ThreatDown™
Powered by Malwarebytes

Infocom 2024

Athens 10-11 April 2024

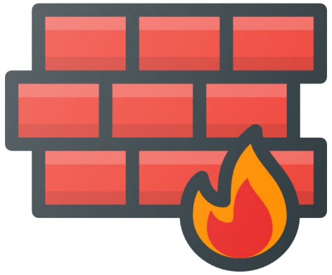
Claudio Tosi

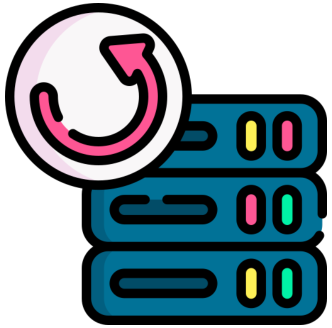
Global Solutions Engineering Manager

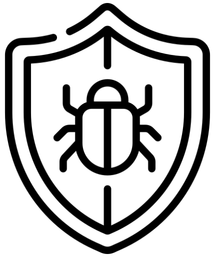
EMEA Regulations

IT Challenges – 12 years ago

- Standard Practice
  - Firewall
  - Backups
  - Remote Access
  - Anti-Virus
  - Projects
  - Tickets







IT/Security Challenges - Today

Cybersecurity:
Threat Detection and Response
Compliance with Data Protection Laws
Firewall and Network Security
Endpoint Security
Security Training and Awareness
Incident Response Planning

Infrastructure Management:
Network Monitoring and Management
Server Administration
Storage Management
Virtualization Technologies (e.g., VMware, Hyper-V)
Cloud Infrastructure (e.g., AWS, Azure, GCP)
Patch Management
Backup and Disaster Recovery

Monitoring and Performance Management:
Network Performance Monitoring
Application Performance Management
User Experience Monitoring

Communication and Collaboration Tools:
Email Systems (e.g., Microsoft Exchange, Google Workspace)
VoIP Systems
Video Conferencing Tools (e.g., Zoom, Microsoft Teams)

Mobility and Remote Work Solutions:
Virtual Private Networks (VPNs)
Mobile Device Management (MDM)
Remote Desktop Solutions

Compliance and Reporting:
Compliance Auditing and Reporting
IT Governance
Risk Management

Technology Stack Management:
Operating System Deployment and Management (e.g., Windows, Linux)
Application Management (e.g., Microsoft 365, Salesforce)
Database Management (e.g., SQL Server, Oracle)
Middleware Management

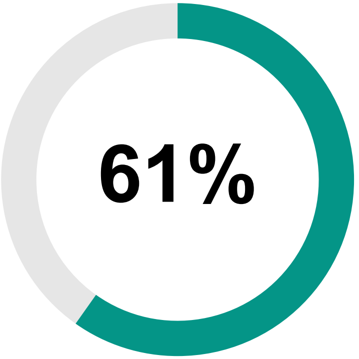
Strategic IT Consulting:
IT Budget Planning
Technology Roadmapping
Business Continuity Planning

Automation and Optimization:
Process Automation
IT Operations Analytics
Asset Management

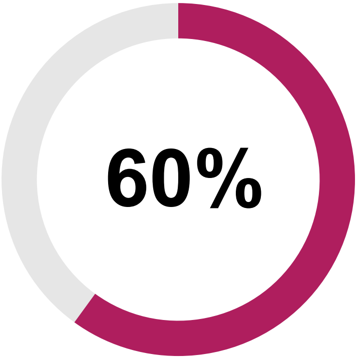
ThreatDown™
Powered by Malwarebytes

Endpoint security challenges

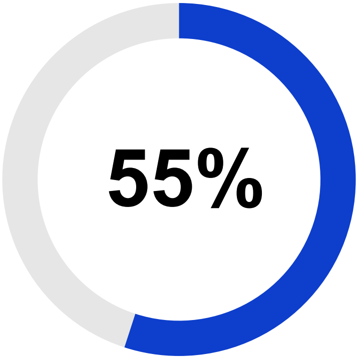
Complexity



Effectiveness



Performance



Source: 2022 Endpoint Detection and Response Study, Ponemon Institute

How is this happening?

Cyber Criminals are going after the easy targets

68%

The number of known Ransomware attacks increased in 2023

82%

82% of ransomware attacks were against companies with fewer than 1,000 employees.

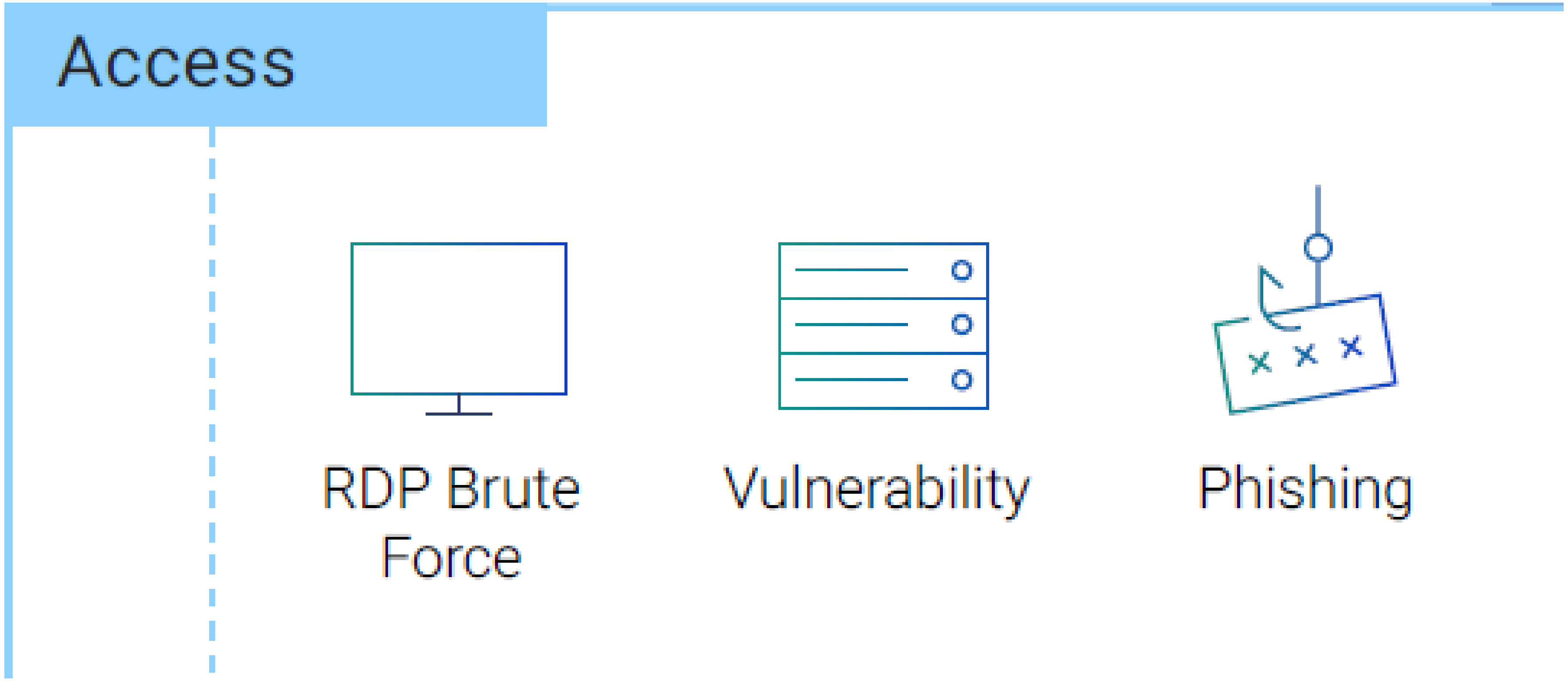
Source: Malwarebytes: 2024 State of Malware Report

Source: https://www.strongdm.com/

ThreatDown™
Powered by Malwarebytes

How is this happening?

Cyber Criminals are going after the easy targets


Access

RDP Brute Force

Vulnerability

Phishing

Source: Malwarebytes: 2024 State of Malware Report

Advanced Threats

- AV, EP cannot detect fileless attacks. The most effective way to detect fileless malware is to investigate suspicious activity. While the EDR system can flag suspicious behavior, up to 80% of EDR alerts are ignored.

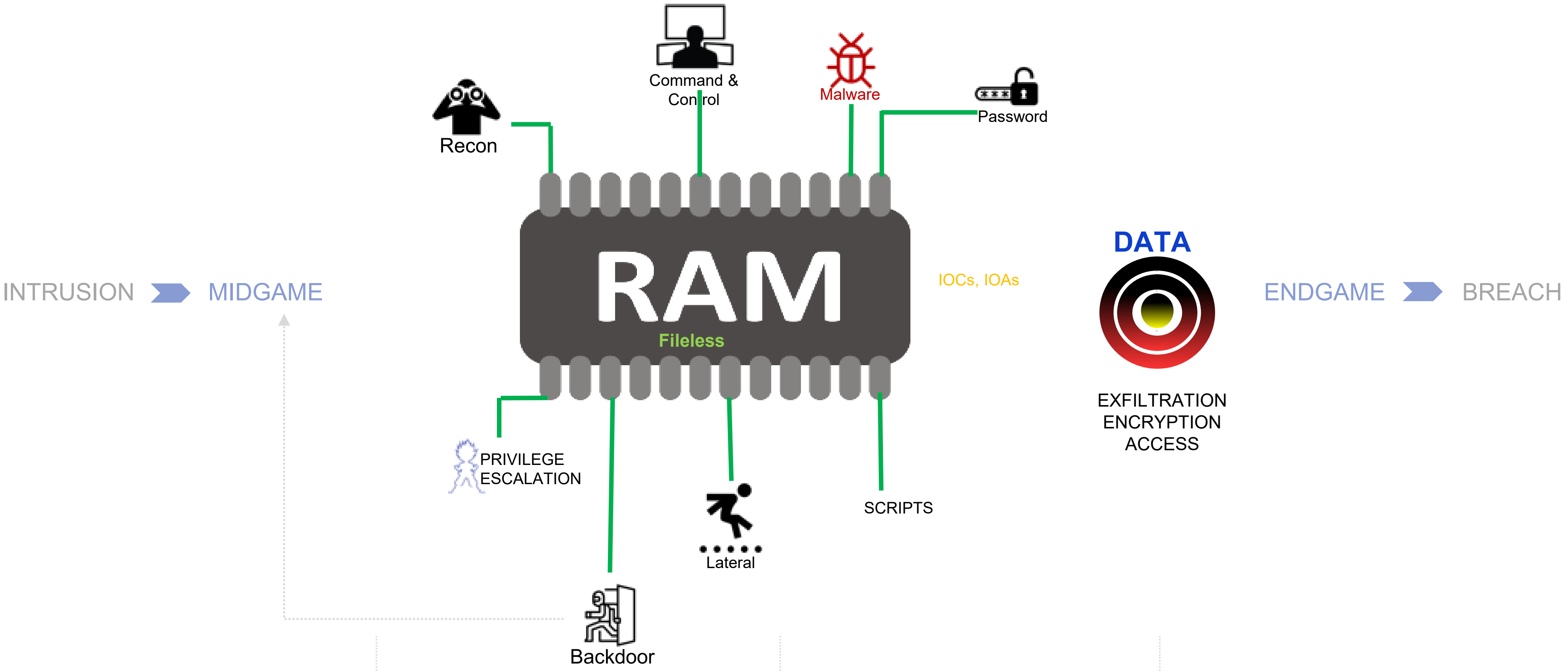
- 60
  - Percent data breaches from known vulnerabilities
- 62
  - Percent attacks that use fileless malware
- 80
  - Percent daily EDR alerts that are ignored
- 485
  - Percent increase in ransomware attack

ThreatDown™
Powered by Malwarebytes

[1]ServiceNow- Ponemon 2019 Vulnerability Survey
[2]CrowdStrike 2022 Global Threat Report
[3]Internal MWB customer survey
[4]2020 Consumer Threat Landscape Report (Bitdefender

Threat Actor Playbook

The midgame is evolving in sophistication and evasion: over 245 attacker techniques (Mitre)



INTRUSION ➤ MIDGAME

Recon

Command & Control

Malware

Password

RAM

Fileless

IOCs, IOAs

PRIVILEGE ESCALATION

Lateral

SCRIPTS

Backdoor

DATA

EXFILTRATION
ENCRYPTION
ACCESS

ENDGAME ➤ BREACH

PREVENT
- BLOCK
- ANTI-EXPLOIT
- PATCH

DETECT
- MITRE
- SCAN
- BEHAVIOR
- ALERTS
- IOCs

RESPOND
- QUARANTINE
- ISOLATION
- ERADICATE
- REVOKE
- SANDBOX

RECOVER
- ROLLBACK
- RESTORE
- REIMAGE
- CLEAN

Malvertising

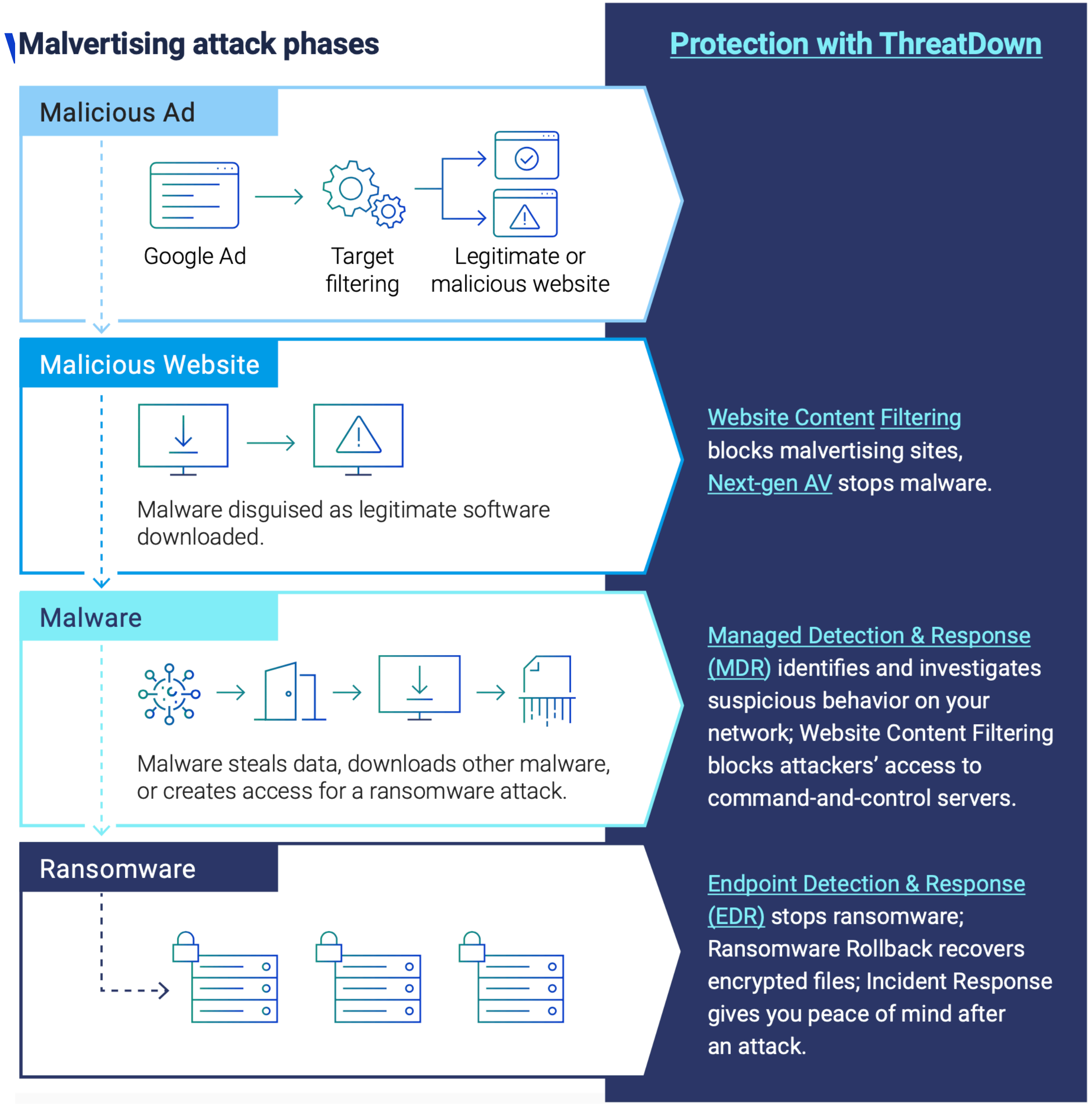
Using malicious ads to spread mal

What you need to know:

- Newly-popular malware distribution channel that saw a huge increase in 2023

Why should you care?

- This is a hard-to-detect way of distributing malware
- The bundle protects against malvertising and its consequences



Malvertising attack phases

Protection with ThreatDown

Malicious Ad

Malicious Website

Malware disguised as legitimate software downloaded.

Website Content Filtering blocks malvertising sites, Next-gen AV stops malware.

Malware

Malware steals data, downloads other malware, or creates access for a ransomware attack.

Managed Detection & Response (MDR) identifies and investigates suspicious behavior on your network; Website Content Filtering blocks attackers' access to command-and-control servers.

Ransomware

Endpoint Detection & Response (EDR) stops ransomware; Ransomware Rollback recovers encrypted files; Incident Response gives you peace of mind after an attack.

ThreatDown™
Powered by Malwarebytes

Living off the Land

Using an organization’s own tools to work undetected

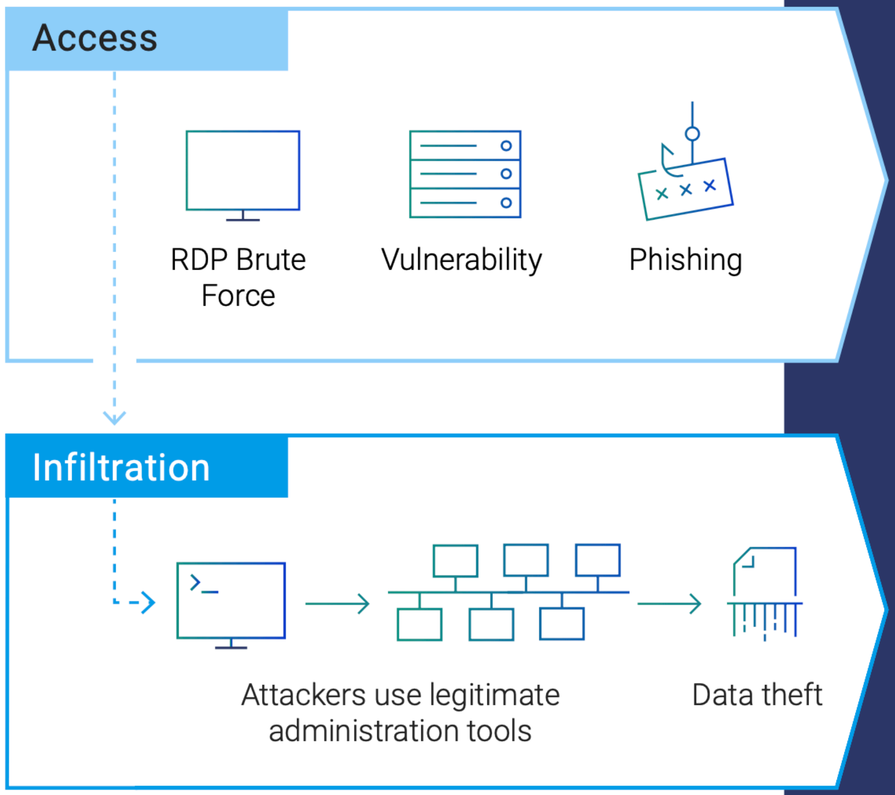
What you need to know:

- Difficult to detect, does not rely on malware

Why should you care?

- Prevention is better than cure
- Why customers need Application Block
- Why customers need humans in the loop

Living Off The Land attack phases



Protection with ThreatDown

Brute Force Protection, Vulnerability Assessment, Patch Management, Anti-Exploit Protection and Website Content Filtering stop different forms of access.

Managed Detection & Response (MDR) identifies and investigates suspicious behavior on your network; App Block denies attackers access to their tools; Website Content Filtering blocks attackers’ access to command-and-control servers.

ThreatDown™
Powered by Malwarebytes

Zero-day ransomware

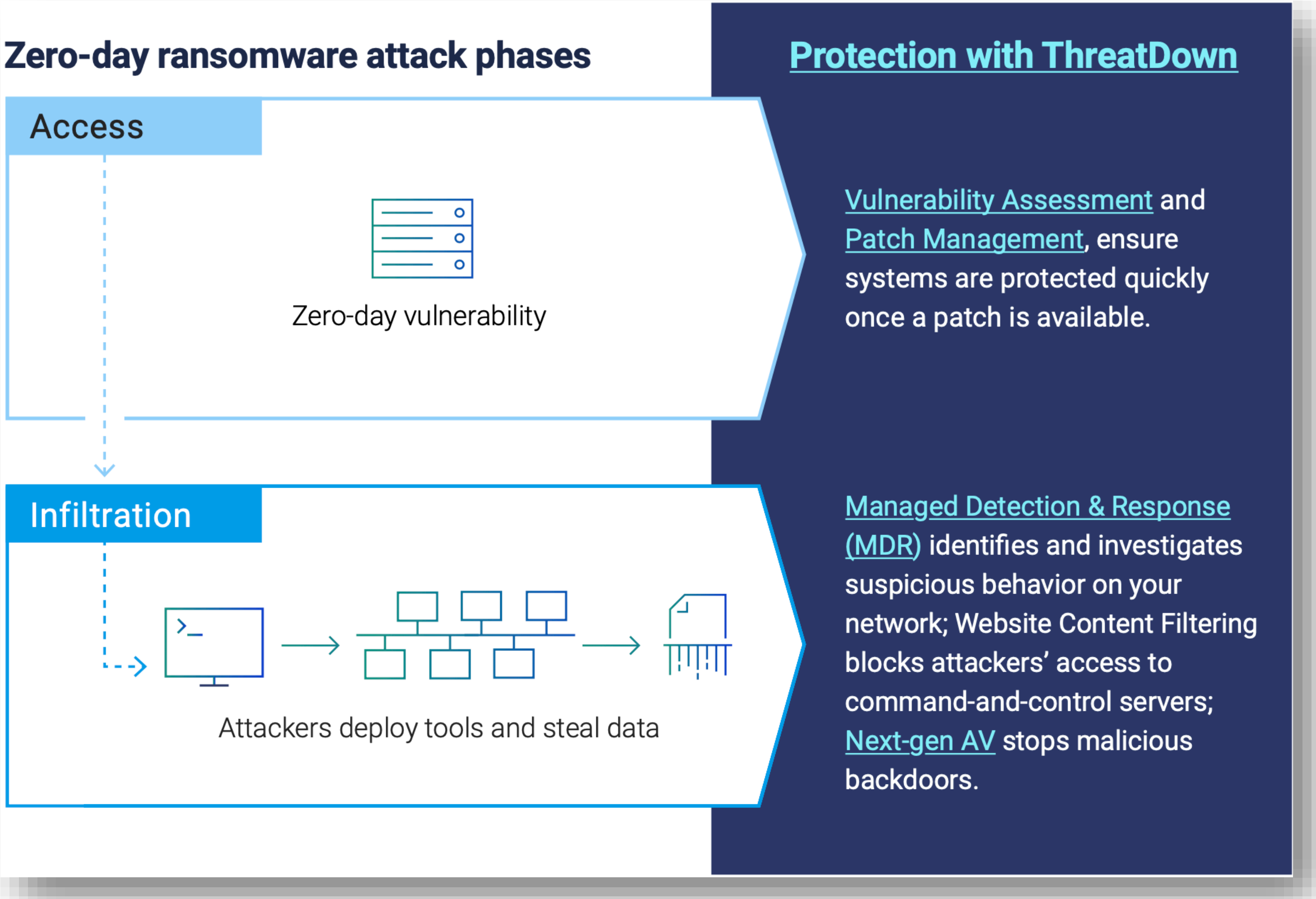
Using zero-day exploits to spread ransomware in automated campaigns

What you need to know:

- New tactic that allows ransomware to expand

Why should you care?

- Shows the sophistication of cybercriminals
- Why customers need humans in the loop



Zero-day ransomware attack phases

Access

Zero-day vulnerability

Infiltration

Attackers deploy tools and steal data

Protection with ThreatDown

Vulnerability Assessment and Patch Management, ensure systems are protected quickly once a patch is available.

Managed Detection & Response (MDR) identifies and investigates suspicious behavior on your network; Website Content Filtering blocks attackers' access to command-and-control servers; Next-gen AV stops malicious backdoors.

ThreatDown™ Powered by Malwarebytes

The Problem: EP is not enough

- 50% of MSPs surveyed report that ransomware attacks averted anti-virus and anti-malware solutions*

- 59
- Percent attacks where anti-malware filtering (email, network and web-based) was evaded

- 42
- Percent attacks where legacy signature-based antivirus was evaded

- 24
- Percent attacks where EDR software was evaded

- 12
- Percent attacks where NextGen antivirus was evaded

Datto survey of more than 1,000 MSPs

ThreatDown™
Powered by Malwarebytes

EDR PLATFORM

Monitor endpoints to identify potential threats

Indicate criticality of threats to help prioritize team response actions

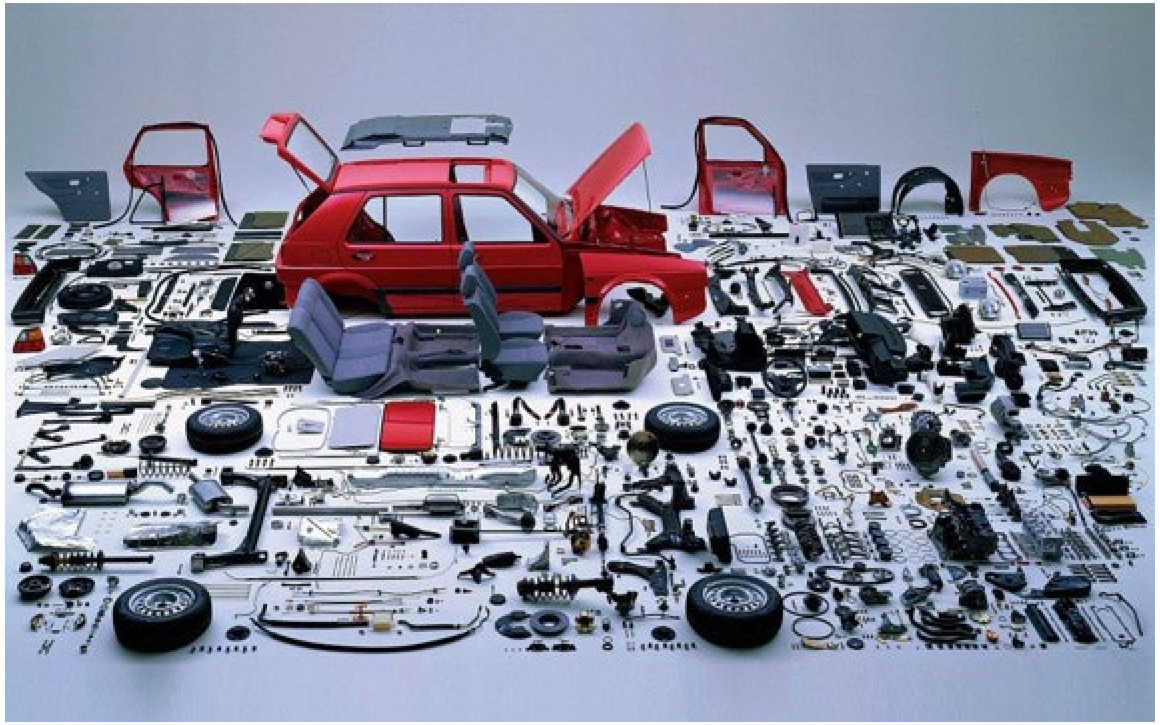
Provide forensics and analysis tools to hunt unseen threats

ThreatDown™
Powered by Malwarebytes

Security Challenge

- EDR Promise

Market EDR Solution



Reality of EDR Without Skilled Team

ThreatDown™
Powered by Malwarebytes

KEY FEATURES OF ThreatDown MDR

- 24x7x365 coverage
- Threat hunting
- Tiered notifications
- Rapid set-up
- Skilled MDR Analysts
- Flexible remediation options
- AI-based threat modeling
- Two-way communication

ThreatDown™

Powered by Malwarebytes

Prevent

- BFP
- DNS Protection
- APP Block
- VPM

Block

- Web Protection
- Exploitation Mitigation
- Device Control
- Payload Analysis
- ML and Behaviour Analysis

Recover Fast

- EDR
- MDR
- MTH

ThreatDown™
Powered by Malwarebytes

ctosi@malwarebytes.com