



Cloud Enabled Security Services (CESS)

Dr. Hossen Asiful Mustafa

Assistant Professor, IICT, BUET

<https://hossenmustafa.buet.ac.bd>



European Union





Security Issues for Network Services

- DNS Attacks:

- **Domain hijacking:** Domain hijacking is defined as changing the name of a domain without the knowledge or permission from the domain's owner or creator. This enable the intruders to access the sensitive information.
- **Cross site scripting:** It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials.

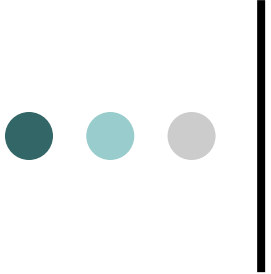
- Man in the Middle Attack:

- This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured.



Security Issues for Network Services

- IP Spoofing:
 - **DOS attack:** When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests.
- Network Sniffing:
 - Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network.

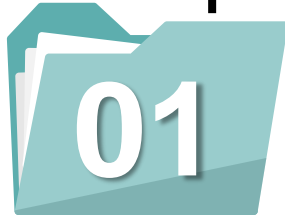


Security as a service (SECaaS)

- Security as a service (**SECaaS**) is a business model in which a service provider integrates their security services into a corporate infrastructure
- SECaaS is inspired by the “Software as a Service (**SaaS**)” model as applied to information security type services
- It does not require on-premises hardware, avoiding substantial capital outlays
- SECaaS provides users with Internet security services providing protection from online threats and attacks such as DDoS.



Security Services



Identity and access management (IAM)



Web Content Filtering



Intrusion detection and prevention (IDP)



Email security



Security information and event management (SIEM)



Vulnerability Management



Identity and Access Management (IAM)

- IAM enables organizations to achieve access control and operational security
- Use cases that need IAM:
 - Organization employees accessing SaaS service using identity federation
 - IT admin access CSP management console to provision resources and access for users using a corporate identity
 - Developers creating accounts for partner users in PaaS
 - End users access storage service in a cloud
 - Applications residing in a cloud serviced provider access storage from another cloud service



IAM Practices

- IAM process consists of the following:
 - User management (for managing identity life cycles),
 - Authentication management,
 - Authorization management,
 - Access management,
 - Data management and provisioning,
 - Provisioning , Monitoring and auditing,
 - Credential and attribute management,
 - Entitlement management,
 - Compliance management,
 - Centralization of authentication and authorization,



Intrusion Detection and Prevention (IDP)

- An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations
- Different Method:
 - Signature-based
 - Anomaly-based, and
 - Stateful protocol analysis
- An intrusion prevention system (IPS) attempts to block an attack detected by IDP



Security Information and Event Management (SIEM)

- SIEM is an approach to security management that combines
 - Security Information Management (SIM) and
 - Security Event Management (SEM)
- SIEM
 - aggregates relevant data from multiple sources,
 - identifies deviations from the norm and
 - takes appropriate action.
- It provides real-time analysis of security alerts generated by applications and network hardware.



Web Content Filtering

- Web Content filtering takes place at two levels:
 - **Application level:** where the filtering is based on URL which may result in blocking a selected web page
 - **Network level:** based on packet filtering which may require routers
 - To examine the IP address of the every incoming or outgoing traffic packet.
 - To perform deep packet inspection (DPI)
- Several levels of filtering
 - Adult content
 - Malicious content
 - Illegal content,



Email Security

- Protection from SPAM
- Protection from malware, virus, etc., attached in the email
- Protect against advanced email attacks such as ransomware by isolating weaponized attachments.
- Block Data Theft With Content-Aware DLP
- Stop credential theft by rendering suspicious websites in read-only mode, preventing users from submitting sensitive data



Vulnerability Management

- The vulnerability management is a continuous process for information security risk that requires management oversight.
- Four high-level processes that encompass vulnerability management:
 - Discovery,
 - Reporting,
 - Prioritization and
 - Response.



CESS

- **Cloud Enabled Security Service (CESS) is a Security as a Service**
- CESS allows a provider to host network security and monitoring services in a cloud
- CESS
 - Is cost effective
 - Is scalable
 - Requires less maintenance
 - Can replace some on-premise appliances



Why CESS?

- Various security measures are available in end devices:
 - Anti-virus software
 - Host based Intrusion Detection Systems (HIDS)
 - Host based firewalls
 - Application whitelisting
 - Endpoint encryption
 - Trusted platform module
 - Mobile device management
 - Sandboxing

Today's Cyber Threat Reality



Not all end devices in the network have protection

Today's Cyber Threat Reality

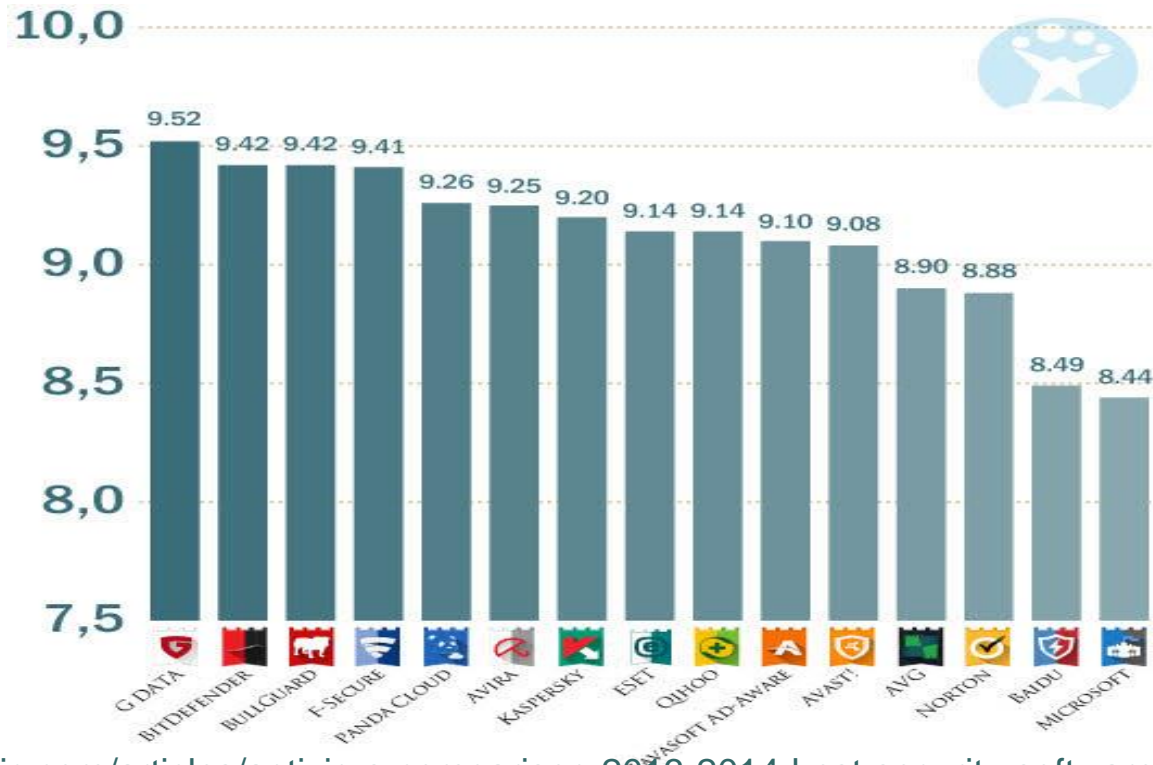


Security is at risk

Threats:	none
Protection components:	main components enabled
 Databases:	out of date
License:	42 days remaining

Protection methods are not regularly updated

Today's Cyber Threat Reality



<https://en.softonic.com/articles/antivirus-comparison-2013-2014-best-security-software?ex=BB-682.1>

No protection method is perfect

Today's Cyber Threat Reality



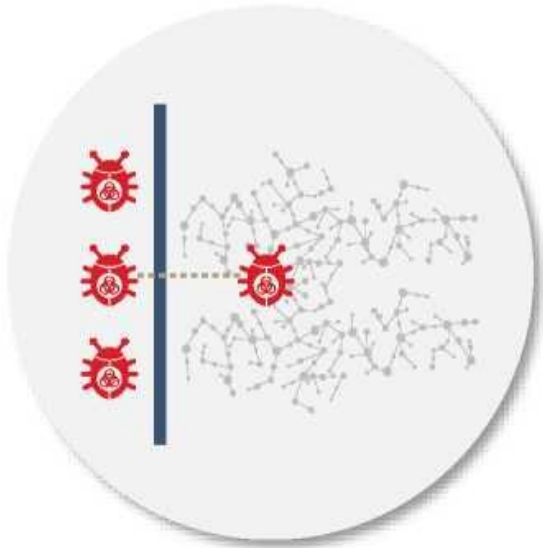
Guest/Own Devices make network more vulnerable

Today's Cyber Threat Reality



The growing number of mobile devices and cloud services creates more opportunities for attacks.

Today's Cyber Threat Reality



Your environment will get breached

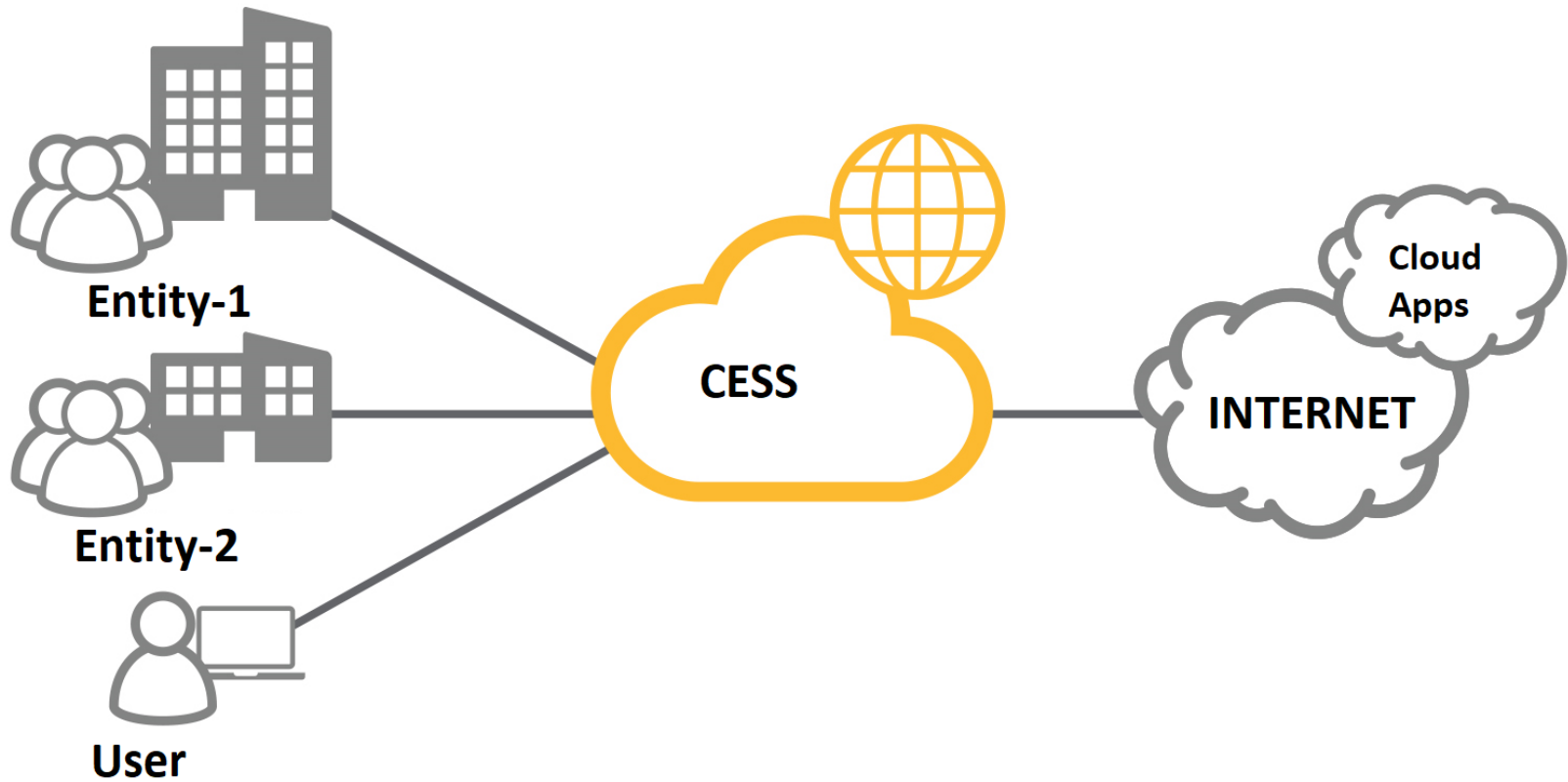


You'll most likely be infected via email



Hackers will likely command and control your environment via web

CESS Can Give Protection to the Whole Network





CESS @ DCNDS

- A proof-of-concept CESS will be deployed in the BdREN cloud to secure web traffic for participating institutions.
- Existing web traffic for BdREN will be diverted through CESS.
- The web security policies will be enforced in the appliances running on the CESS cloud service platform
- All inbound and outbound network traffic for the BDREN will be controlled.



CESS @ DCNDS

- CESS would ensure that security policies can be managed and updated for participating institutions within the NREN in real time.
- Metadata and web usage statistics will be captured and kept in the BdREN cloud
- The captured data will be anonymized
- The anonymized datasets will be shared among stakeholders for research.

Technologies



CISCO Web Security Appliance (WSA)



InstaSafe Security-as-a-Service Solution



Smoothwall Unified Threat Management



Forcepoint Cloud and Email Security



Zscaler Solutions



CESS Case Study

We are implementing CESS at BDRen
as a case study

For implementing, we will be using a
state-of-the-art solution



CESS Benefits

- Broad threat intelligence
- Multiple layers of defence
- Web security
- Email security
- Malware Protection
- Get advanced threat detection
- Vital data loss prevention capabilities
- Reduce costs
- All-in-one solution



Key Features

- Protection **before**, **during**, and **after** an attack
- Get automated monitoring and analysis across the network.
- When compromise occurs, quickly determine the scope of the damage, remediate it, and bring operations back to normal.



Key Features

- Flexible deployment options
- Can be deployed in different hardware
 - on an appliance
 - as a virtual machine, and
 - on a branch router
- Scalable



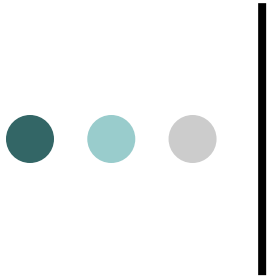
Key Features

- Automated traffic analysis, inbound and outbound
- Scan all web traffic in real time for both known and new malware.
- Use dynamic reputation and behavior based analysis on all web content.
- Fast identification of zero-day attacks
- Scan for suspicious activity over time to find abnormal behaviors.



Key Features

- Application visibility and control
- See what is happening on your network and control it.
- Create and enforce granular policies for websites like Facebook and LinkedIn with embedded applications.
- Protect without slowing productivity or burdening IT resources.



Before, during and after an attack: A security framework

The Attack Continuum





Before an Attack: Use Global Threat Data

- CESS will detect and correlate threats in real time by tapping into the largest threat-detection network in the world
- The detection network can pull massive quantities of information to discover threats across multiple vectors
 - Firewall,
 - IPS,
 - Web,
 - Email,
 - VPN.
- Constantly can refresh information every 3 -5 minutes

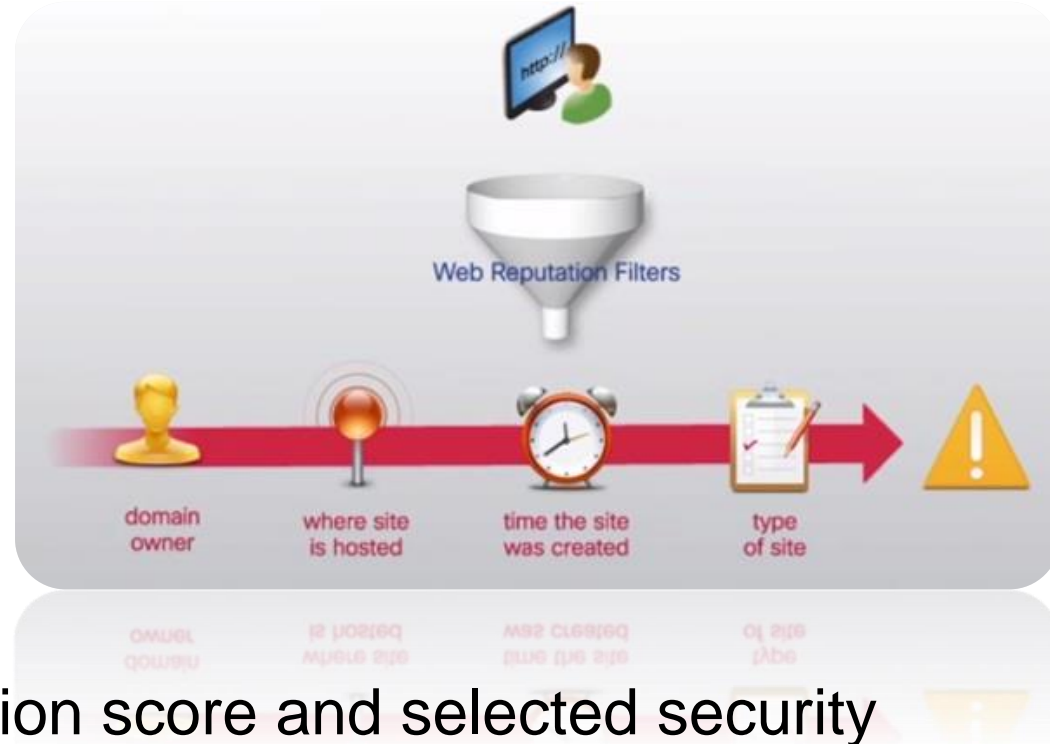


Before an Attack: Web Reputation Filters

- CESS **analyzes** and **categorizes** unknown URLs
- **Blocks** those falling below a defined security threshold.
- **Analyzes** more than 200 different web traffic and network-related parameters to determine the **level of risk** associated with a site.

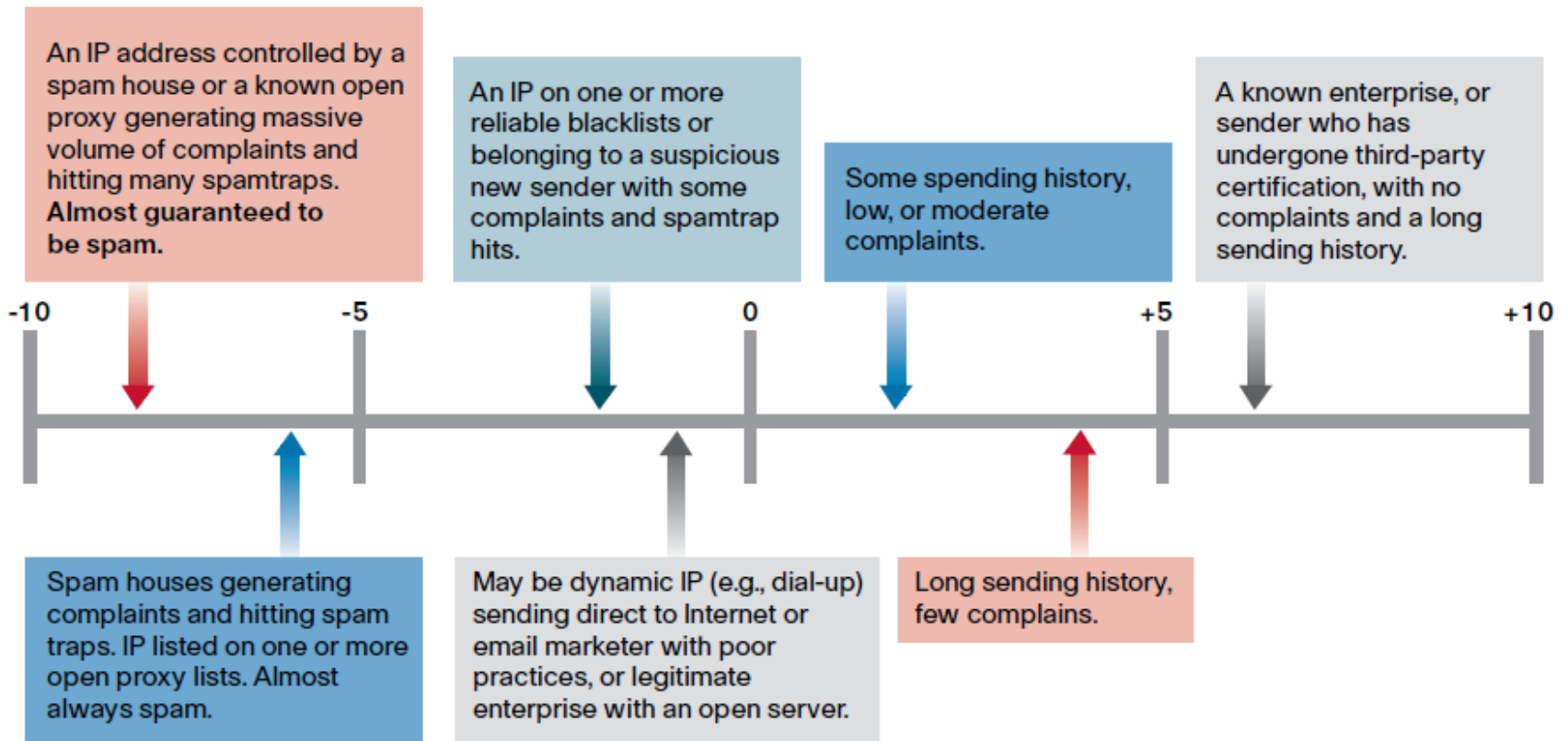
Before an Attack: Web Reputation Filters

- A site is assigned a reputation score based on
 - domain owner
 - Hosting server
 - Time the site was created
 - Type of site



- Based on that reputation score and selected security policies, the site is **blocked**, **allowed**, or **delivered** with a warning.

Reputation Score





Before an Attack: Web Usage Controls

- Traditional URL filtering is combined with real-time Dynamic Content Analysis (DCA).
- Shut down access to sites known to host malware with specific policies
- URL filtering checks against a list of known websites from database (more than 50 million blocked sites).



Before an Attack: Dynamic Content Analysis Engine

- Accurately identified Inappropriate content in real time for 90% of unknown URLs
- Matches closest category by
 - Scanning and
 - Scoring
- Calculates model document proximity



During an Attack: Real-Time Antimalware Scanning

- Malware defense coverage with multiple signature scanning engines run in parallel on a single appliance.
- Robust antimalware inspection
 - optimizes processing speeds
 - prevents traffic bottlenecks
- Adaptive Scanning
 - dynamically selects the most relevant scanner based on URL reputation, content type, and scanner efficacy
 - improves the catch rate by scanning high-risk objects first during increased scan loads.
- Information on the latest coverage with automated updates.



During an Attack: Layer 4 Traffic Monitor

- Scans all traffic, ports, and protocols to detect and block spyware
- Identifies infected clients to help stop malware
- Dynamically adds IP addresses of known malware domains to its list of malicious entities to block.
- Monitor the movement of malware in real time.



During an Attack: Data Loss Prevention (DLP)

- DLP can control and block outbound content
 - file-sharing applications in cloud
 - sensitive information
- Basic DLP : by creating context-based rules
- Third-party DLP solution : can be integrated
 - deep content inspection
 - regulatory compliance
 - intellectual property protection.
 - enforcement of DLP policies.

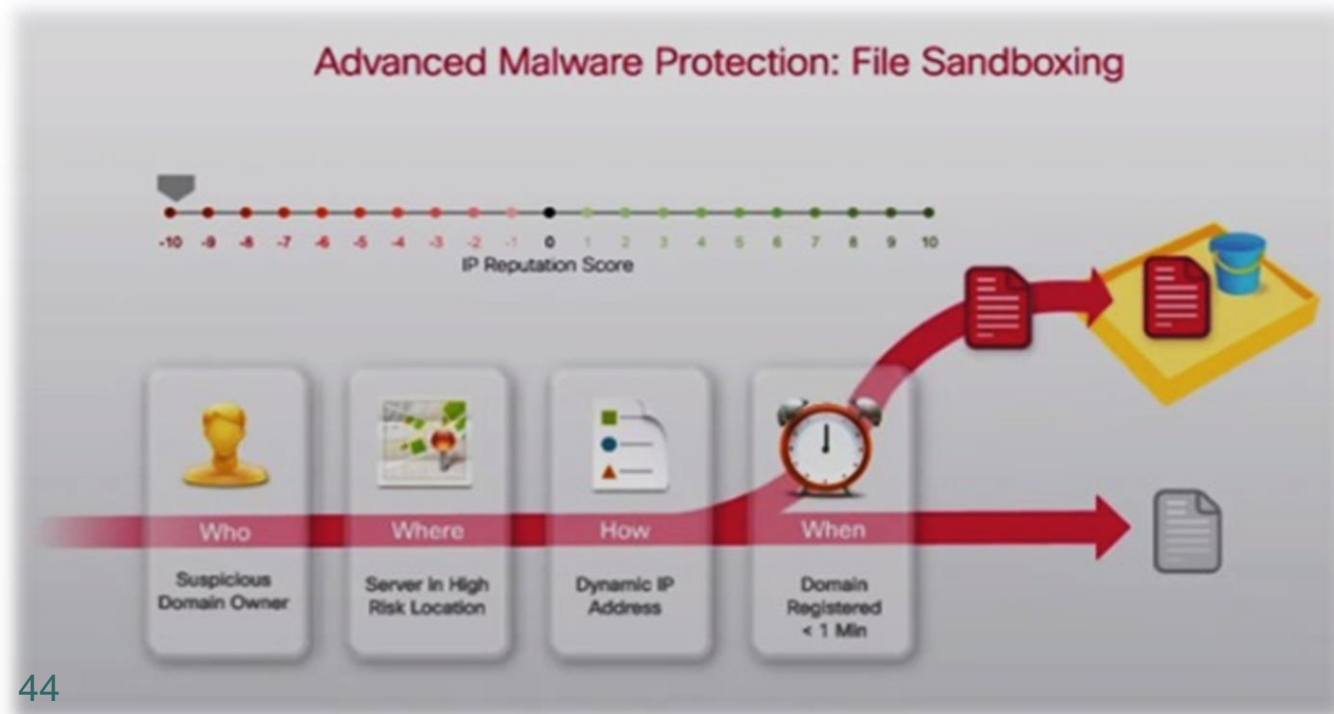


During an Attack: Cloud Access Security

- Partnered with leading Cloud Access Security Broker (CASB)
- Monitor cloud app usage in real time.
- Full visibility of cloud app environment
- Classify all cloud traffic passing through the gateway
- Detect intrusions and data leakage
- Automatically enforcing any new global security policies across all sanctioned and unsanctioned apps.

During an Attack: File Sandboxing

- If a given file is analysed by all other antimalware engines and identified is **unknown**, it automatically send to an analysis engine in an **isolated environment**.





During an Attack: Advanced malware protection (AMP)

- Uncovered precise details about the sandboxed files behaviour
- Combines that data with details with human and machine analysis
- Determine it's disposition.



During an Attack: File Reputation and Analysis

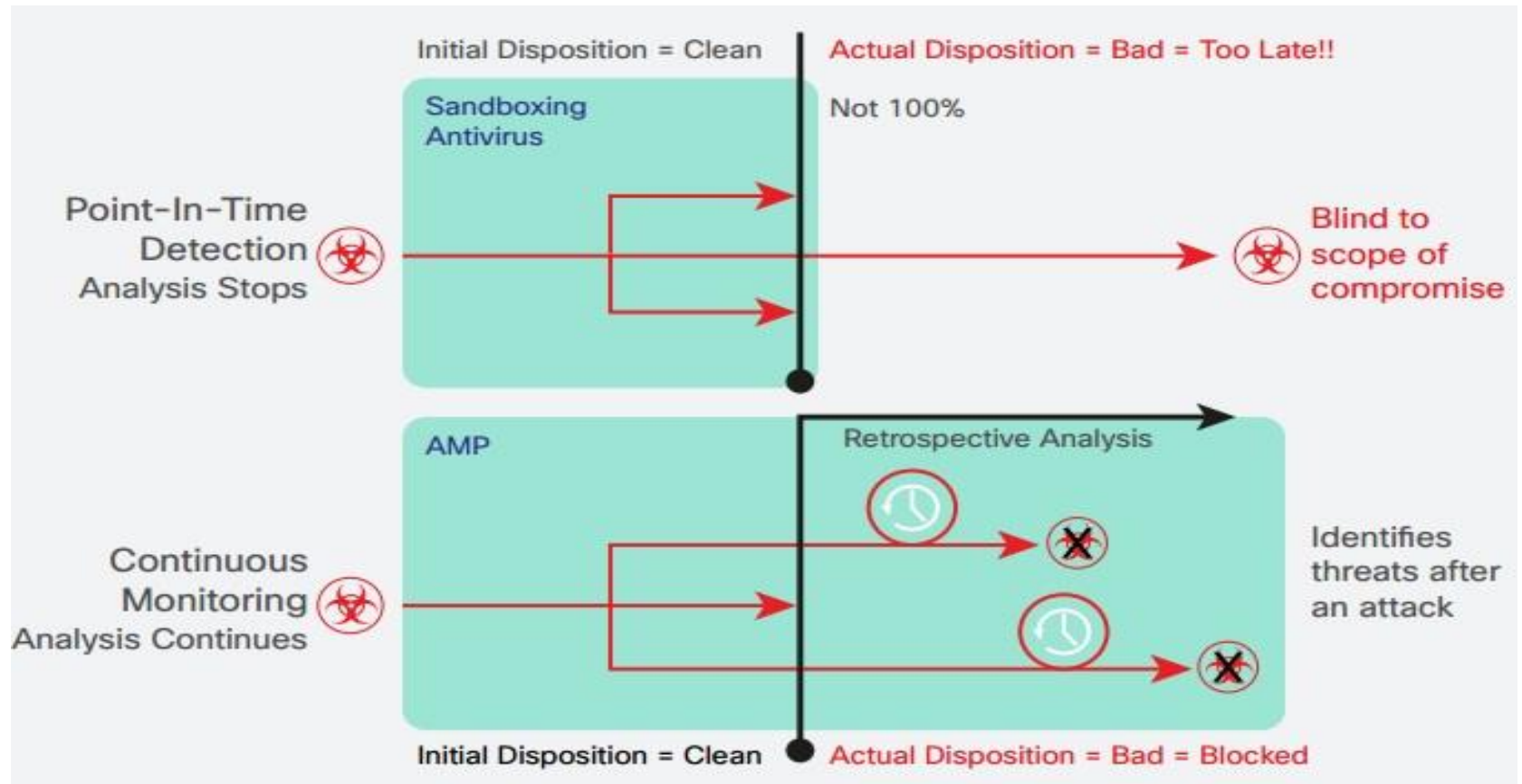
- AMP Captures a fingerprint of each file
- Sends it to the cloud-based threat intelligence network for a reputation verdict checked against zero-day exploits.
- When malware is detected, AMP
 - finds precise detail about a file's behavior
 - combines that data with detailed human and machine analysis
 - determines the file's threat level in a sandbox.



After an Attack: File Retrospection by AMP

- It continuously analyzes files that have traversed the security gateway, regardless of their initial disposition.
- Retrospective verdict alerting
- Visibility into who on the network may have been infected and when.
- Security teams can then identify and address an attack quickly, before it has a chance to spread

After an Attack: Retrospective Analysis with AMP





After an Attack: Cognitive Threat Analytics (CTA)

- The integration of CTA with AMP allows to:
 - Automatically identify and investigate suspicious or malicious web based traffic.
 - Analyze information generated by existing web security solutions without the need for additional hardware or software.
 - Zero in on malicious activity that has bypassed security controls and is using web-based communications, including standard, encrypted, and anonymous channels that can be used to attack the organization.



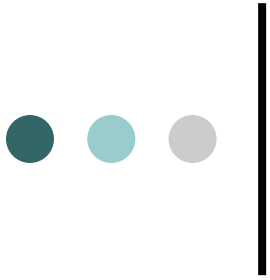
After an Attack: Cognitive Threat Analytics (CTA)

- The integration of CTA with AMP for Web Security allows to:
 - Create a baseline of **normal activity** and identify **anomalous traffic** occurring within the network.
 - Analyze device behavior and web traffic to pinpoint command-and control communications and data exfiltration.



Research Goals

- Provide security to the institutions connected
- Understand and study effectiveness/limitations of the solution
- Collect metadata for research which may be used for
 - New algorithms
 - Weakness analysis
 - Data analytics
 - More
- Implement a version of web reputation filter



Questions?