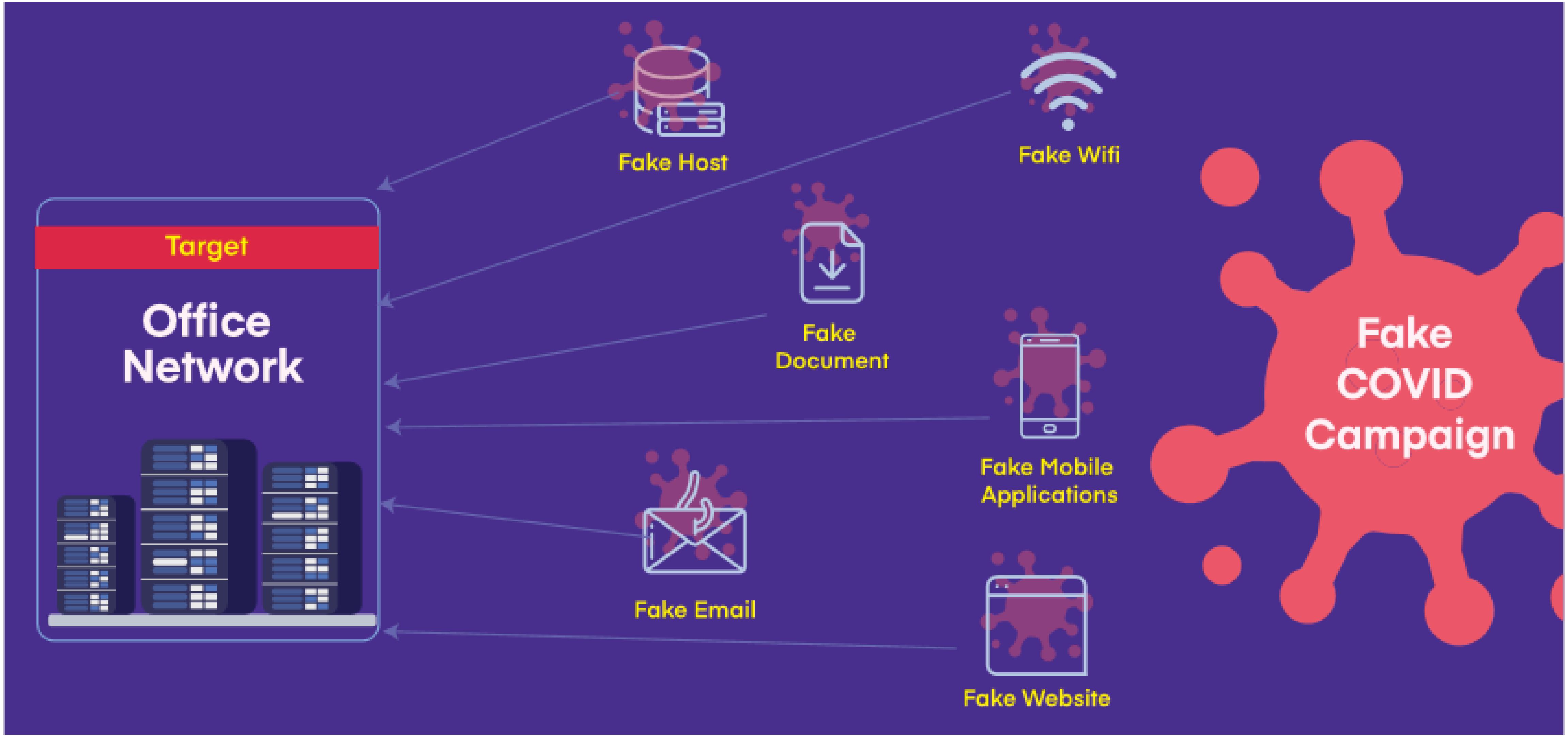
Technical Approach

Cyber Threat of WFH & How to Digitally Sanitize

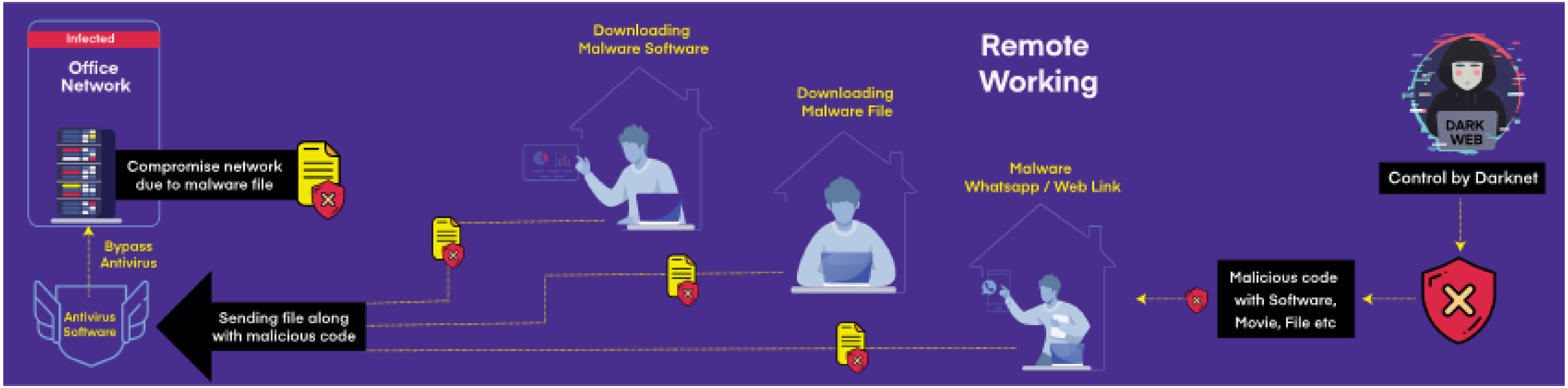
Infopercept

INVINSENSE

WFM2020 Malwares Strategy – Unknown Unknown Situation



Proposed Definition


Infected
Office Network
Compromise network due to malware file
Bypass Antivirus
Antivirus Software
Sending file along with malicious code
Downloading Malware Software
Downloading Malware File
Remote Working
Malware Whatsapp / Web Link
DARK WEB
Control by Darknet
Malicious code with Software, Movie, File etc

CEO Concerns Intellectual Properties

- Formulas
- Pricing
- Business Secrets
- Go-To-Market Strategy
- Innovation etc.

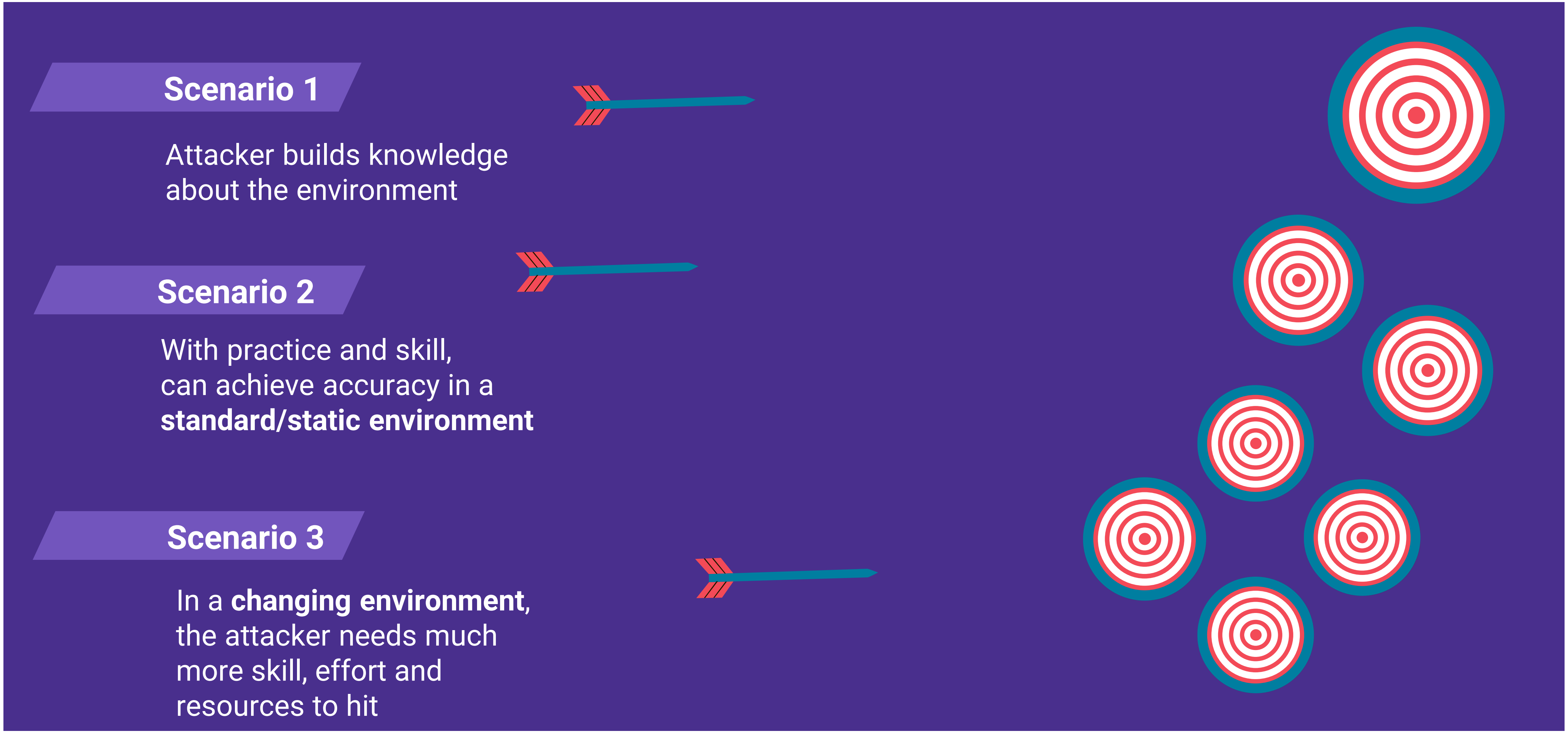
Companies are ready with

- Compliance
- Best practice
- secure remote user access with MFA
- Anti-Virus

CIO and CISO are worried about

- Advance Attacks on endpoints
- Existing endpoint solutions not enough
- What will happen when this compromised system will come back to network

The Science of Targeting



Scenario 1

Attacker builds knowledge about the environment

Scenario 2

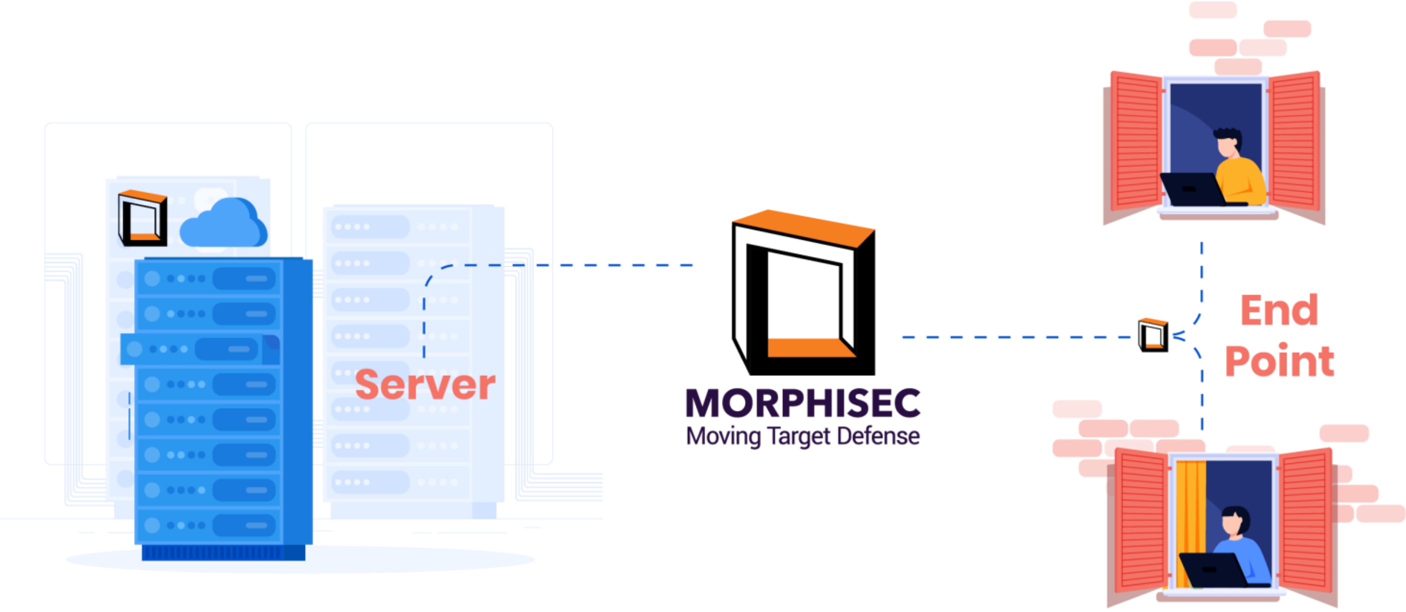
With practice and skill, can achieve accuracy in a **standard/static environment**

Scenario 3

In a **changing environment**, the attacker needs much more skill, effort and resources to hit

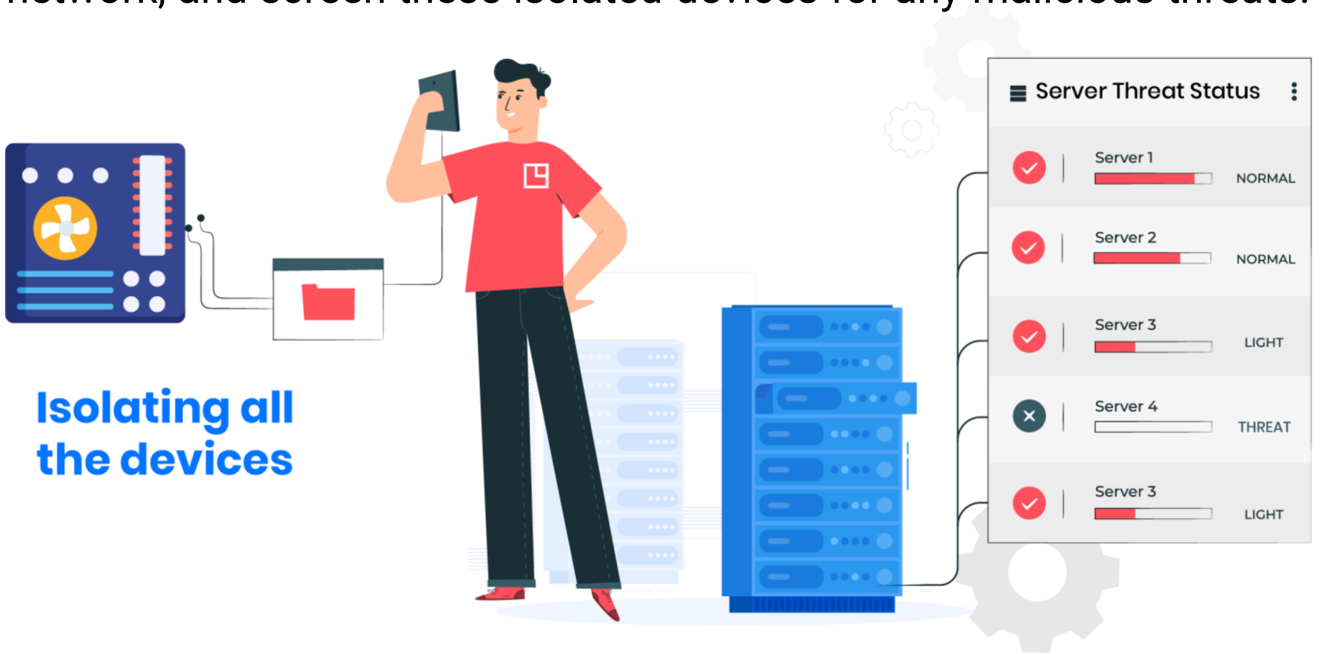
Step 1

Installing the Morphisec Agent on all End Points and Servers, which is a next generation solution that has a disruptive approach and uses a moving target defense to protect advanced threats.



Step 2

Isolate all the devices that come back from “Work from Home” and will be connecting to the network, and screen these isolated devices for any malicious threats.

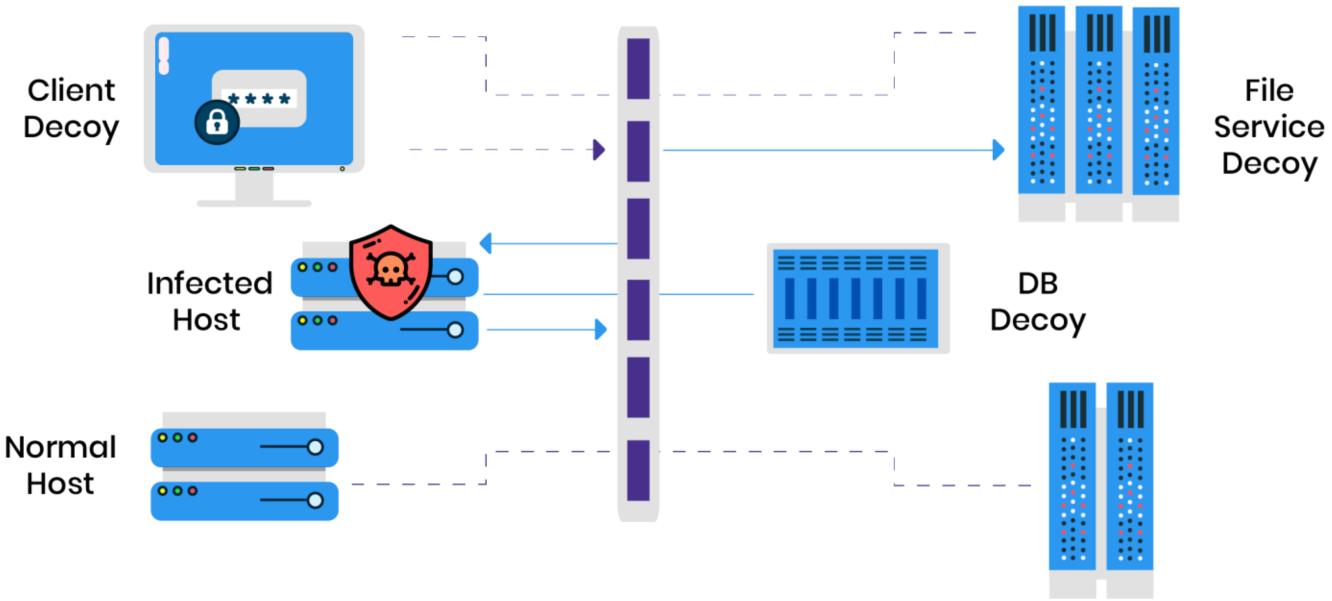


Server Threat Status

✓	Server 1	NORMAL
✓	Server 2	NORMAL
✓	Server 3	LIGHT
✕	Server 4	THREAT
✓	Server 3	LIGHT

Step 3

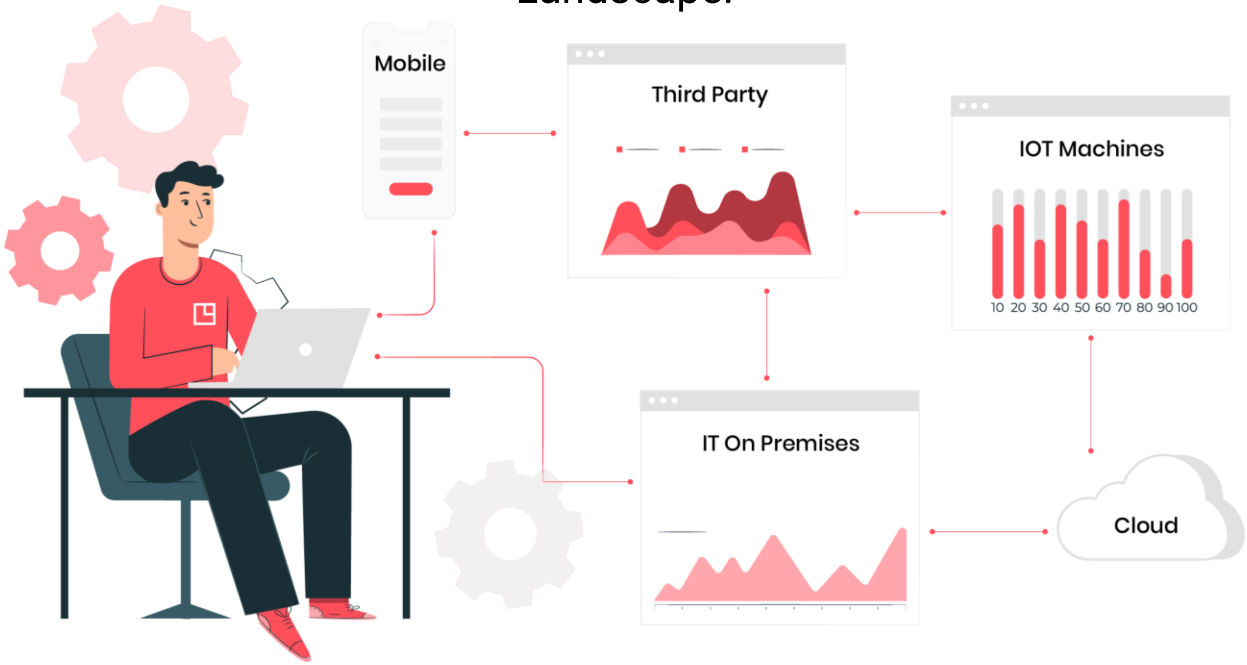
Strategize the Decoy's implementation across business networks to be able to early detect - later movements, detect potential breaches and advance attacks in the environment.



Partial list of technical test cases performed by Infopercept

Step 4

Perform 24*7 Security Monitoring to Actively look for new threats that may arise in the IT Landscape.

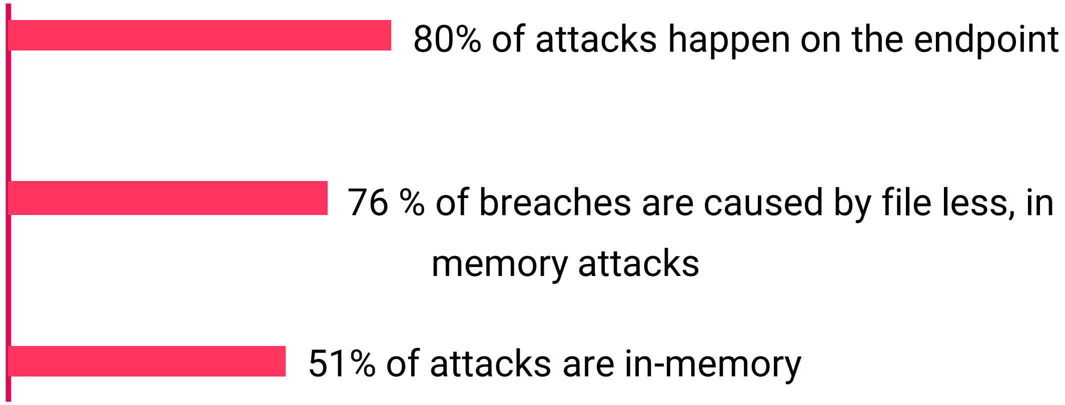


Discussion

Recent Example

- LockerGoga ransomware cost Norsk Hydro $45 million so far and gains dropped 82%
- Lake City and Riviera Beach, Florida together paid attackers over $1 million following ransomware attacks
- POS malware stole millions of customer payment details from restaurant chains Buca de Beppo, Planet Hollywood and other Earl Enterprise companies

The 2017 State of Endpoint Security Risk, Ponemon Institute, October 2017



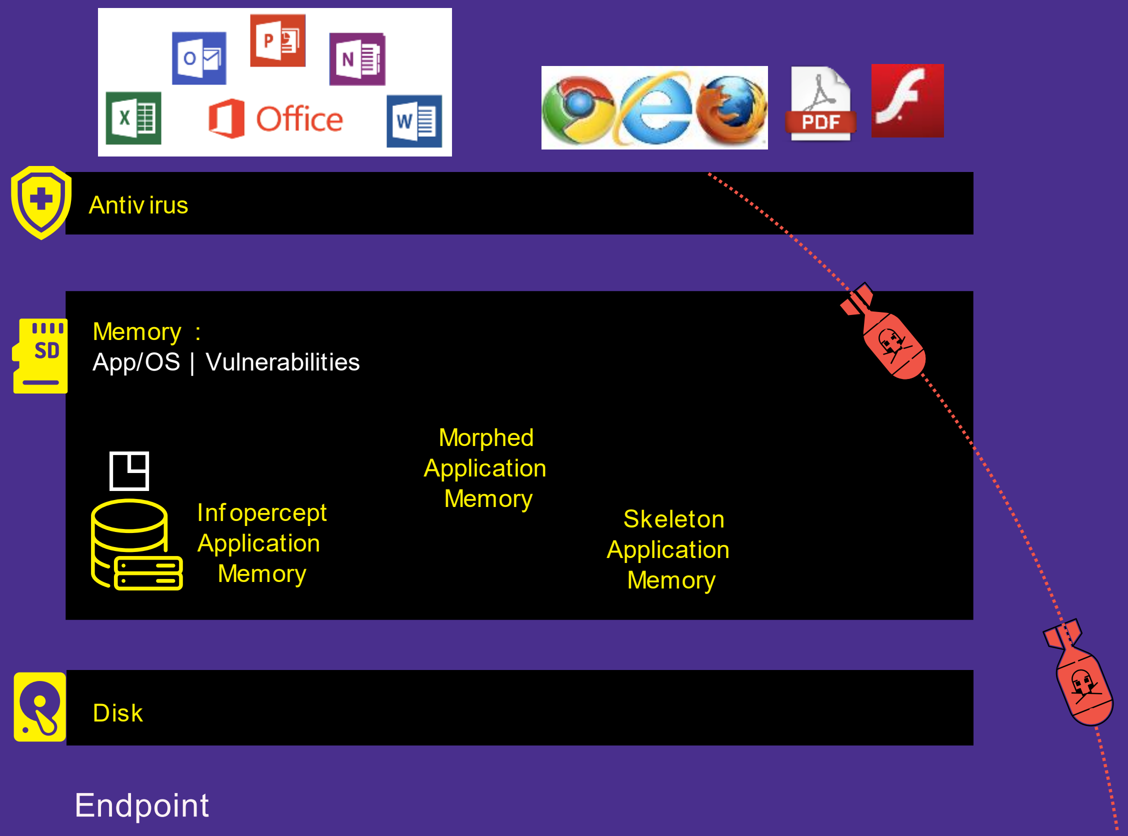
EXISTING SOLUTIONS rely on **PRIOR KNOWLEDGE** and are **DEFENSELESS** against **unknown, evasive threats**.

Moving Target Defense Implementation

Prevention
Prevents zero-days, targeted and unknown attacks, with no prior knowledge

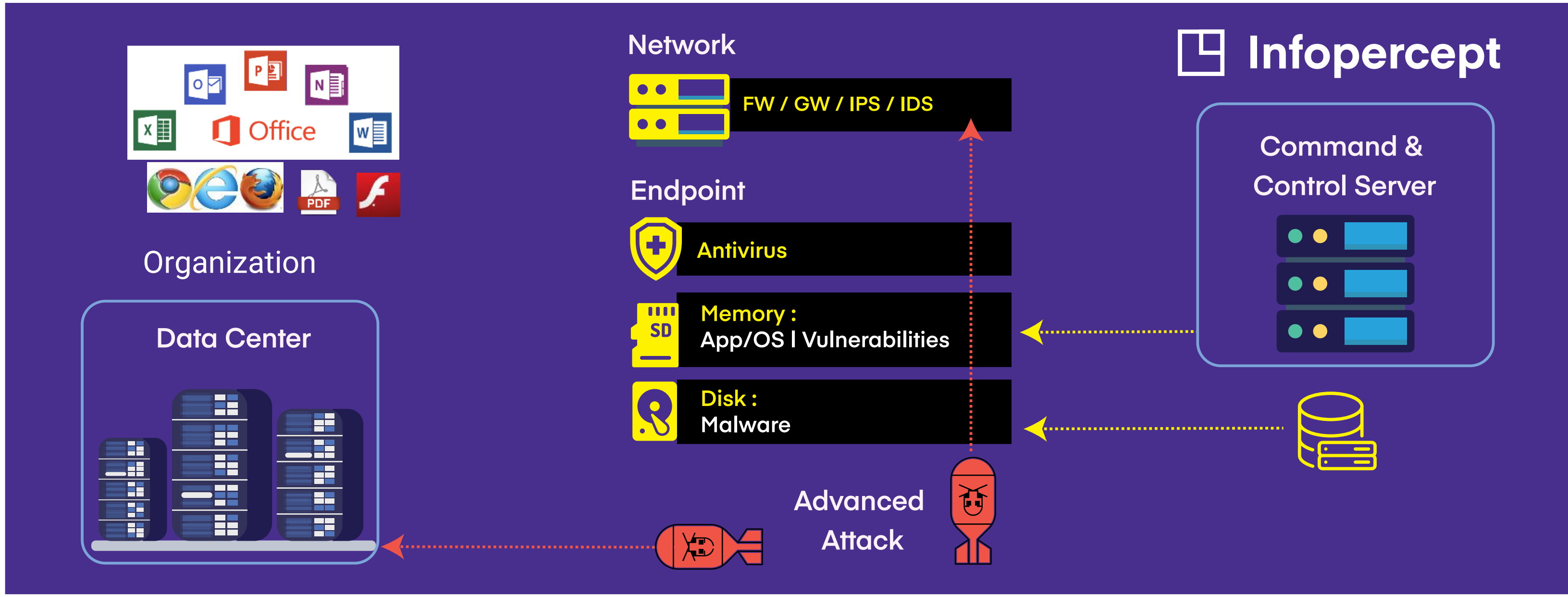
Deterministic
Eliminates false positives

Resilience
Randomization of each process
• Moving Target


Office
PDF
Antiv irus
Memory :
App/OS | Vulnerabilities
Morphed Application Memory
Inf opercept Application Memory
Skeleton Application Memory
Disk
Endpoint

Infopercept

Memory A Mission Critical Battlefield



Denial-of-attack stops attacks at initial penetration stage, before malware downloaded from C2C or if malware already persistent and tries to evade

Most of advanced attacks uses memory resources and vulnerabilities in applications and operating systems

Memory is used at one or multiple stages in the attack kill chain in order to penetrate or evade from traditional Prevention and Detection systems

Traditional security products focus on executables and inefficient memory scanning thus fail to prevent advanced memory based attacks

Current Cyber-Defense Landscape

	USE CASE	SHORTCOMINGS
Signature / Whitelist	Implemented at both network and endpoint	Requires constant updates
Sandbox	Devices placed at the perimeter to emulate files in a contained environment and assess risk	Sandbox aware malware can easily evade sandbox detection by delaying mechanism
Artificial Intelligence	Machine Learning/Deep Learning work on principle of training set deployed on the cloud.	IOA needs to be downloaded to the host to prevent if connectivity to cloud is not present. - League of signature based solution plus false positive - also adds burden to users
Behavior Monitoring	Looks for behavior anomalies of processes to make a decision	Based on known behaviors only

The Current Anti-APT Technologies

ADDITIONAL LIMITATIONS

Signature / Whitelist	Only known attacks can be prevented.
Sandbox	**Time:** On average sandboxes require 5 mins to analyze a file and most have a cut-out time of 20 mins, after which file is released termed as benign. This is enough time for a patient zero infection to occur in the environment.
Artificial Intelligence	Works on principle of prior knowledge. The training set needs to be configured by humans to understand the pattern. If the malware strain is not identified by the training set then it is marked as clean, resulting in infection in network. If IOA downloaded locally does not identify the malware, then it needs to be sent to cloud and await results, bringing to prominence Time factor
Behavior Monitoring	Programmed to detect certain anomalies which means it works on principle of prior knowledge. If malware evades the detection mechanism, then it bypasses the solution.

Benefits of Infopercept Approach

Endpoints

- Prevention of in-memory zero days or file-less attacks
- Application Virtual Patching against in-memory attacks for commonly used applications
- Protection from Mimikatz Credential Stealing attacks
- Enhanced Lateral movement attack prevention by WMI coverage
- Prevention of Shell Code Injections

Servers

- Enhanced Lateral movement attack prevention by WMI coverage
- Prevention of Shell Code Injections
- Protection from Mimikatz Credential Stealing attacks
- Application Virtual Patching capabilities against in-memory attacks on default applications installed on server's(ex browsers, adobe etc)

Network

- Identify Compromise System
- Identify Horizontal Movement
- Real-time Threat Intelligence specific to environment
- Less False Positive

About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Imprint

Address

3rd floor, Optionz Complex
Opp. Hotel Regenta,
CG Road, Navrangpura,
Ahmedabad - 380 009,
Gujarat, India.

Contact Info

M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

Global Office

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait

India
+91 9898857117

Infopercept