변화하는 금융 보안 위협에 따른 대응 방안

인텔시큐리티 코리아 김수영 부장

Senior Sales Engineer / Darren.kim@intel.com

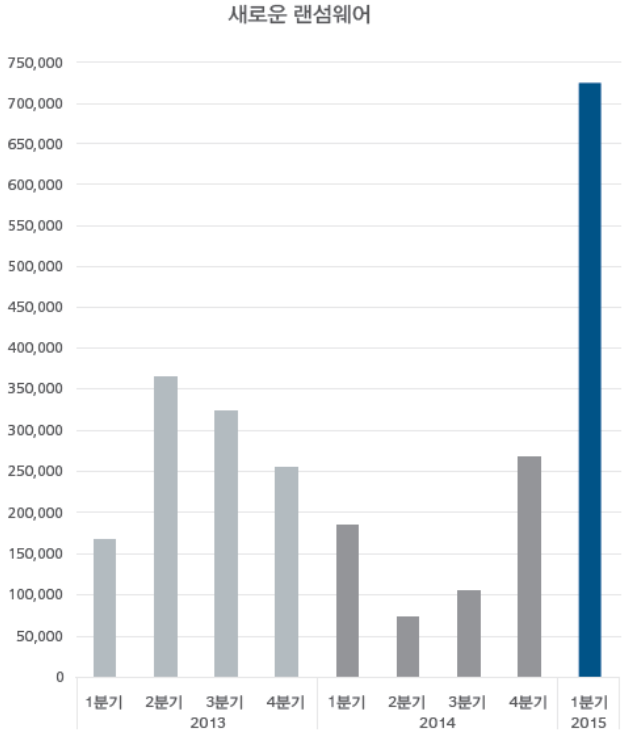
Threat Trends

Threat Landscape

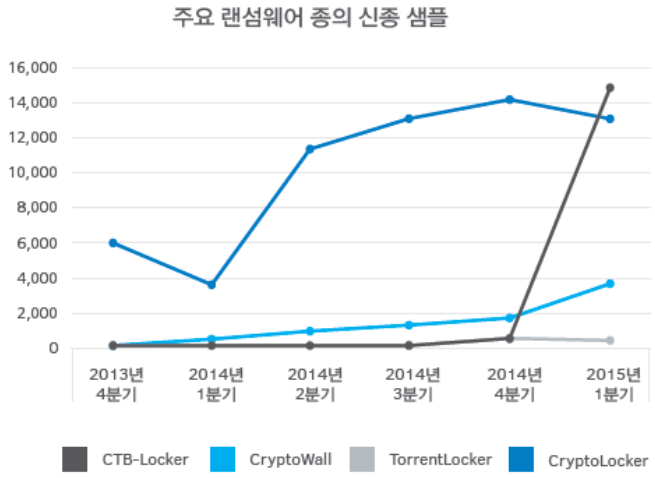
362	New threats every minute, or more than 6 every second
13%	Growth of the McAfee Labs malware zoo between Q4 2014 and Q1 2015
49%	Rise in mobile malware samples from Q4 2014 to Q1 2015
81%	Jump in new suspect URLs found in Q1 2015 compared to Q4 2014
165%	Increase in new ransomware in Q1 2015
317%	Growth in Adobe Flash exploits in Q1 2015
400,000,000+	Unique malware samples in the McAfee Labs Zoo as of Q1 2015

Source: McAfee Labs Threats Report: 1st Quarter 2015

Ransomware trend



출처: 맥아피 연구소, 2015.



출처: 맥아피 연구소, 2015

Ransomware trend

Ptt posta hizmetleri

EA273182901BE takip numaralı kargonuz **09 Mart 2015** adresinize teslim edilememiştir. Lütfen adres bilgilerinizi güncelleyerek kargonuzu teslim alınız.

Teslimat adresi değiştirmek için PTT Adres Değişikliği Formu indirip dikkatlice ve eksiksiz olarak doldurmanız gerekmektedir.

Adres Değişikliği Formu İndir

Dikkat

Kargonuz 15 iş günü içinde almanız gerekmektedır. Fazladan her gün için PTT sizden 25TL/günlük tazminat talep etme hakkına sahip olacaktır.

Gizlilik Politikası

PTT olarak ilgili kuralların tarafımızca tümü ile eksiksiz bir şekilde yerine getirileceğini teyit etmekteyiz. Böylelikle, aşağıda belirtilen kişisel bilgi toplama ilkelerine bağlı olarak, tüm gayretimizi tarafımızca toplanmış olan her türlü bilgiyi ekibimizce alınan sıkı güvenlik ve gizlilik önlemleri ile saklama hususunda özen göstermekteyiz. Kişisel bilgi toplama ve kullanımını en aza indirgeyerek, toplanan kişisel bilgileri sadece işlemlerin gerçekleşebilmesi için gerekli olan süre kadar tutmakta, öte yandan size en kaliteli hizmeti ve birbirinden güzel fırsatları sunmaktayız. Web sitemiz, gizlilik konusunda yeterince duyarlı olduğunu gösterebilen ve standartlarımıza uygun olan sitelere bağlantılar içermektedir. Ancak ilgili sitelerin içeriği ya da gizlilik uygulamalarından PTT sorumlu tutulamaz.

Bu e-posta baha_guler@mcafee.com için gönderilmistir. Eğer artık ilgilenmiyorsanız haber grubu üyeliğinizi iptal edebilirsiniz

PTT Posta Hizmetleri
Posta ve Telgraf Teşilatı A.Ş. 2015

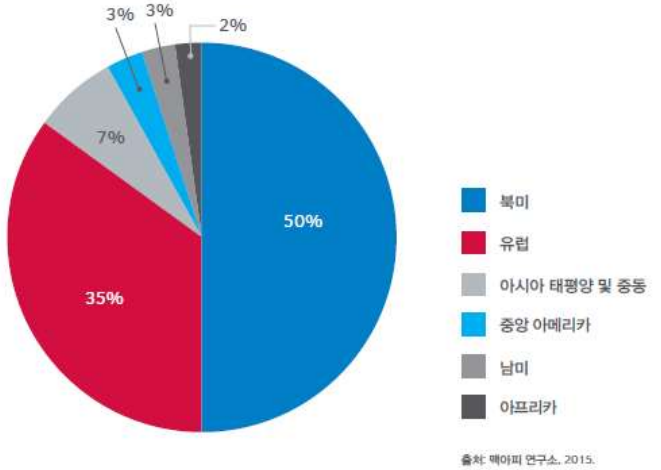
Ransomware trend

Dyre 네트워크 공격 단계

Dyre 네트워크는 다음 단계를 따라 시스템을 감염시킵니다.

- a_la_clinique_vtrinaire_lavalle.scr
- aliments_universelles_lolivier.scr
- alte_poststr_25_72250_freudenstadt.scr
- an_der_wassermhle_3_28816_stuhr.scr
- andros_consultants_limited.scr
- b_n_r_roofing_2000_ltd.scr
- b_van_brouwershaven_and_zn_bv.scr
- bill39C6113.scr
- fairview_rehab_and_sports_injury_clinic.scr
- fashioncrest_ltd.scr
- feedback_instruments_ltd914.scr

CTB-Locker 희생자 위치 분포



출처: 맥아피 연구소, 2015.

Ransomware is strong than……Before

Bit Coin

Tor Network

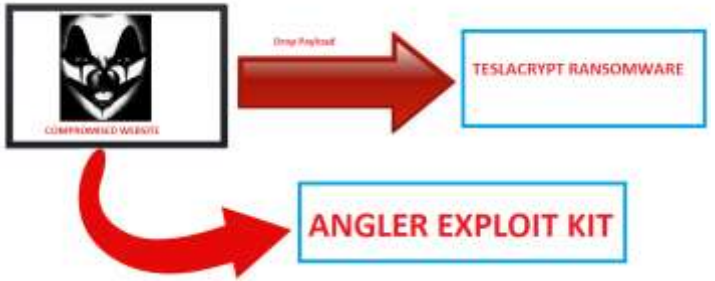
Go to the mobile

NAS storage

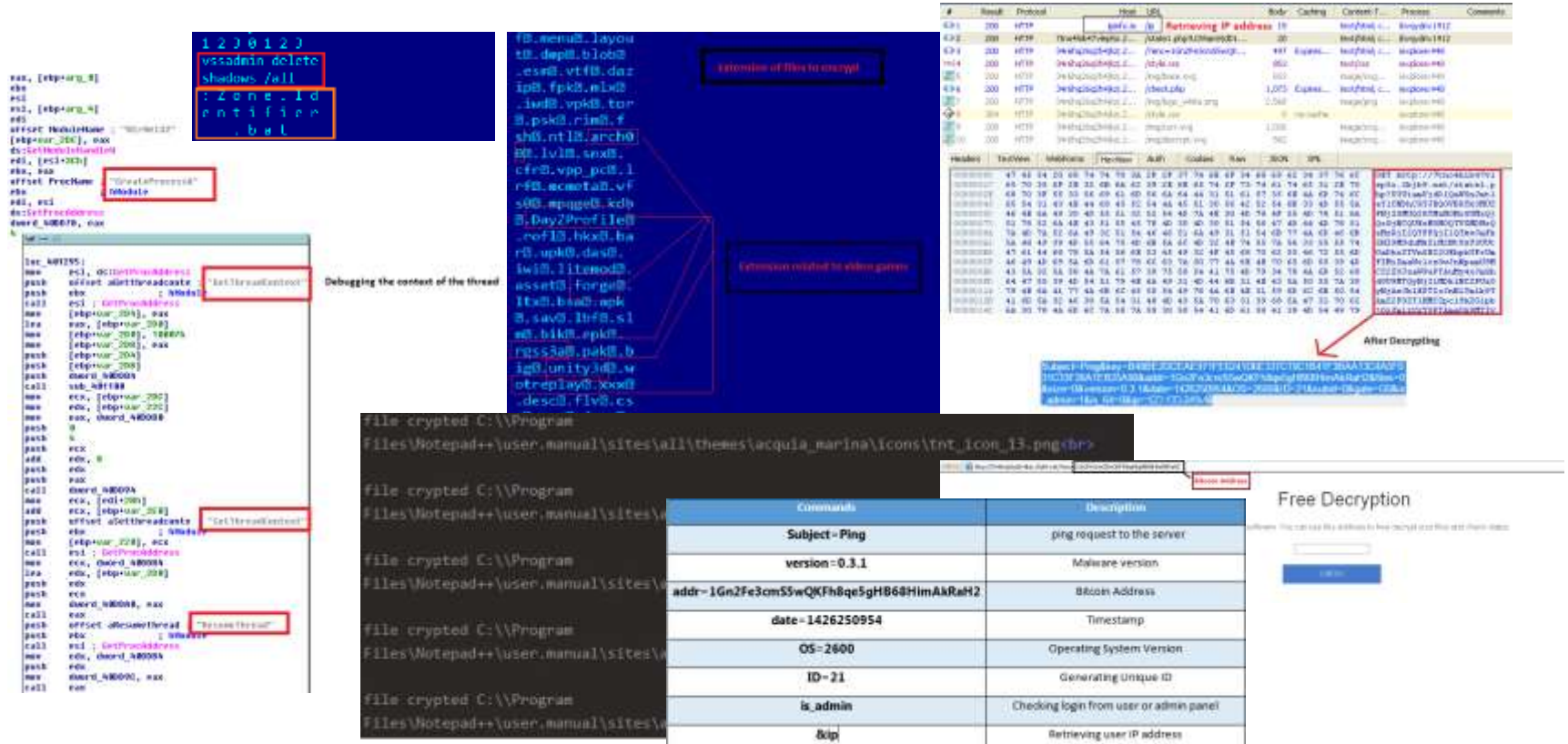
How to prevent Ransomware

New Ransomware

New type of Ransomware : Teslacrypt



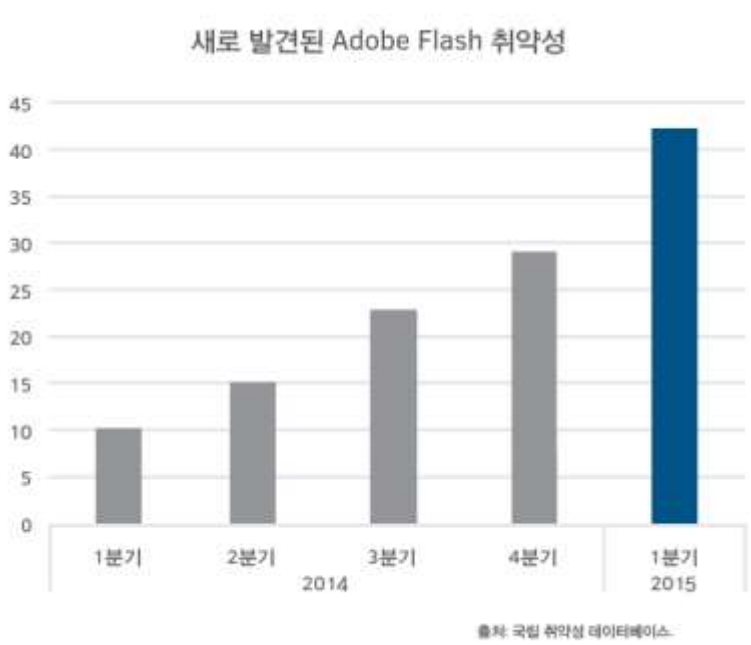
Analysis report

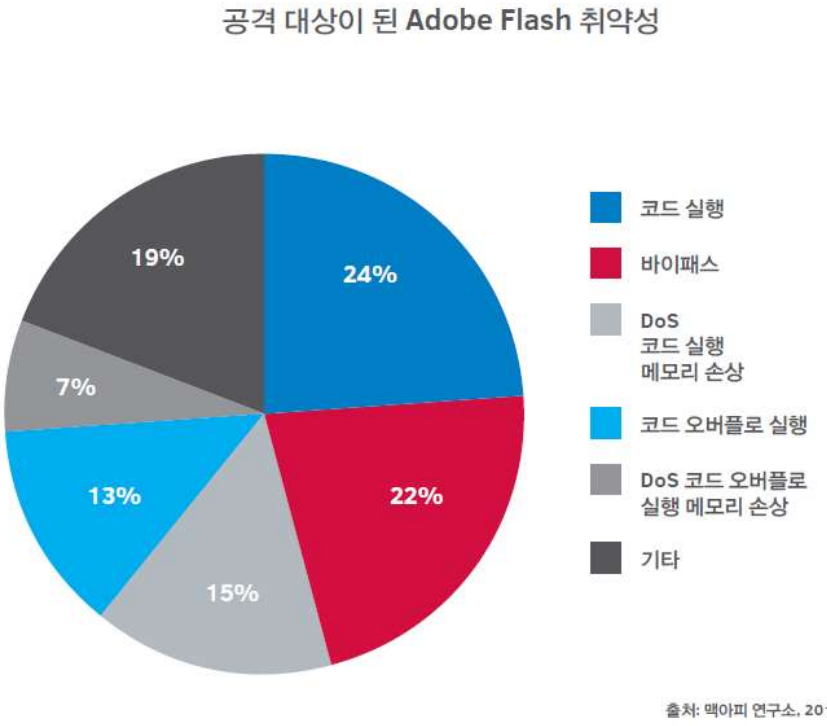


Commands	Description
Subject=Ping	ping request to the server
version=0.3.1	Malware version
addr=1Gn2Fe3cmS5wQKFh8qe5gH868HimAkRaH2	Bitcoin Address
date=1426250954	Timestamp
OS=2600	Operating System Version
ID=21	Generating Unique ID
is_admin	Checking login from user or admin panel
&ip	Retrieving user IP address

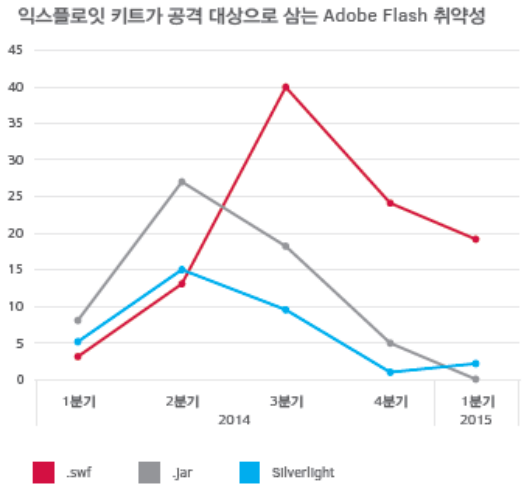
Adobe Flash: the new target

Adobe Flash: the new target

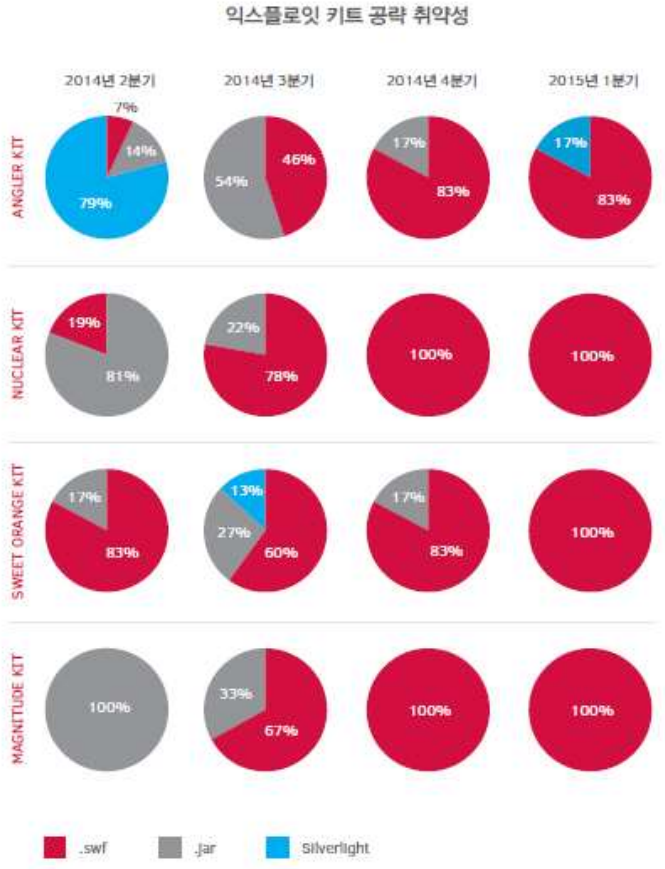




Adobe Flash: the new target



출처: 맥아피 연구소, 2015.



4개의 주요 익스플로잇 키트는 Flash 취약성만을 이용할 정도로 초점을 옮겼습니다.

Why Flash?

```
public function sadad(param1:int) : *
{
   if(param1 == 1)
   {
      return "A501-0-000-00A-4-0B-003-17279-7-37-4616C6C6-9-7-A32A0-0-C6-E-6-16D-657-3706163-68-0-0317-2797374-6-16-C6C697A-3-22-0627-9-205065-747-2
   }
   if(param1 == 2)
   {
      return "EB4-89-090-9-09090-90-9-090909-090-90-90-90-9090-909-0-9-0909090-9-09-09090-90-909090-90909090-909-090-90909-0-9-09090909-0-909090-90-9
   }
}

function read_memory(param1:Vector.<int>, param2:uint, param3:uint) : uint
{
   if(param3 >= param2)
   {
      return param1[(param3 - param2) / 4];
   }
   return param1[1073741824 - (param2 - param3) / 4];
}

private function InitEx() : void
{
   ggew = jtyk.xxfrh();
   var _loc1_:* = kryuje.wecy();
   var _loc2_:* = new RegExp("[3892754016]+","g");
   var _loc3_:* = "1581467g595a839d024B304y549c110e672a730".replace
   _loc1_[_loc3_](ggew);
   stage.addChild(_loc1_);
}
```

```
public function kryuje()
{
   super();
}

public static function wecy() : Loader
{
   var _loc1_:* = new Loader();
   return _loc1_;
}
```

```
if("win 11,7,700,202" !== _loc7_)
{
   if("win 11,7,700,224" !== _loc7_)
   {
      return null;
   }
   _loc5_ = _loc5_ - 10450228;
   _loc6_ = _loc5_ + 13082624;
   _loc4_.writeUnsignedInt(_loc5_ + 4646881);
   _loc4_.position = 64;
   _loc4_.writeUnsignedInt(_loc5_ + 52090);
   _loc4_.position = 76;
   _loc4_.writeUnsignedInt(_loc5_ + 4293);
   _loc4_.writeUnsignedInt(_loc5_ + 9376924);
   _loc4_.writeUnsignedInt(_loc5_ + 93510);
   _loc4_.writeUnsignedInt(_loc5_ + 1145378);
   _loc4_.writeUnsignedInt(_loc5_ + 1909483);
   _loc4_.writeUnsignedInt(param2);
   _loc4_.writeUnsignedInt(4096);
   _loc4_.writeUnsignedInt(64);
   _loc4_.writeUnsignedInt(param2 - 4);
```

"Loader.LoadBytes(RC4_decode(RC4_encrypted_data))"

How to prevent Flash Vulnerability?

Flash 취약성 익스플로잇 차단

맥아피 연구소는 Flash 기반 공격으로부터 시스템을 차단하기 위한 몇 가지 방법을 권장합니다.

- Flash 패치가 배포되는 즉시 이를 설치합니다. 패치는 일반적으로 Flash CVE가 제출된 당일에 제공됩니다. Flash의 최신 업데이트 정보는 여기서 확인할 수 있습니다. 패치를 완벽하게 적용하고 방화벽을 등에 업은 컴퓨터는 사이버 공격에 맞서는 난공불락의 성과 같습니다.
- 자동 운영 체제 업데이트를 활성화하거나 운영 체제 업데이트를 주기적으로 다운로드하여 운영 체제를 알려진 취약성에 대해 패치 적용된 상태로 유지하십시오.
- 모든 이메일과 인스턴트 메시지 첨부파일을 자동으로 검색하도록 바이러스 백신 소프트웨어를 구성하십시오. 이메일 프로그램이 첨부 파일을 자동으로 열거나 그래픽을 자동으로 렌더링하지 않도록 하고 미리보기 창을 해제시키십시오.
- .swf 확장자를 포함한 첨부 파일을 차단하도록 바이러스 백신 소프트웨어를 구성하십시오.
- 브라우저의 보안 설정을 중간 이상으로 지정하십시오.
- 브라우저 플러그인을 사용하여 스크립트와 iFrame의 실행을 차단하십시오.
- 신뢰할 수 없는 브라우저 플러그인은 설치하지 마십시오.
- 특히 확장자가 .swf인 첨부 파일을 열 때는 각별히 주의하십시오.
- 요청하지 않은 이메일 또는 예상하고 있지 않던 첨부 파일은 절대 열지 마십시오. 알고 있는 사람의 이메일일 때도 마찬가지입니다.
- 스팸을 이용한 피싱 시도에 주의하십시오. 이메일이나 인스턴트 메시지의 링크를 클릭하지 마십시오.
- 브라우저의 주소 표시줄에 URL을 입력하거나 복사하고 웹 광고를 클릭하는 대신 주소를 확인하십시오.
- 신뢰할 수 없는 웹 사이트에서 Flash 동영상을 클릭하지 마십시오.

What Is Advanced Malware?

Gartner

Key Challenges

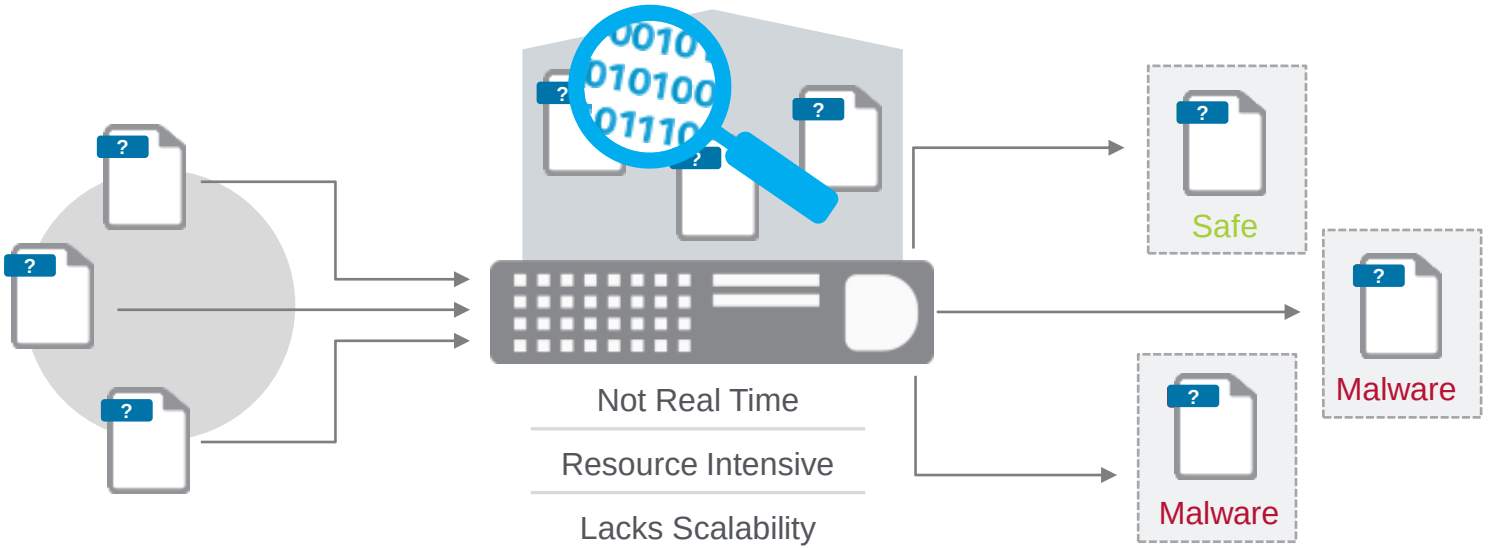
- Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers.
- Many of these attacks are not advanced in techniques; they are simply designed to bypass traditional signature-based mechanisms.

Source: Designing an Adaptive Security Architecture for Protection From Advanced Attacks (Published 12 February 2014)

Advanced Malware

Market wisdom

However, Sandboxing by Itself Should Not be Your Only Defense



Not Real Time

Resource Intensive

Lacks Scalability

Alert vs Actions

Not effective against all malware

Unknown

Because No Signature Match

Identified

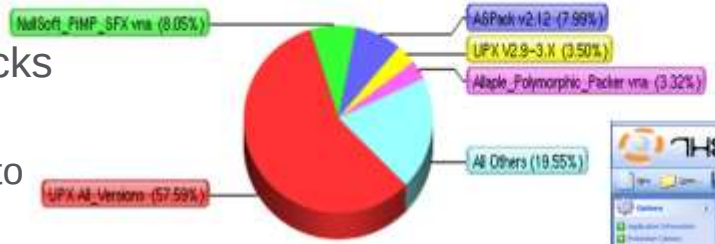
Because of Behavior Analysis

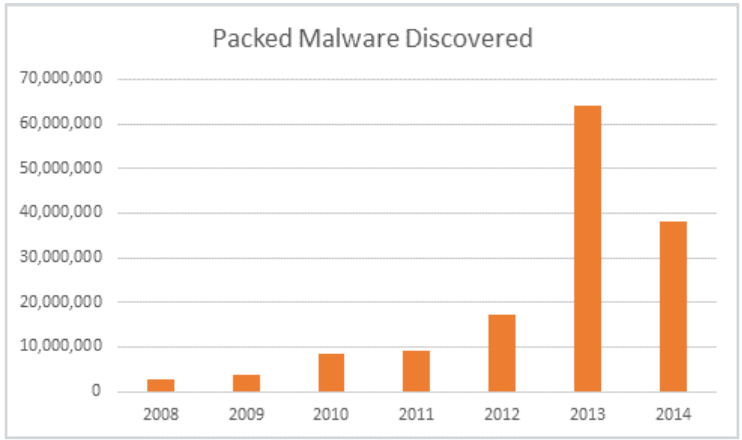
Broadest OS Support

- Target-specific analysis: Analyze threats under the exact conditions of the actual host profile within the organization
  - Reducing the chances of missed malware or false positives
  - Faster results: Scales sandboxing capacity
- Customizable sandbox images
- Broad support covers corporate environments, including server and mobile traffic

The Packing Challenge

- Custom packers used in targeted attacks
  - Packing or protecting changes the composition of the code or obfuscates it to evade detection and reverse engineering
- Need to unpack to get to original executable code for analysis
- Packed malware can hide
  - Delayed execution
  - Alternative execution paths





Source: McAfee Labs Q2 2014

Understand Your Adversary

- Advanced Threat Defense immediately identifies the file as malicious with 14 specific classifications
- Note, that static code analysis also shows the 43% of the code did not execute in the sandbox
- So what else is missed if only dynamic analysis is used?

Behavior Summary (57 percent code coverage):

Hides file by changing its attributes	Manipulated with active content in the admin temporary directory
Detected executable content dropped by the sample	Obtained and used icon of legit system application
Created executable content under Administrator temporary directory	Created executable content under Windows directory
From Microsoft: CreateURLMoniker can produce results that are not equivalent to the input, its use can result in security problems	Executed active content from Windows system folder
Committed a region of memory within the virtual address space of a foreign process	Set callback function to control system and computer's hardware events
Tried to connect to a specific service provider	Downloaded data from a webserver
Created content under Windows System directory	Registered (unregistered) the service name in a Dynamic Data Exchange (DDE) server supports

Static Code Analysis

- Advanced Threat Defense unpacks and reverse engineers the file to expose the actual code for analysis
- Compares code to known malicious code, identifying this relatively unknown file as part of the Trojan.Win32.simda malware family
- Static code analysis finds 96% similarity to known malware family

Down Selector's Analysis:

Engine	GTI File Reputation	Gateway Anti-Malware	Anti-Malware	Custom Yara	Sandbox	Final
Threat Name	---	---	---	---	---	
Severity	N/A	N/A	N/A	None	5	5

This sample is considered malicious based on static code analysis matching on known malware families: final severity level 5

Family Classification

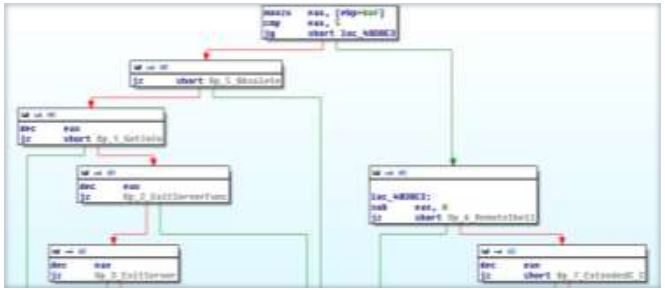
Family Name: **Trojan.Win32.simda**

Similarity Factor: **96.25**

Description: Simda is a Trojan threat which steals data from the victim's machine. It is a multi- component malware which can act as a file-infector, backdoor, password stealer and malware downloader. It is known to target certain banking sites. It can also give malicious hackers backdoor access and provides control to the victim's machine.

Quarian – Designed for Sandbox Evasion

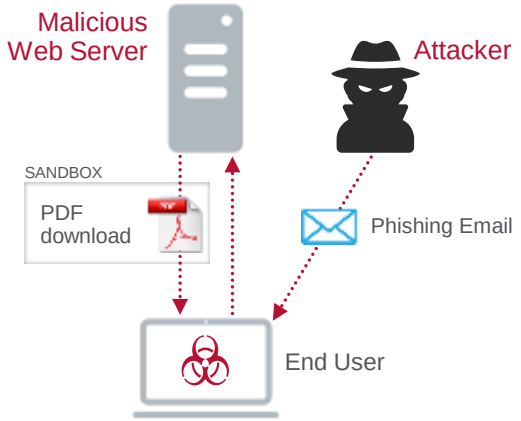
Quarian leverages older code but designed to identify a sandbox and stay silent



Majority of code remains the same as previously known attack

In Action

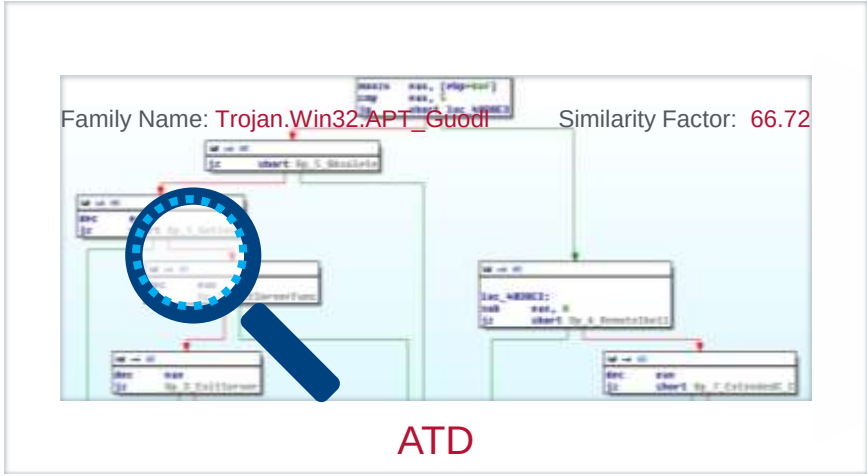
1. User receives phishing email
2. User Clicks link and downloads PDF
3. Other sandboxes see no bad behavior

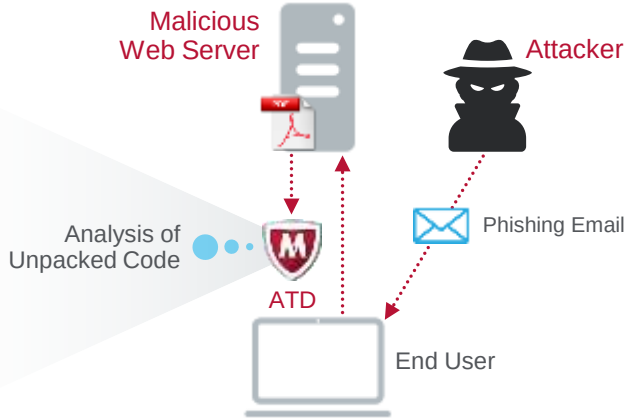


Stopping Quarian and Sandbox Evasions

Advanced Threat Defense and Static Code Analysis

- Advanced Threat Defense scans incoming PDF
- Dynamic Analysis sees no bad behavior
- Static Code Analysis unpacks and identifies code as known malicious





Advanced Threat Defense

Key differentiators

Advanced
Threat Defense

Comprehensive Approach	High-detection Accuracy	Centralized Deployment

Comprehensive Approach to Malware

Advanced Threat Defense

Key differentiators

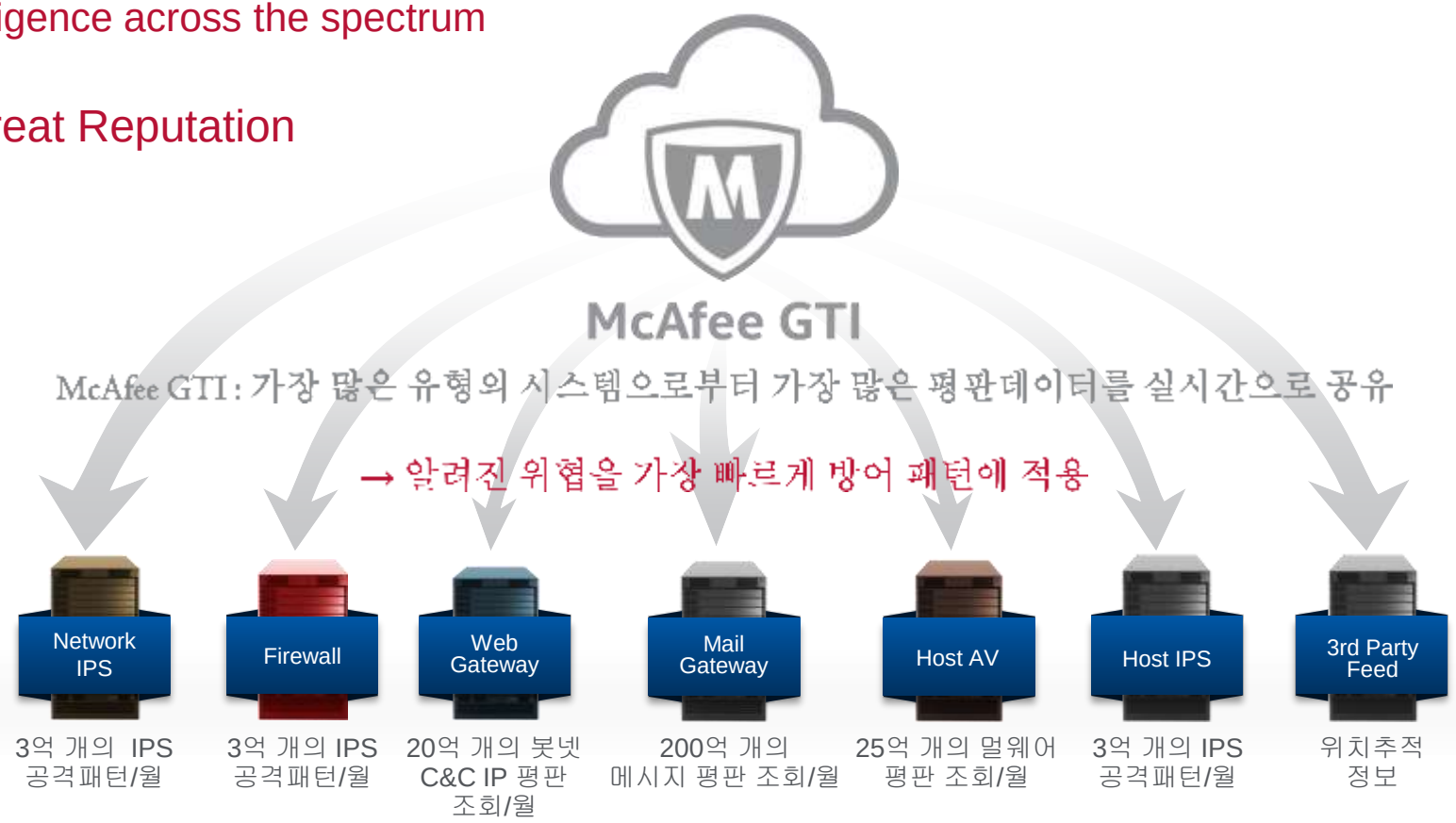
Advanced
Threat Defense

Comprehensive Approach	**High-detection Accuracy**	Centralized Deployment

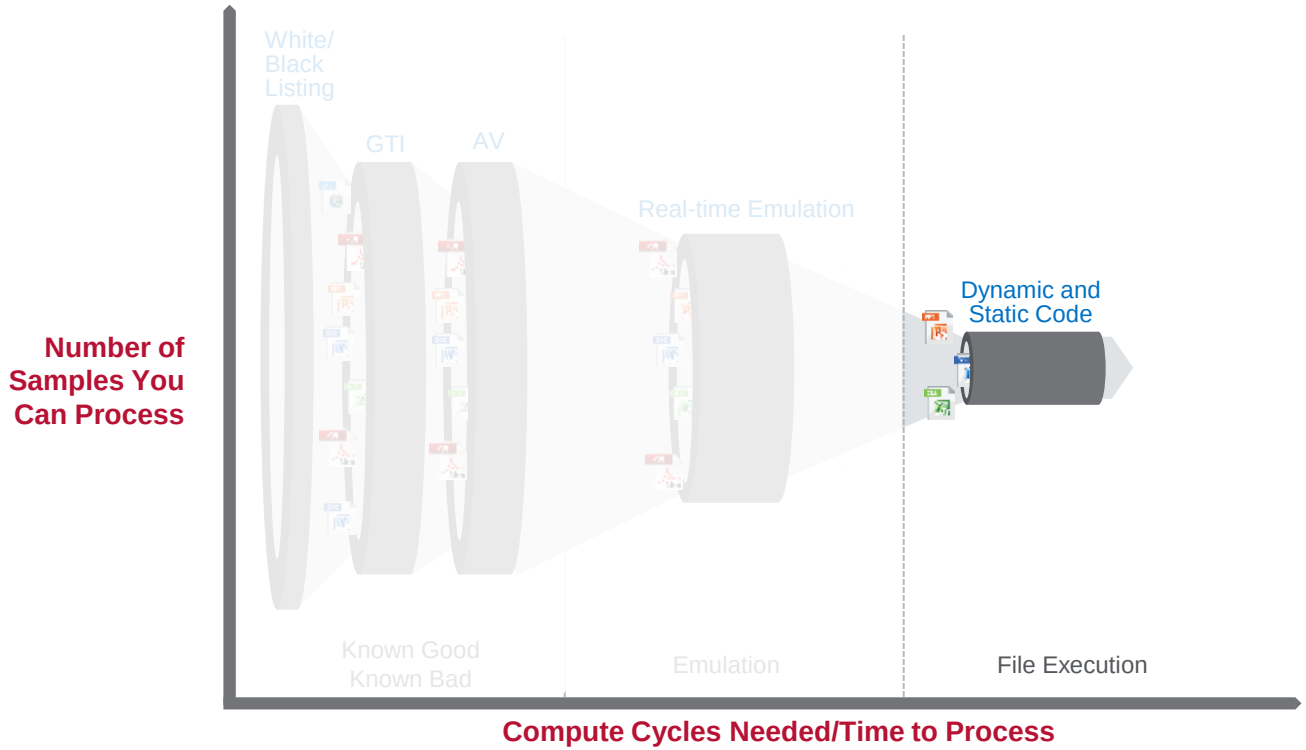
Global Threat Intelligence

Intelligence across the spectrum

Threat Reputation

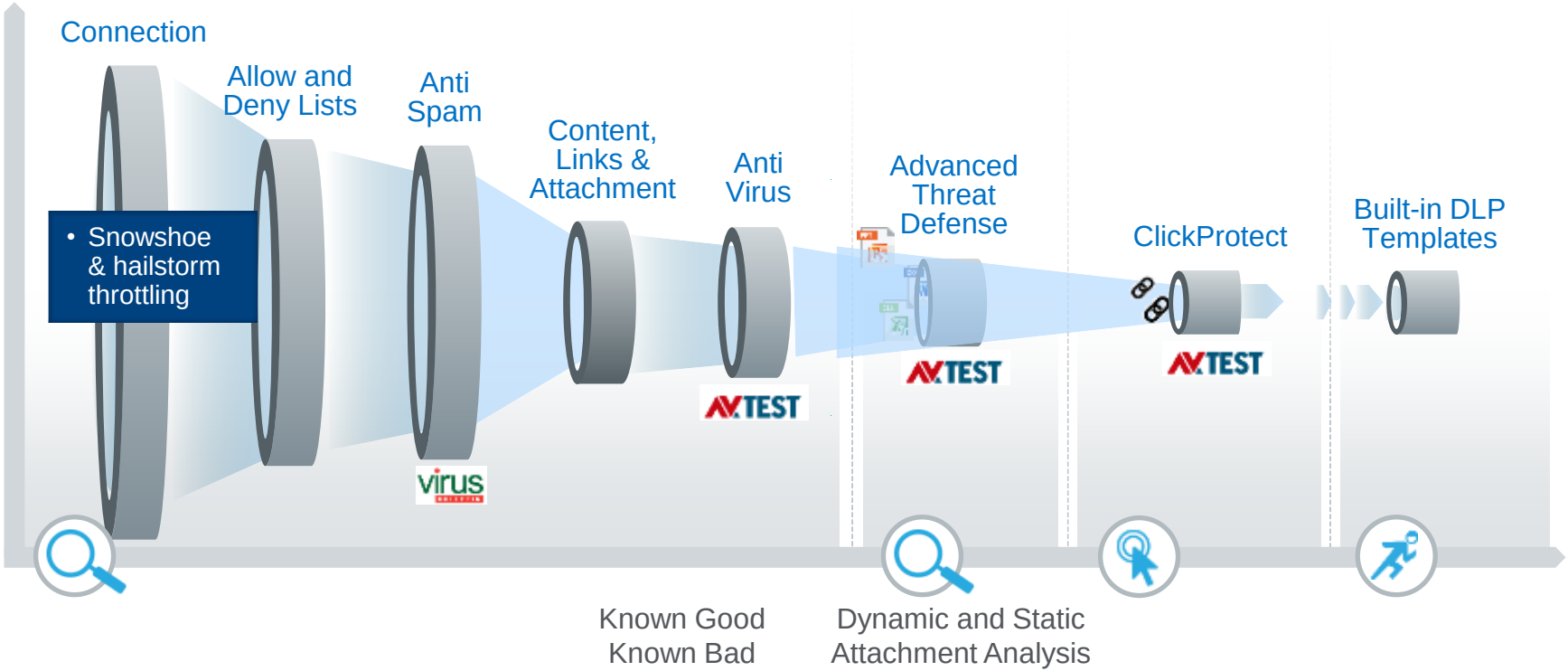


Comprehensive Layered Approach

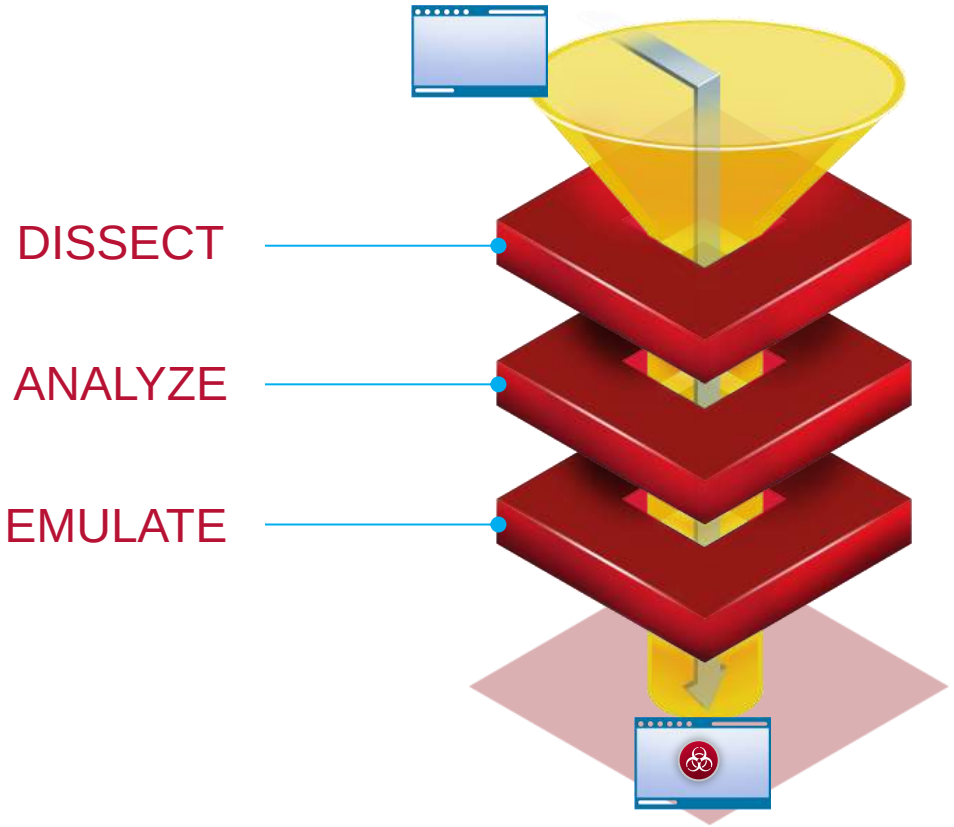


Proven Layered Security for Email

Scan-time, Click-time, and Outbound Data Protection

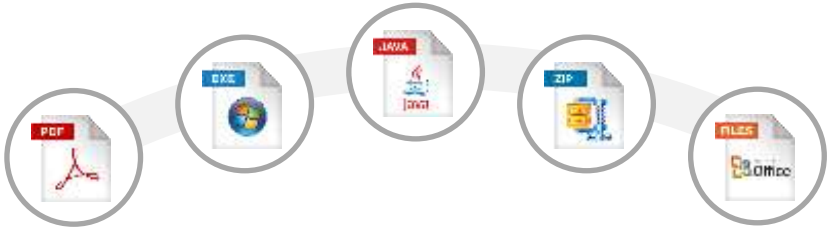


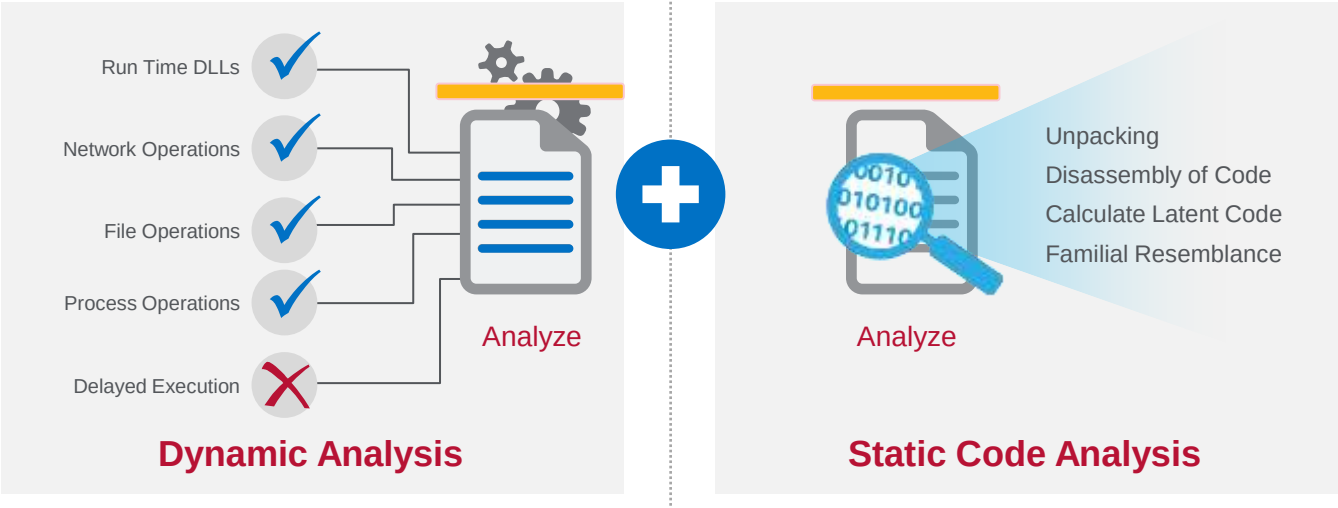
McAfee **Gateway Anti-Malware** Engine Scanning



- 고유한 McAfee 기술
- 에뮬레이션은 실시간 보호를 지원
- 가장 효과적인 zero-day 보호

Dynamic and Static Code Analysis





Advanced Threat Defense

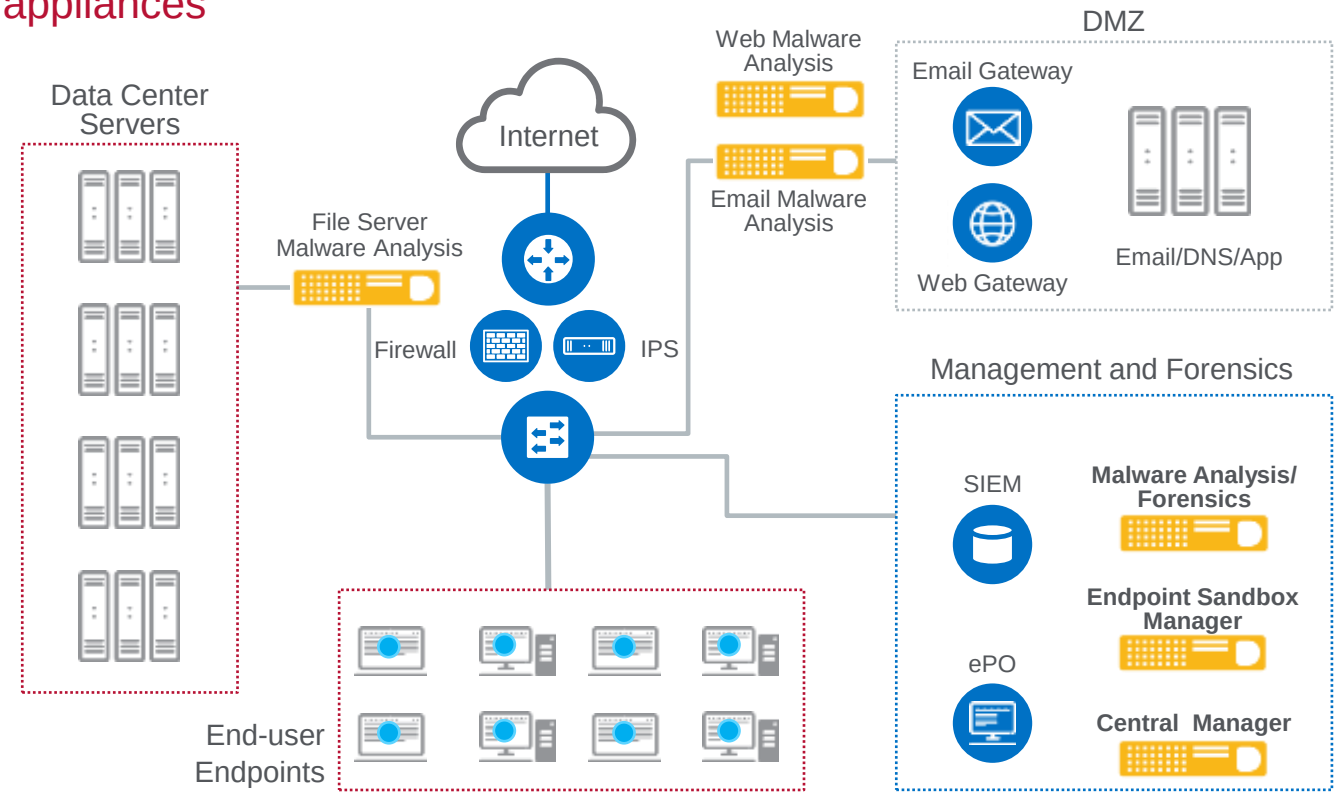
Key differentiators

Advanced
Threat Defense

Comprehensive Approach	High-detection Accuracy	**Centralized Deployment**

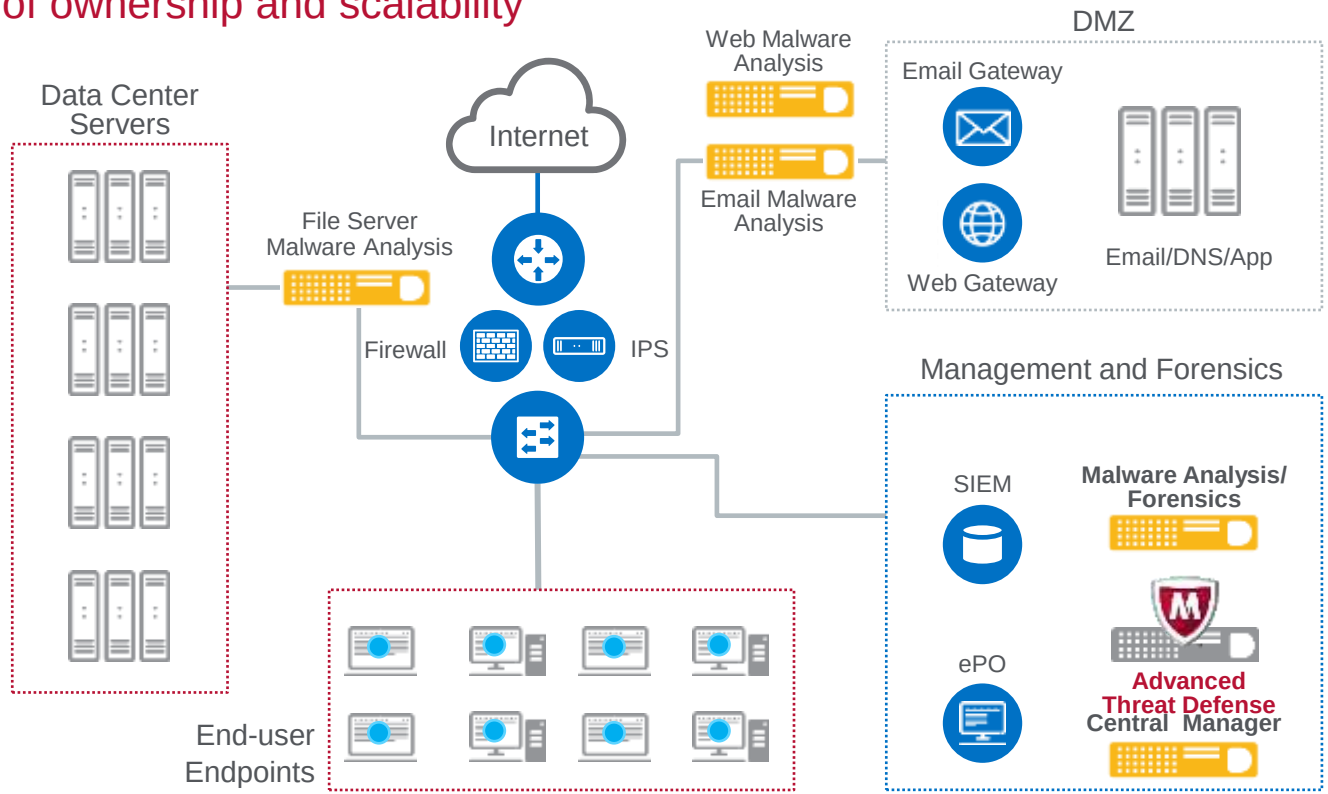
Protocol-Specific Deployment

Numerous appliances



Centralized Deployment

Lower cost of ownership and scalability



Advanced
Threat Defense

Faster Time to Malware Conviction, Containment, and Remediation.

Better Detection, Better Protection.

Lower Total Cost of Ownership.

AV-TEST Results

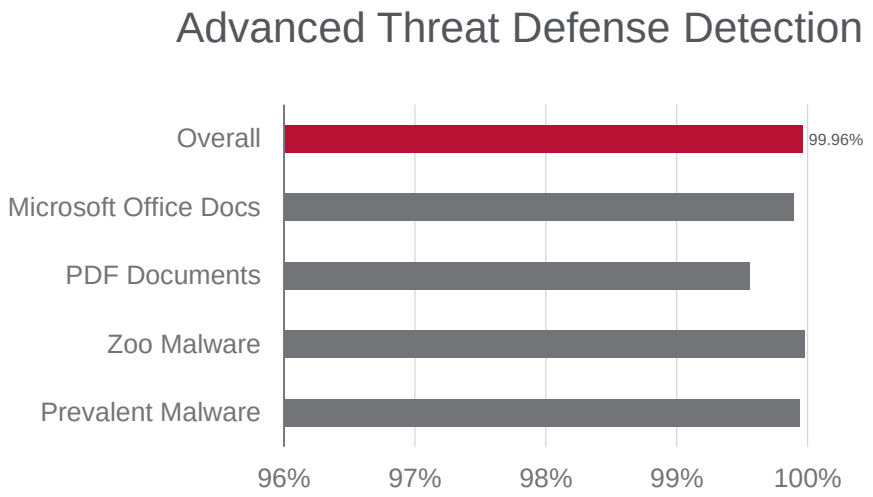
“The appliance showed great performance detecting 99.96% overall and no less than 99.5% in any single tested malware category. It also had a minimum of false positive detections at 0.01%.”

Sample Size: Malicious Files

- 7,616 Microsoft Office docs
- 4,752 PDF docs
- 131,871 Zoo malware
- 12,132 Prevalent malware

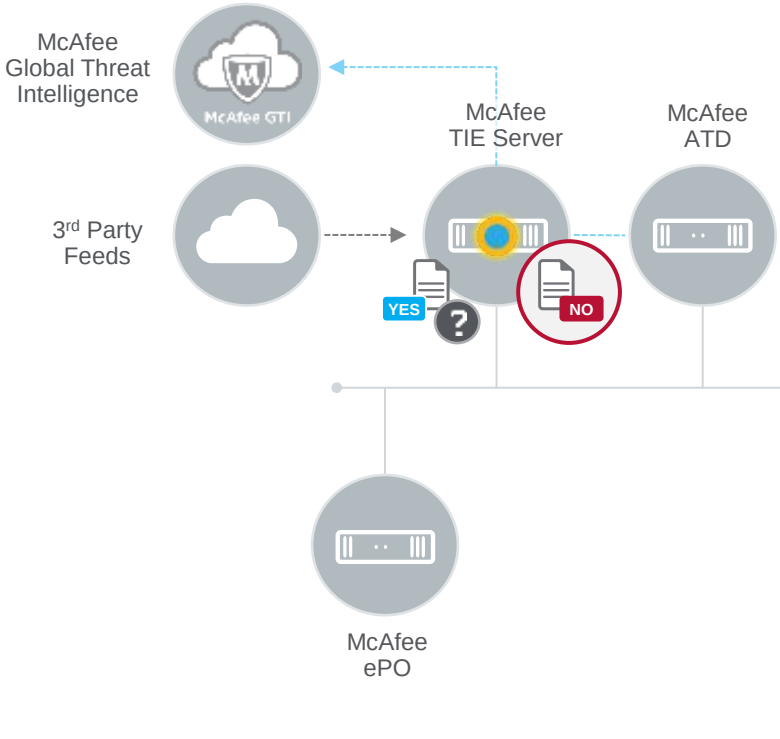
Sample Size: Clean Files

- 96,722 clean files



McAfee Threat Intelligence Exchange

Adapt and immunize—from encounter to containment in milliseconds



Adaptive security improves anti-malware protection

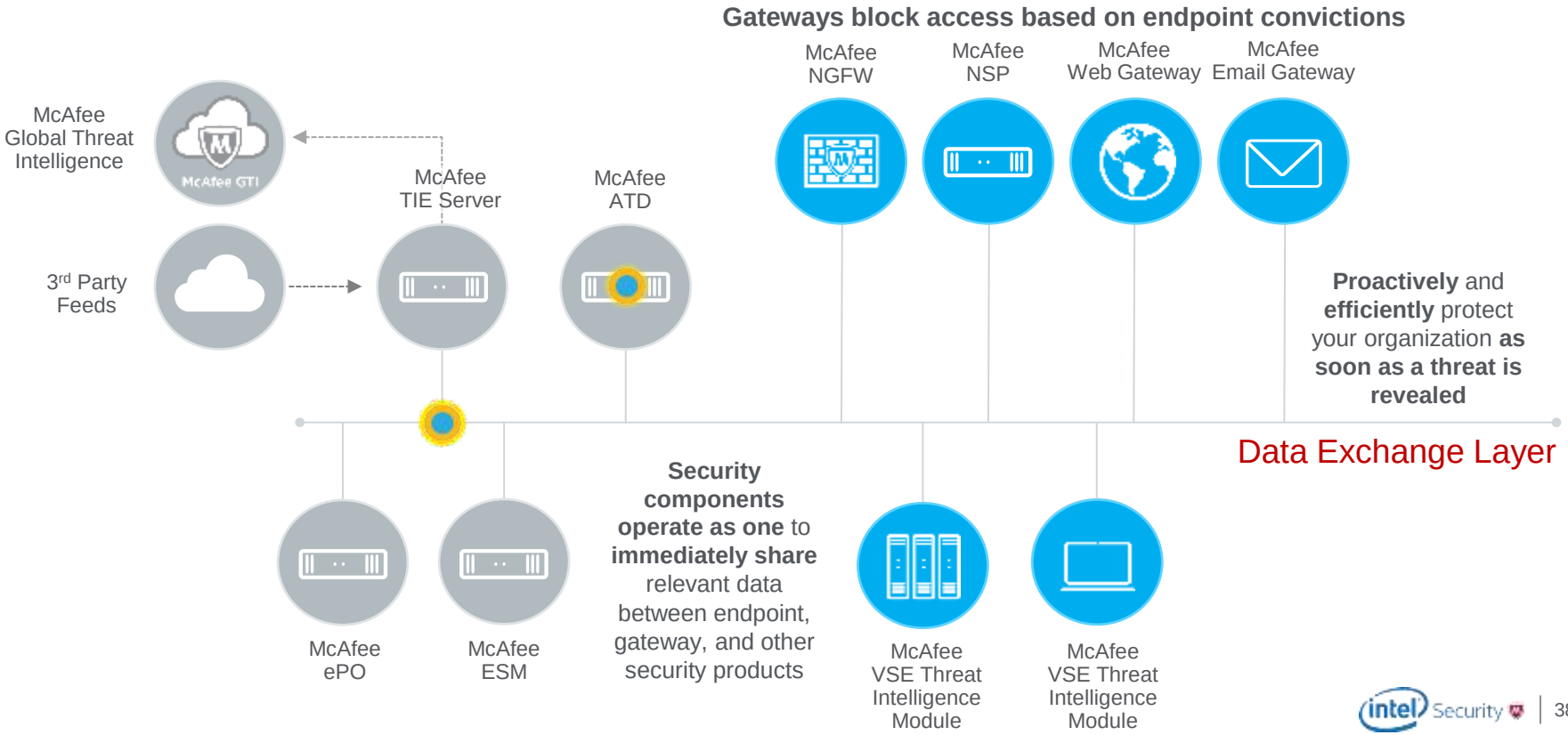
- Better analysis of the gray
- Crowd-source reputations from your own environment
- Manage risk tolerance across departments/system types

Actionable intelligence

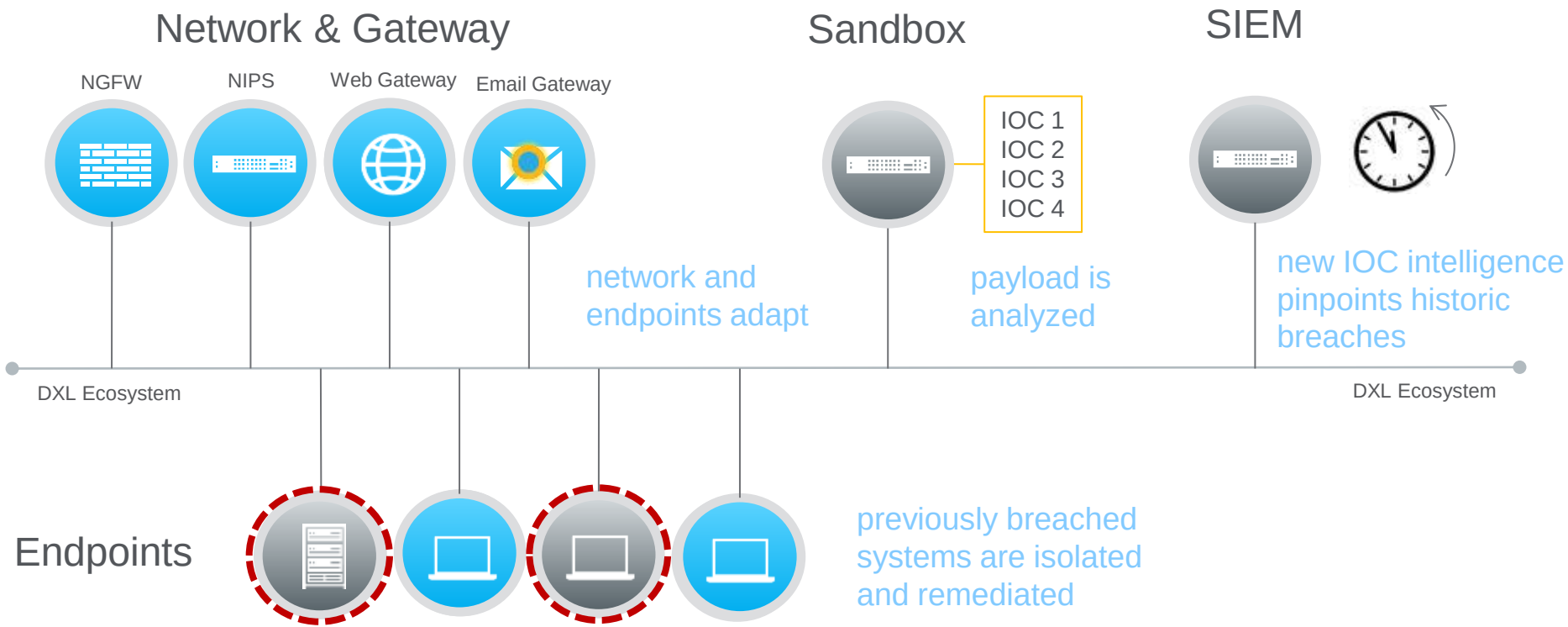
- Early awareness of first occurrence flags attacks as they begin
- Know who may be/was compromised when certificate or file reputation changes

McAfee Threat Intelligence Exchange

Instant protection across the enterprise



Adaptive Threat Prevention and Detection



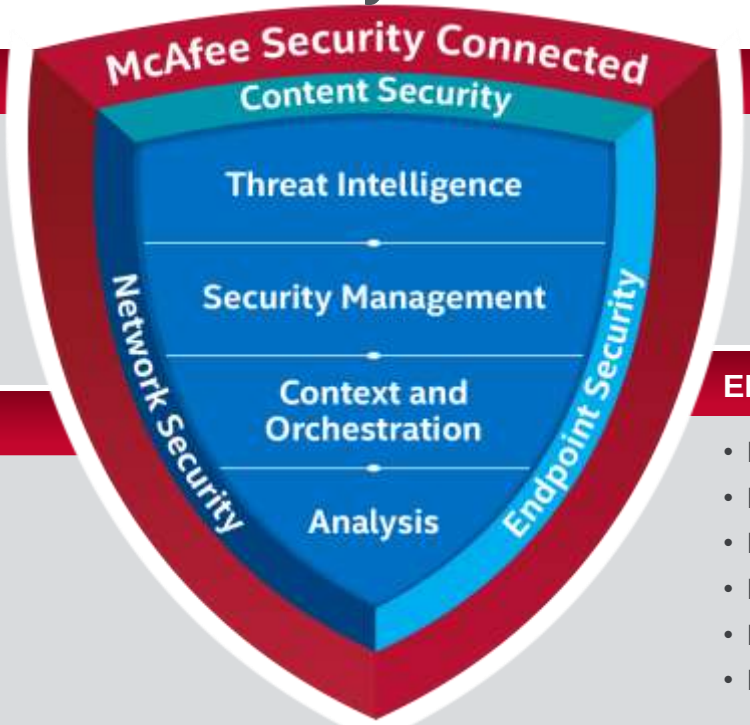
The Security Connected Platform Enabling Adaptive Security Solutions!

SECURITY MANAGEMENT

- **Enterprise Security Manager (SIEM)**
- ePolicy Orchestrator
- **Threat Intelligence Exchange**
- Vulnerability Manager

NETWORK SECURITY

- **Advanced Threat Defense**
- **Network Security Platform (IPS)**
- Firewall Enterprise
- **Next Generation Firewall**



CONTENT SECURITY

- **Email Gateway**
- **Web Gateway**
- Data Loss Prevention

ENDPOINT SECURITY

- Endpoint Security Suites
- Data Center Security Suites
- Embedded Security
- Device Control
- Endpoint Encryption
- Hardware Enhanced Security


intel
Security