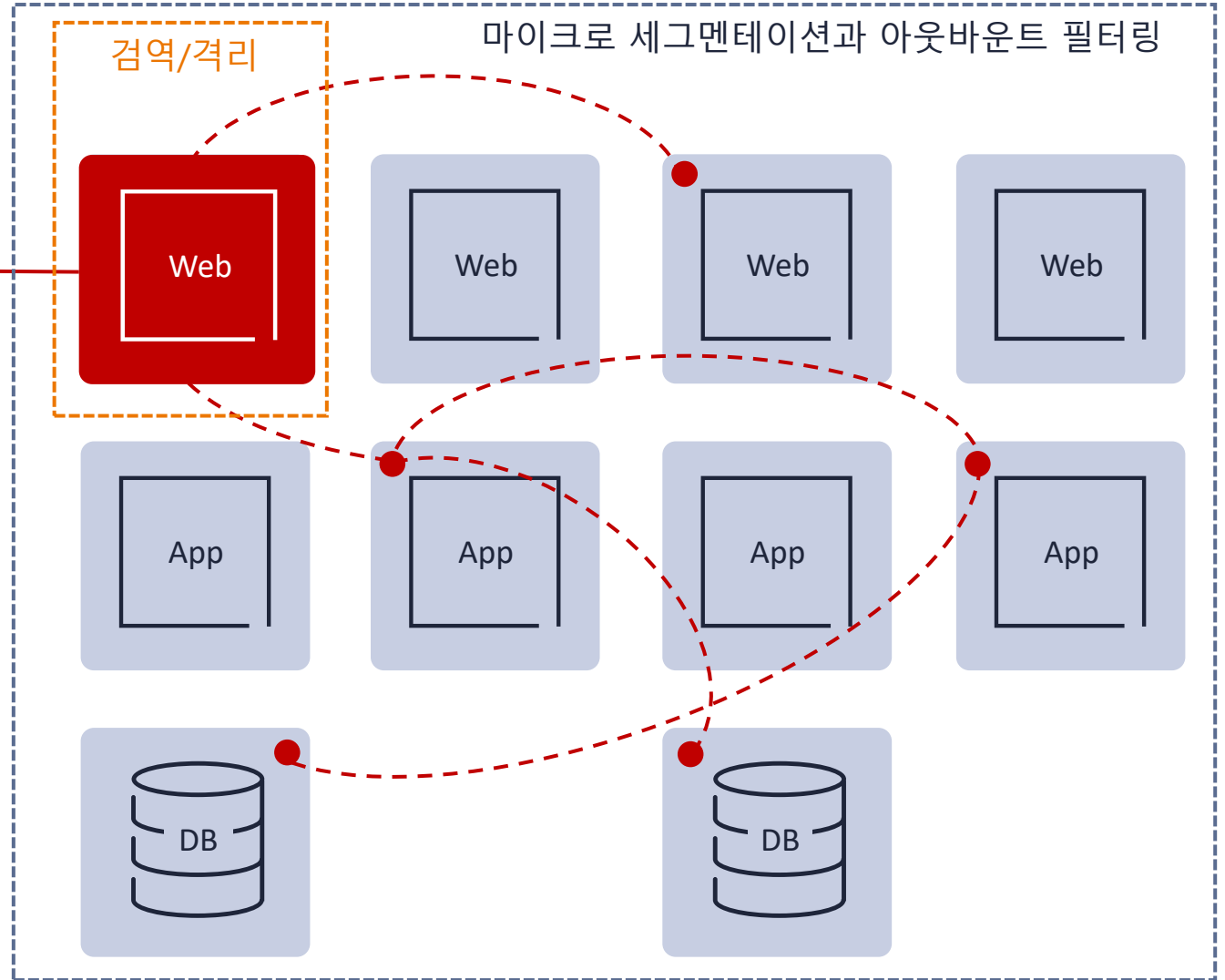
NSX Security – 보호/탐지 (Protect/Detect)

» NSX NDR (Network Detection and Response)을 통한 공격 체인 연결



NSX Security – 대응 (Respond)

» 네트워크 변경 없이 폭발 반경 (Blast Radius) 감소



즉각적인 네트워크 검역(격리)/세그멘테이션

NSX intelligence를 통해 가능한 폭발 반경 (Blast Radius) 식별

해당 blast radius를 줄이기 위한 마이크로 세그멘테이션과 아웃바운드 필터링

추가적인 C2 및 유출을 차단하는 FQDN 및 IP 평판 기반 필터링

태크 지정으로 감염된 워크로드 검역(격리)

NSX Security – 대응 : CB과의 연동

» CBC 'Apply NSX tag' 선택을 통해 NSX 내에서 적절한 규칙을 트리거하여 격리, 검역 또는 사용자 지정 방화벽 작업을 수행

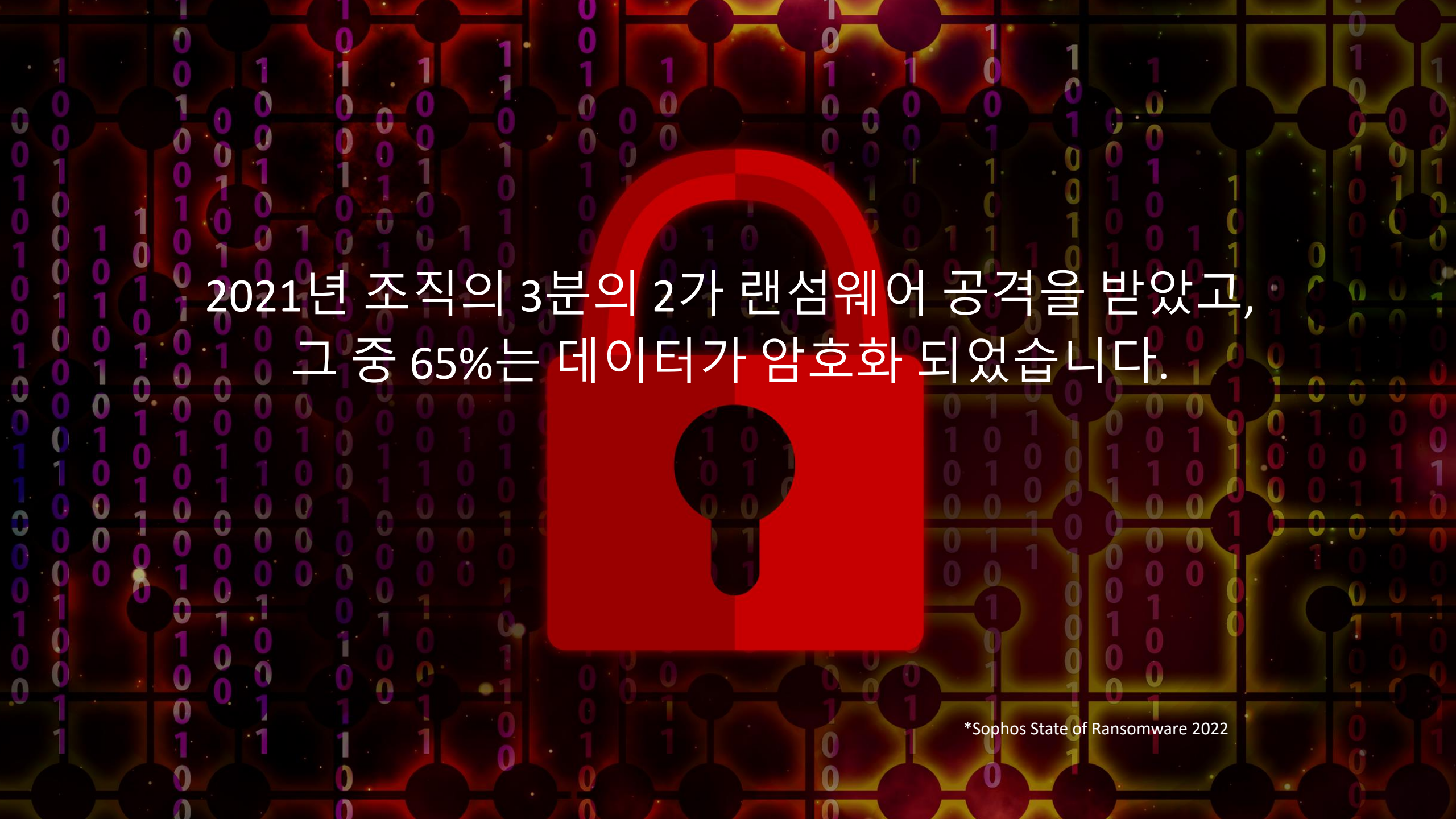
The screenshot displays the Carbon Black Cloud interface. On the left, a navigation sidebar includes sections like Dashboard, Alerts, Investigate, Live Query, Enforce, Harden, Inventory, Endpoints, USB Devices, VM Workloads, Sensor Groups, Kubernetes, and Settings. The main area is titled 'VM WORKLOADS' and shows a table of VMs. One VM, 'CLUS-Win10', is highlighted. An 'ALERTS' panel is open, showing 12 results. The selected alert is a 'Policy Applied' event with a severity of 3, triggered by a file named 'timesht.exe'. The 'REMEDIALTION' panel on the right offers several actions: 'Tune watchlist', 'Delete application', 'Quarantine asset', and 'Apply NSX tag'. The 'Apply NSX tag' option is highlighted with a green box, indicating the recommended response to restrict network access.

STATUS	FIRST SE...	REASON	5	DEVICE
<input type="checkbox"/>	Ran	11:22:03 am Nov 9, 2021	10	MCHOUSE\dmckay -admin MCHOUSE Windows10
<input type="checkbox"/>	Ran	8:48:25 pm Nov 8, 2021	4	MCHOUSE\dmckay -admin MCHOUSE McVault-12
<input type="checkbox"/>	Policy Applied	8:04:10 pm Nov 8, 2021	3	MCHOUSE\dmckay -admin MCHOUSE McVault-12
<input type="checkbox"/>	Policy Applied	4:29:00 pm Nov 8, 2021	3	MCHOUSE\dmckay -admin MCHOUSE McVault-12
<input type="checkbox"/>	Policy Applied	6:15:38 pm Nov 3, 2021	3	netgurus@outlook.com MCHOUSE\DE M-TS400

VMware가 제안하는 랜섬웨어 방어 및 복구 전략

With VMware Cloud DR

오익준 Cloud Solution Architect
July 2023



2021년 조직의 3분의 2가 랜섬웨어 공격을 받았고,
그 중 65%는 데이터가 암호화되었습니다.

랜섬웨어의 사회적 영향

사이버 공격이 전 세계 사람들에게 미치는 영향

The Washington Post

랜섬웨어 공격으로 학교가 문을 닫고
화학 요법이 지연되고 일상 생활이
지연되고 있습니다

After years of warnings, the impact of ransomware finally hits home for regular people

◎CBS NEWS

콜로니얼 파이프라인 랜섬웨어 공격
이후 연료 가격 급등으로 가스 부족
심화

BBC NEWS

해커의 사이버 공격이 부동산 구매
붕괴를 야기합니다

📺 NEWS

미국 병원에 대한 사이버 공격이 더
높은 사망률이 야기한다는 연구
결과가 나왔습니다

The study, conducted by the Ponemon Institute, a Washington, D.C., think tank, interviewed more than 600 information technology professionals across more than 100 health care facilities.

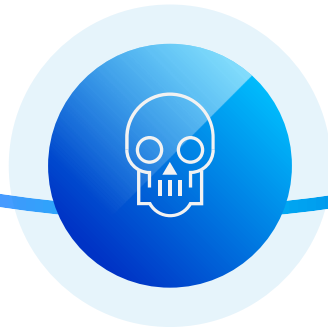
조직이 제로 트러스트 접근 방식을 채택하는 이유

클라우드 혼란 속에서 발생하는 사이버 보안 문제로 인해 랜섬웨어 방어가 필수적임



증가하는 공격 표면

Multiple data centers, public clouds, edge devices



공격의 정교성 향상

Ransomware is lucrative, fileless attacks more frequent



일관성 없는 운영 모델

Distributed, siloed infrastructure and disjointed operations

랜섬웨어의 진화

공격의 수익성이 높아짐에 따라 더욱 정교해짐

Until 2016

- File-based approach
- Examples:
 - TorrentLocker aka CryptoLocker
 - Cerber (Fast-changing files)
- Detected by signature match

Traditional-AV was usually sufficient

Post 2017

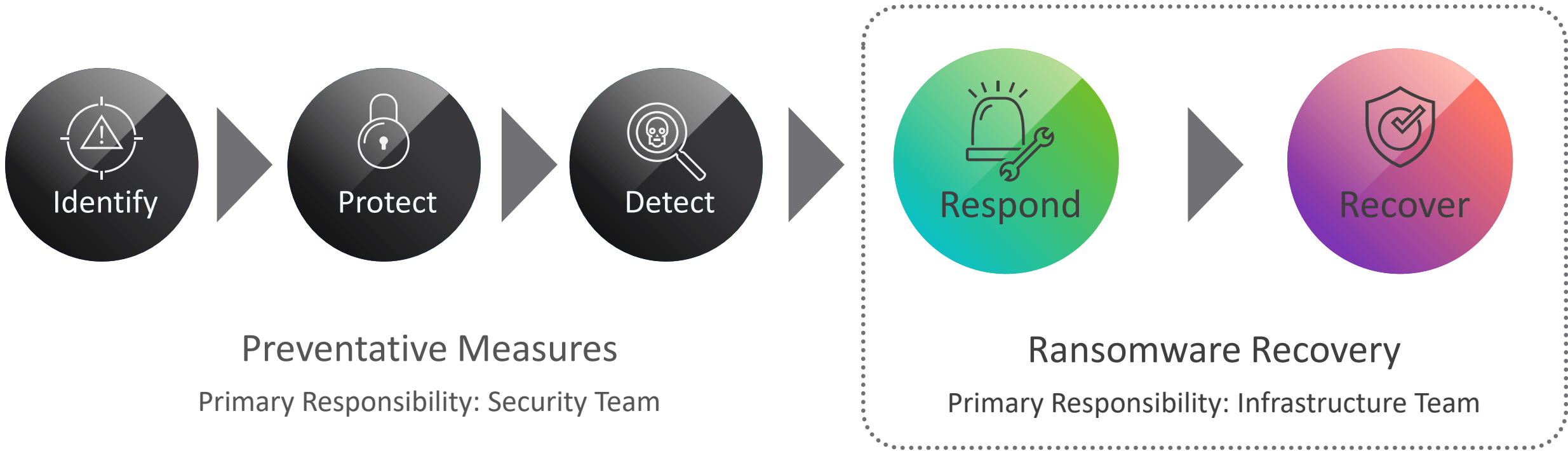
- Fileless, “Living off the Land”
 - Memory
 - Built-in OS programs
 - Stolen credentials (from black market)
- Disables security software¹

Traditional-AV **fails**; need EDR, NGAV, XDR

¹ Conti Ransomware had a playbook to disable all major security software

랜섬웨어 복구는 마지막 방어선입니다

NIST Framework



오늘날의 과제를 해결할 수 없는 과거의 복구 솔루션

1989

First ransomware attack discovered

2010

Birth of Bitcoin

2017

First ransomware fileless attack

2023

Ransomware costs organizations over \$4.5M/breach

Ransomware 1.0

Modern Ransomware

Snapshots

Backups

Offsite copies

Storage immutability

Air-gapping

Traditional file scanning

✔ Next-Gen Anti-Virus w/ Behavioral Analysis

✔ Secure Isolated Recovery Environment

✔ Prevent reinfection and lateral movement

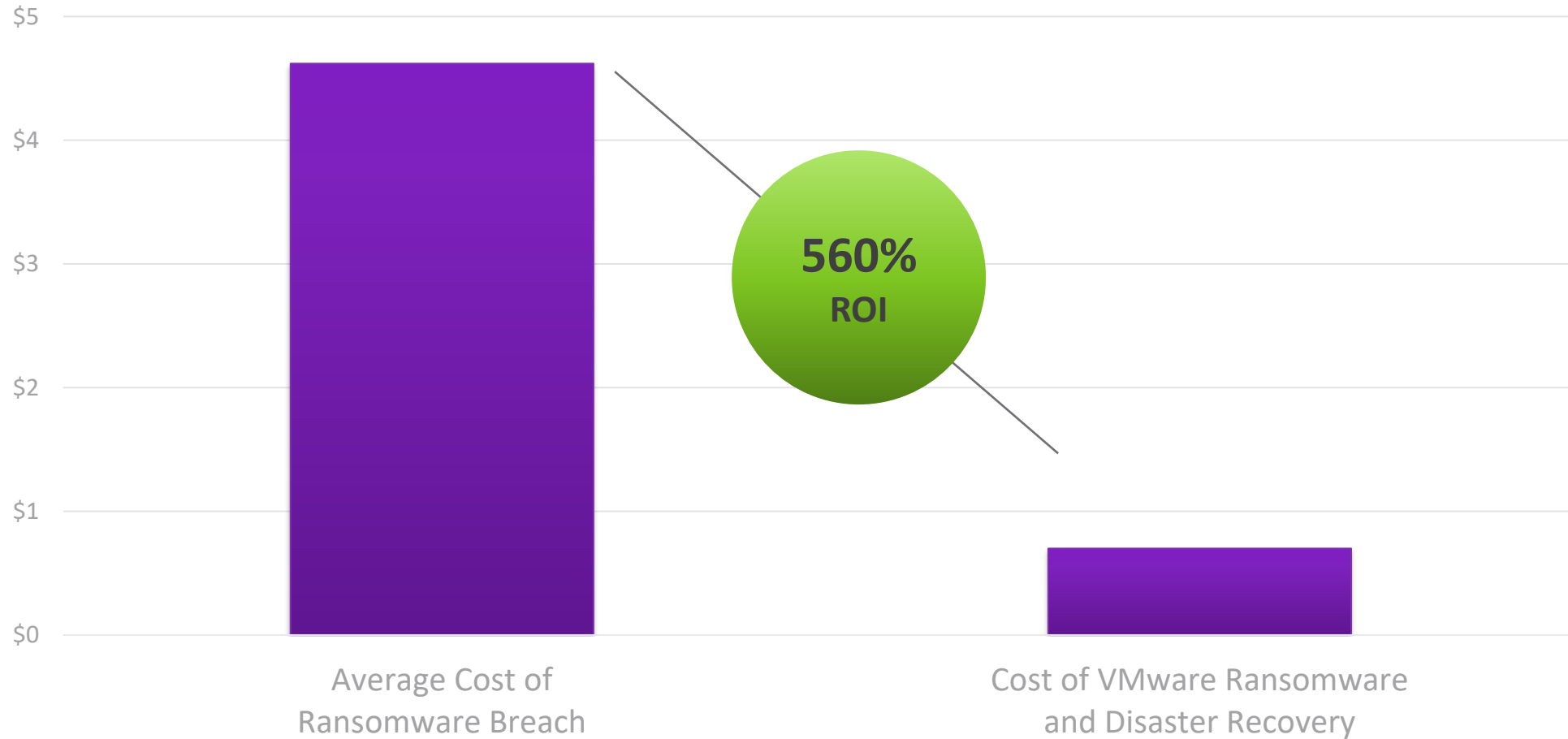
Not Enough

Required

VMware 랜섬웨어 복구를 통해 최대 560%의 ROI 달성

맞춤형 분석을 위해 VMware 클라우드 이코노미스트 팀과 협력

(\$ in millions)



VMware 랜섬웨어 복구의 차이점

Only possible because of VMware's IP across DR, cloud storage, security, networking, public cloud!

Traditional approach challenges



IRE*는 사용자에게 의해 구축, 보안 및 관리됩니다



오프라인 백업 검색, Fileless 공격에 효과적이지 않음



단절된 수동 환경, 다양한 툴 및 프로세스



다수의 스냅샷을 반복하고 평가하는 프로세스가 느림



완전히 관리되는 IRE*를 프로비저닝하여 재감염 방지



내장된 동작 분석을 통해 차세대 랜섬웨어 변종 식별

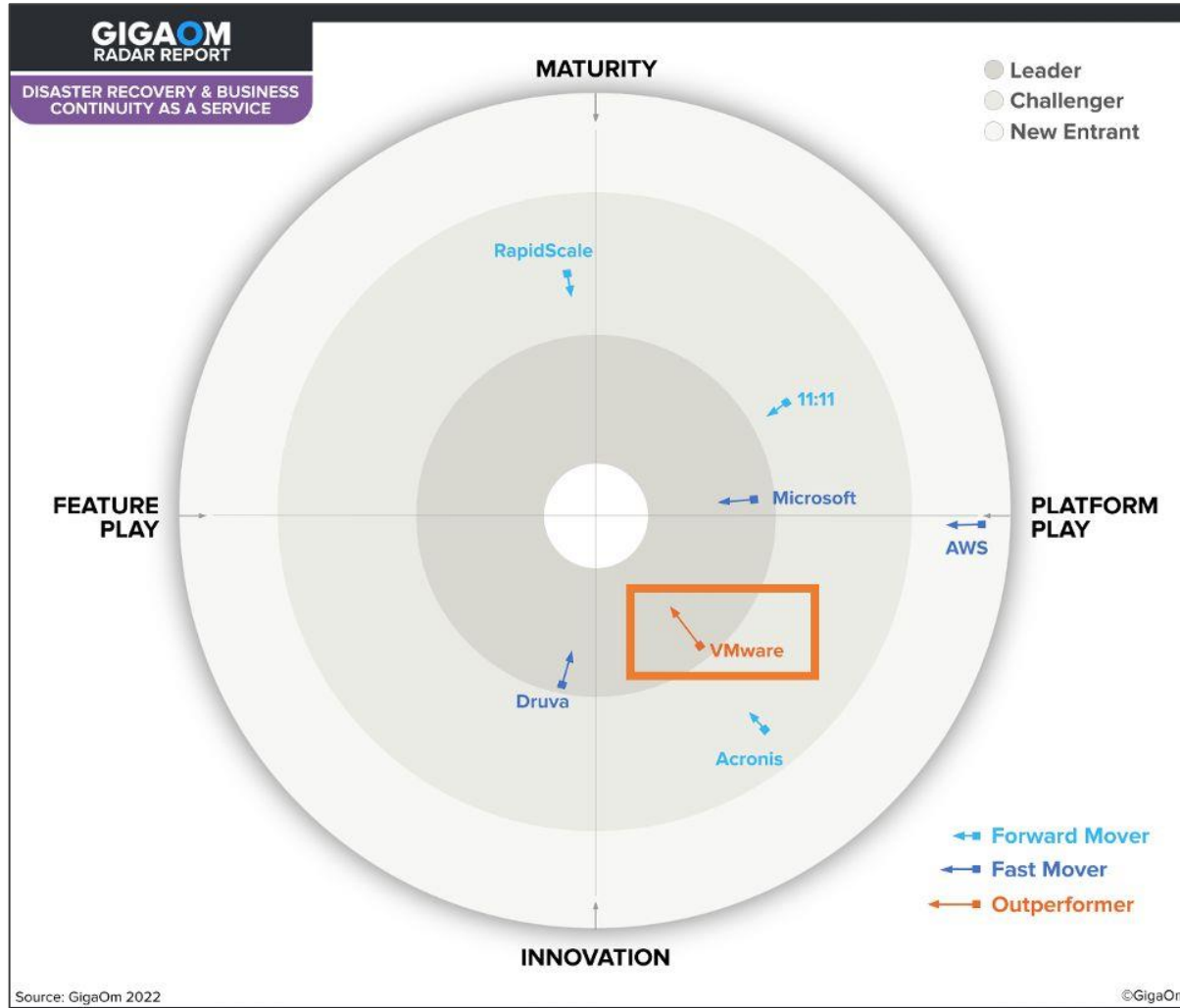


사전 정의된 랜섬웨어 복구 워크플로우를 통해 복구 간소화 및 자동화



복구 지점에 대한 신속하고 반복적인 평가를 통해 복구 가속화

“Stand-out” ransomware recovery & only “Outperformer” in DPaaS

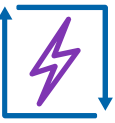


Analyst commentary:

"VMware는 매우 강력한 랜섬웨어 복구 기능을 통해 큰 발전을 이루었는데, 이는 올해 모든 공급업체중에서 두드러진 발전입니다."

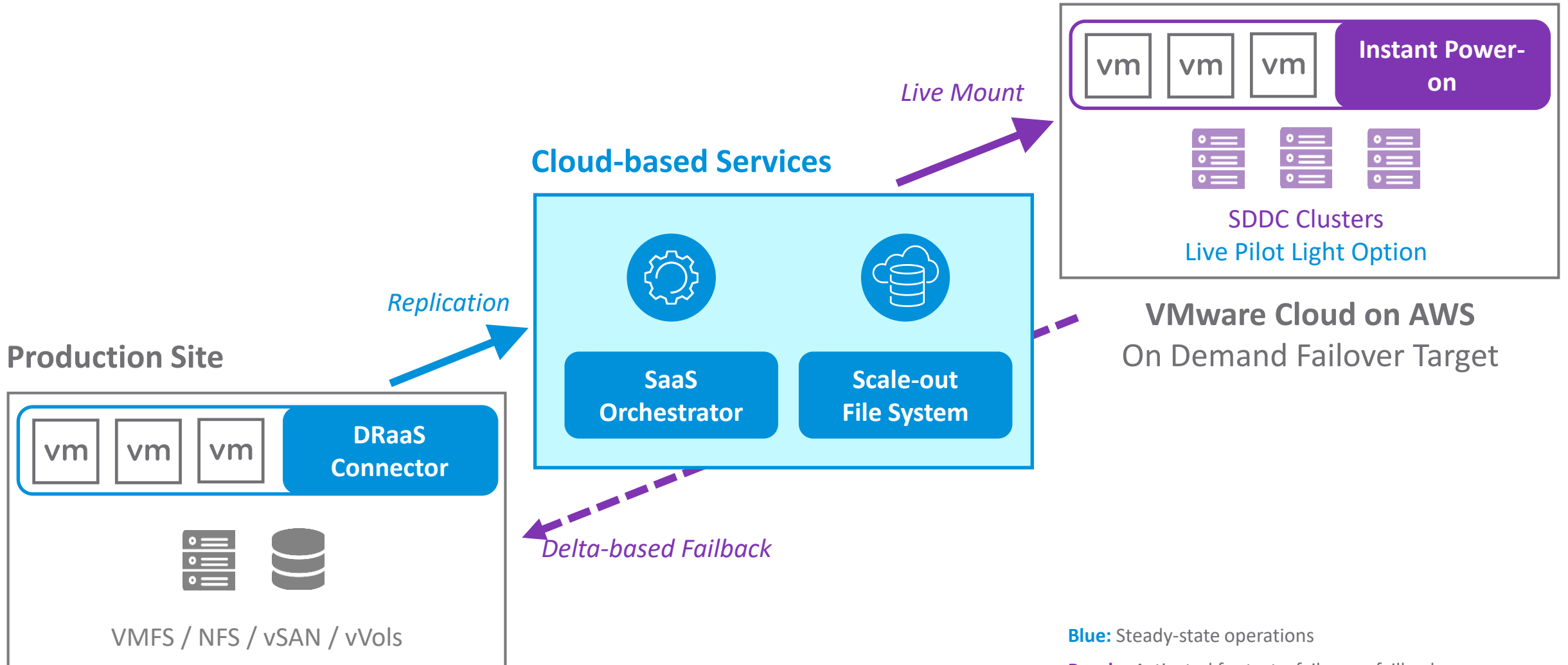
Product Summary

VMware Cloud Disaster Recovery at a glance



VMware Cloud Disaster Recovery: On-Demand DRaaS

On-demand disaster recovery, delivered as an easy-to-use SaaS solution, with cloud economics



Blue: Steady-state operations

Purple: Activated for tests, failovers, failbacks

VMware Cloud Disaster Recovery is available globally



Available Regions

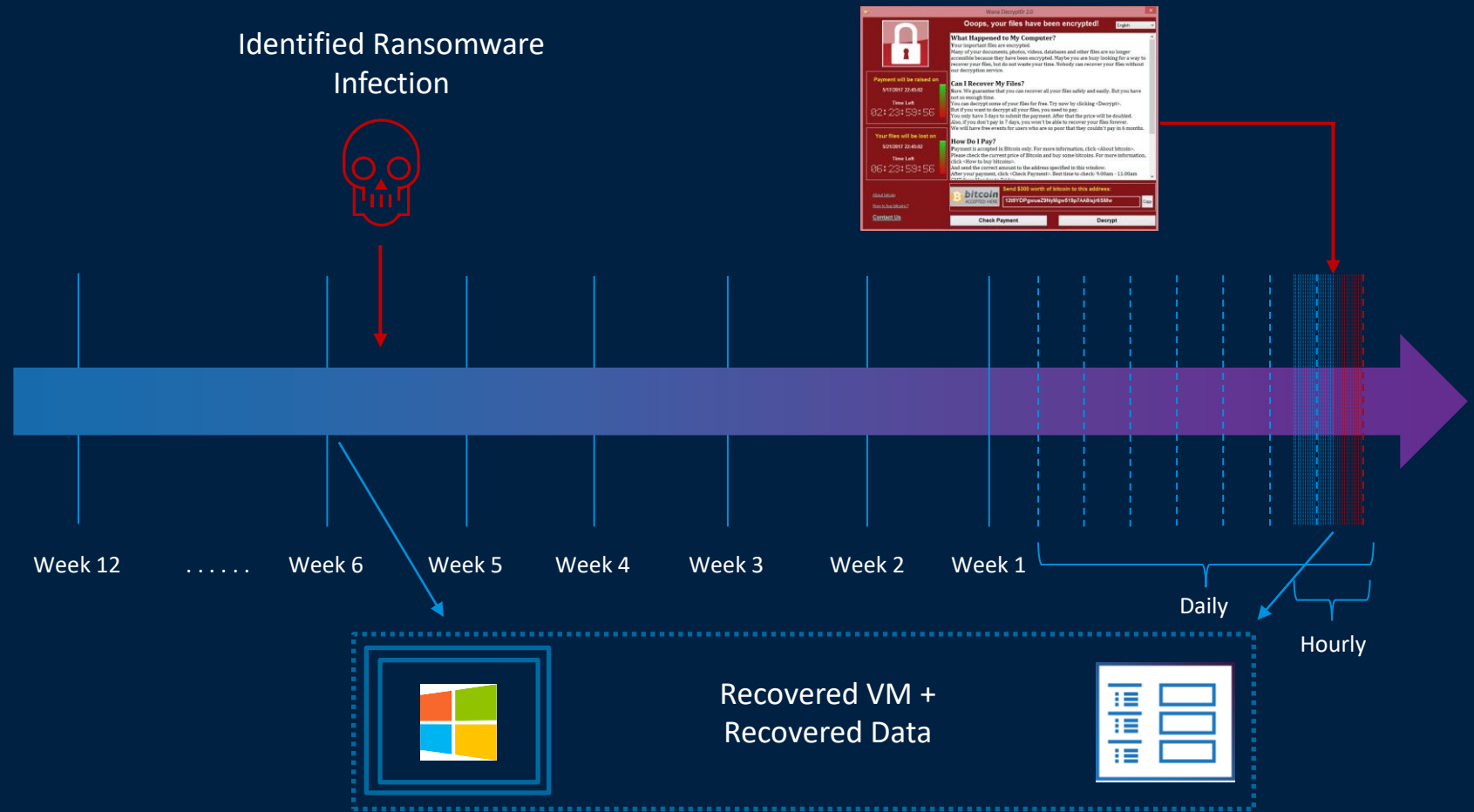
- US West (N. California)
- US West (Oregon)
- US East (Ohio)
- US East (N. Virginia)
- Canada (Central)
- South America (São Paulo)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Frankfurt)
- Europe (Milan)
- Europe (Stockholm)
- Asia Pacific (Mumbai)
- Asia Pacific (Singapore)
- Asia Pacific (Seoul)
- Asia Pacific (Osaka)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Hong Kong)
- Africa (Cape Town)



Ransomware Recovery

Recovery of VM + Recovery of Data = Clean VM with Recent Data

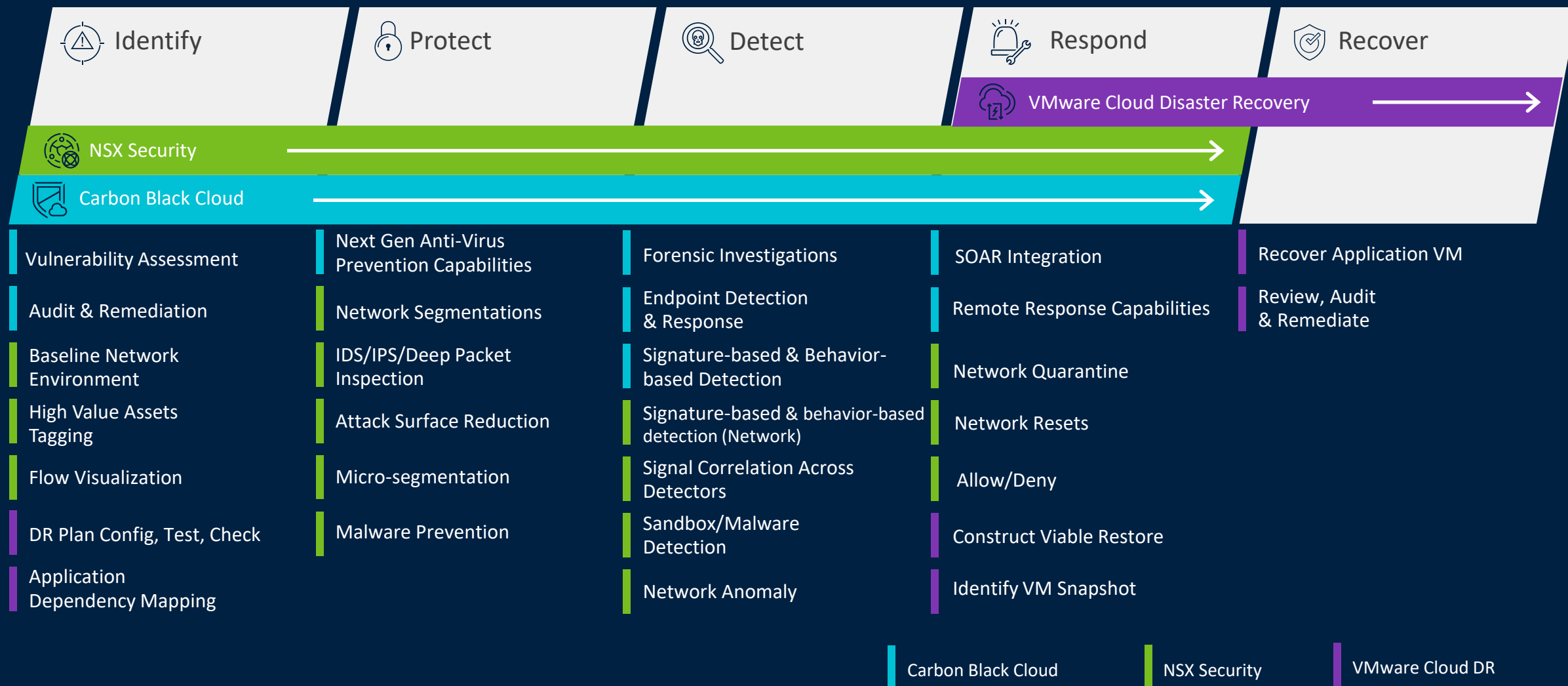
- 멀웨어 이전 OS/VM 복원
- 가장 최근의 데이터를 신속하게 복원
- 반복적으로 Clean 복구 지점 탐색



Coverage of the Ransomware Protection Cycle

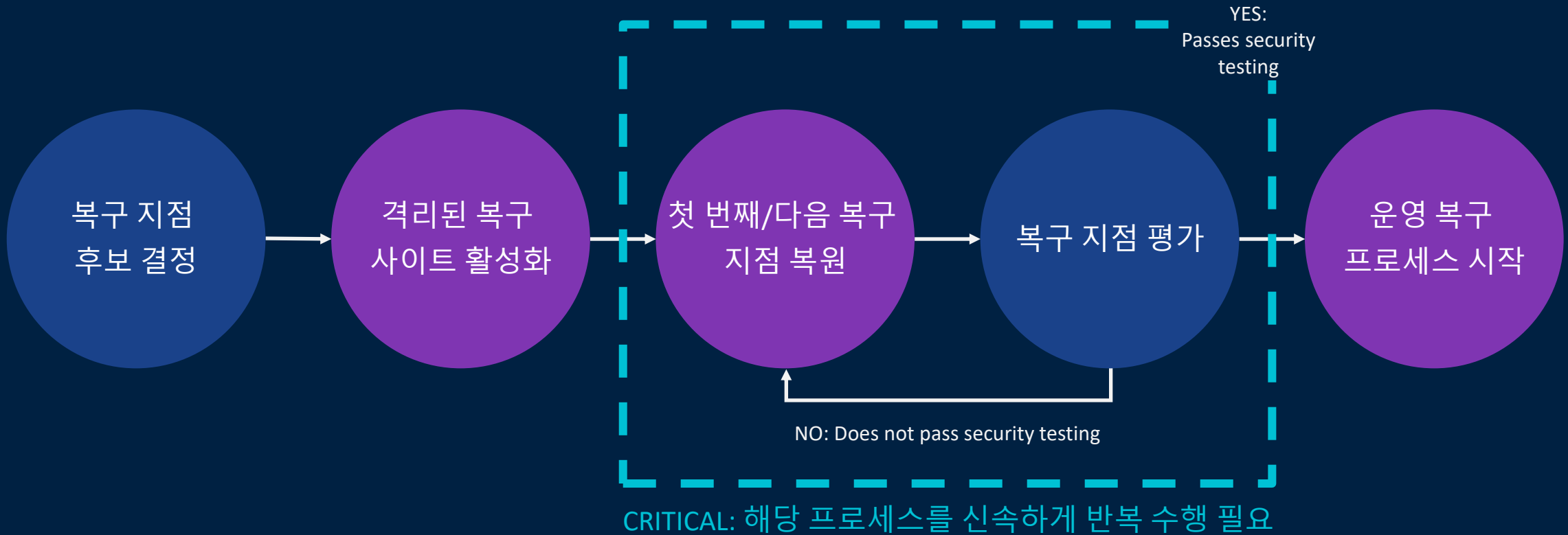
NIST – 5 Cybersecurity Framework Functions

<https://www.nist.gov/cyberframework>



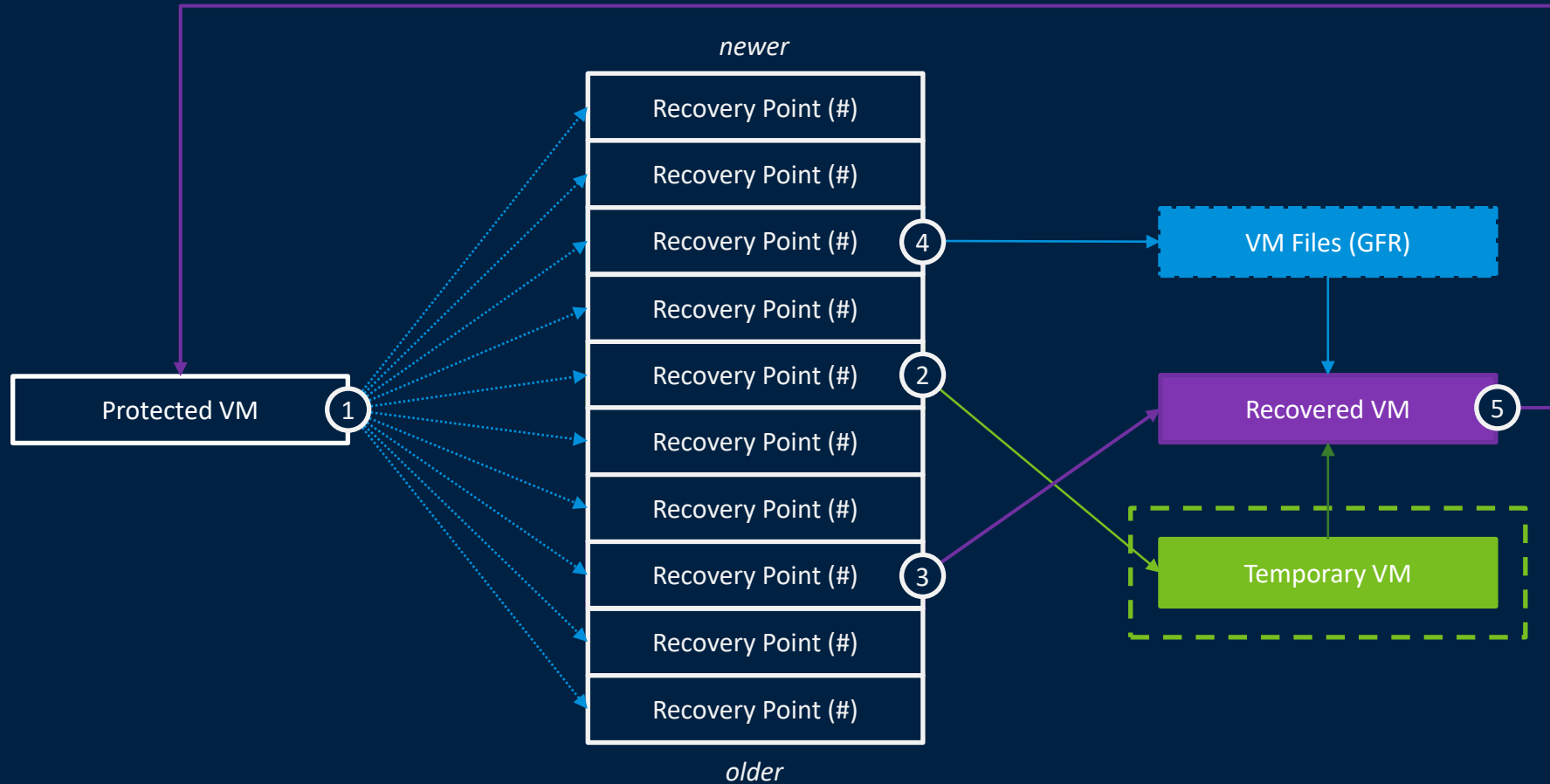
신속한 랜섬웨어 복구 평가 프로세스

가능한 한 신속히 수행되어야 하는 반복 프로세스



병합된 VM 복구 프로세스

복구된 VM에 둘 이상의 복구 지점 결합



Ransomware Recovery Platform Foundation

VMware Cloud DR에서 사용할 수 있는 기존 기능



- 심층 스냅샷 기록(시간, 일, 주, 월)
- RTO에 영향을 주지 않고 스냅샷에서 복구



- 변경되지 않는 스냅샷
- 작동 시 에어 갭
- 데이터 무결성 검사
- 역할 기반 액세스 제어 및 MFA



- 즉각적인 전원 켜기(zero copy, no rehydration)
- 복구 오케스트레이션
- 격리된 복구 환경(IRE)으로서의 VMware Cloud SDDC



- 파일/폴더 수준 복원
- 개별 VM 복원
- 다중 VM 오케스트레이션된 복구

VMware Ransomware Recovery for VMware Cloud DR

특별히 제작된 업계 최고의 랜섬웨어 서비스형 복구 솔루션



Ransomware recovery workflow

Streamline recovery with a step-by-step guide



Pre-configured VM network isolation

Prevent reinfection at recovery



Isolated Recovery Environment (IRE)

On-demand cloud economics



Air-gapped, immutable recovery points

Preserve data integrity of restore points



Next Gen AV + Behavioral Analysis

Embedded within a single UI

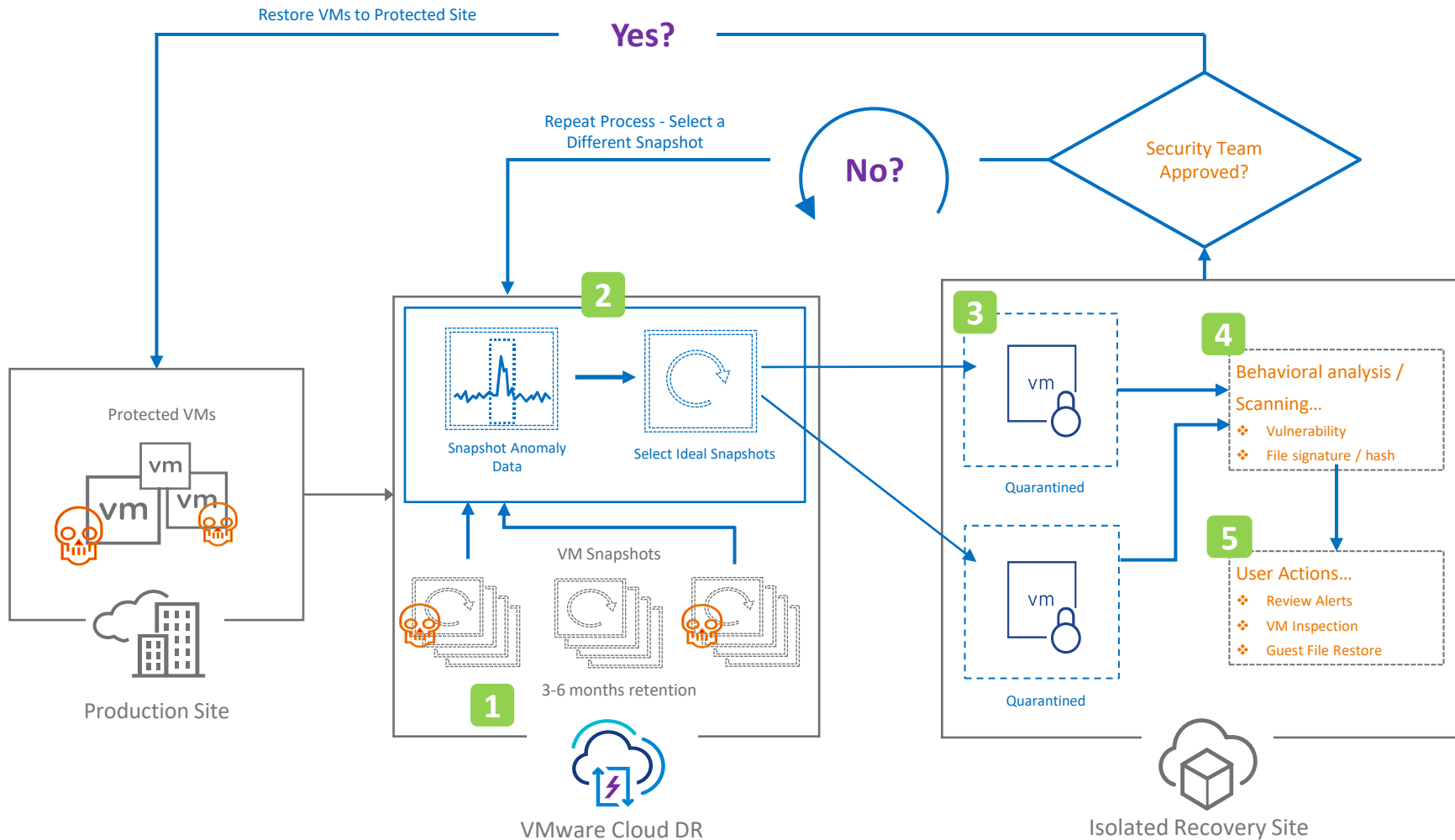


Instant VM power-on

Conduct rapid recovery point iterations

How It Works

VMware Ransomware Recovery



- 1 적절한 스냅샷 보존 구성
- 2 검증할 스냅샷 선택
- 3 IRE(격리된 복구 환경)에서 검증 시작
- 4 자동화된 위협 분석
- 5 최종 검사 또는 큐레이션된 이미지 빌드

사전 구성된 VM 격리 수준

Ensure controlled placement in IRE



Pre-configured VM Isolation Levels

<input type="radio"/>		Isolated	No network access.
<input checked="" type="radio"/>		Quarantined	Only access network and integrated security services.
<input type="radio"/>		External outbound	Allow outbound access to the internet. Use to expose ransomware behavior.
<input type="radio"/>		Internal inbound	Allow inbound access from internal network. No internet access.
<input type="radio"/>		Internal	Allow full access in the internal network. No internet access.
<input type="radio"/>		Open	Full internal and internet access.

DEMO

Ransomware and Disaster Recovery as-a-Service

VMware Cloud Disaster Recovery + VMware Ransomware Recovery

DR 운영을 위한 클라우드 채택

VMware 클라우드 콘솔과의 통합
세분화된 또는 규모에 맞는 복구
일관된 VMware 운영 환경

복원 지점의 무결성 유지

불변 VM 스냅샷
에어 갭 스케일 아웃 클라우드 파일 시스템
매일 데이터 무결성 검사

총 소유 비용 최적화

종량제 페일오버 용량 모델
델타 기반 파일백
보조 데이터 센터 필요 없음



복구 지점 후보 식별

안내식 랜섬웨어 복구 워크플로우
점 이상 징후 관찰 복원
스냅샷 복사본의 상세 내역

복구 지점 유효성 검사

임베디드 NGAV + 동작 분석
검증을 위한 전원이 켜진 워크로드
복구 지점의 신속한 실험

데이터 손실 최소화

높은 빈도의 스냅샷
파일 및 폴더 레벨 복구
사용자 지정 VM 네트워크 분리 수준

The background features a dark blue cityscape at night, with numerous skyscrapers and buildings illuminated. Overlaid on this are several vertical lines of binary code (0s and 1s) and various digital icons. The icons include a shopping cart, a lightbulb, a heart with a pulse line, a padlock, a Wi-Fi signal, a cloud, a house, a headset, a smartphone, a share symbol, and gears. Dotted lines with arrows connect these icons to the city buildings, suggesting a flow of data or information.

Thank you