EXTRAHOP

EDR EVASION 101

29 Ways Attackers are Slipping Past Endpoint Defenses

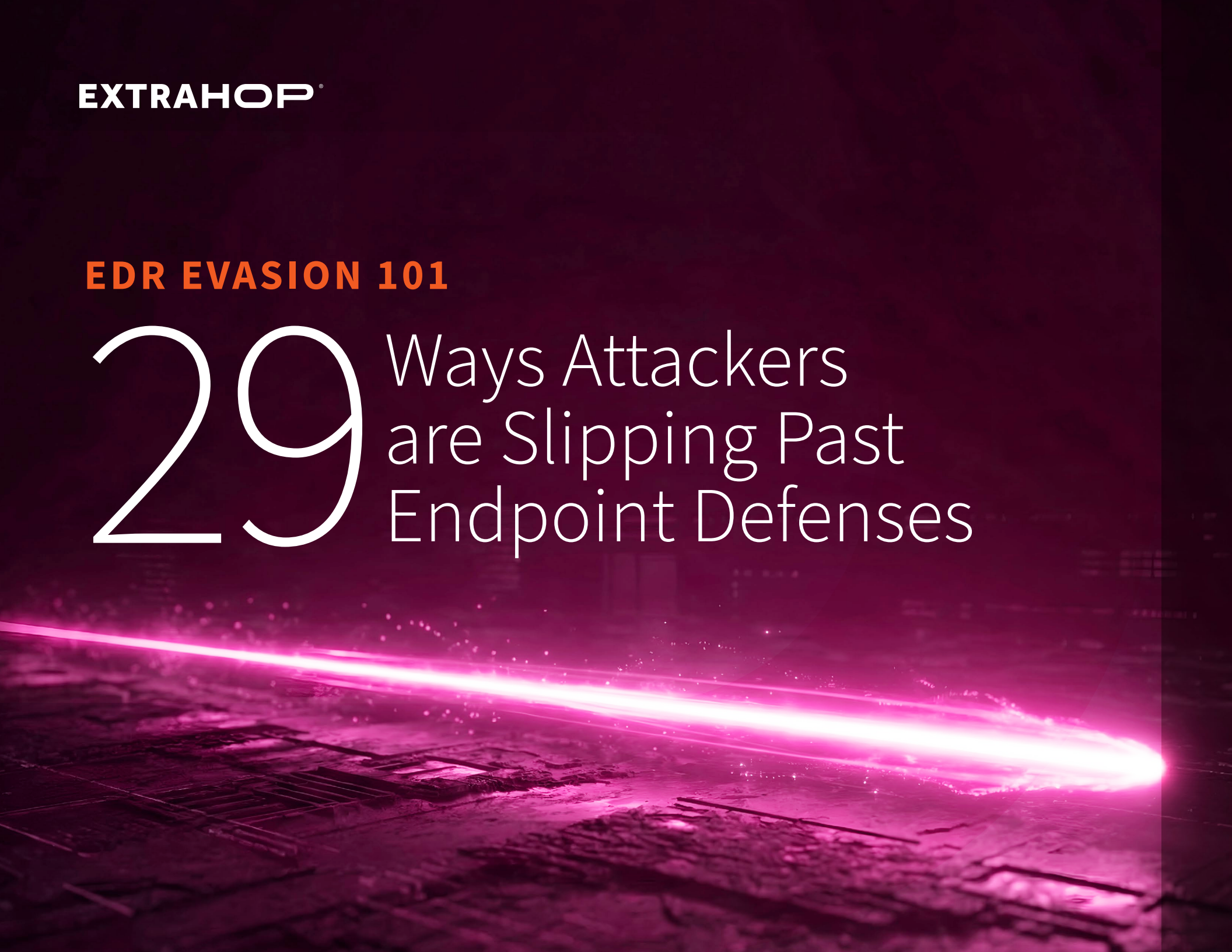


Table of Contents

The Changing Role of EDR in Modern Security 3

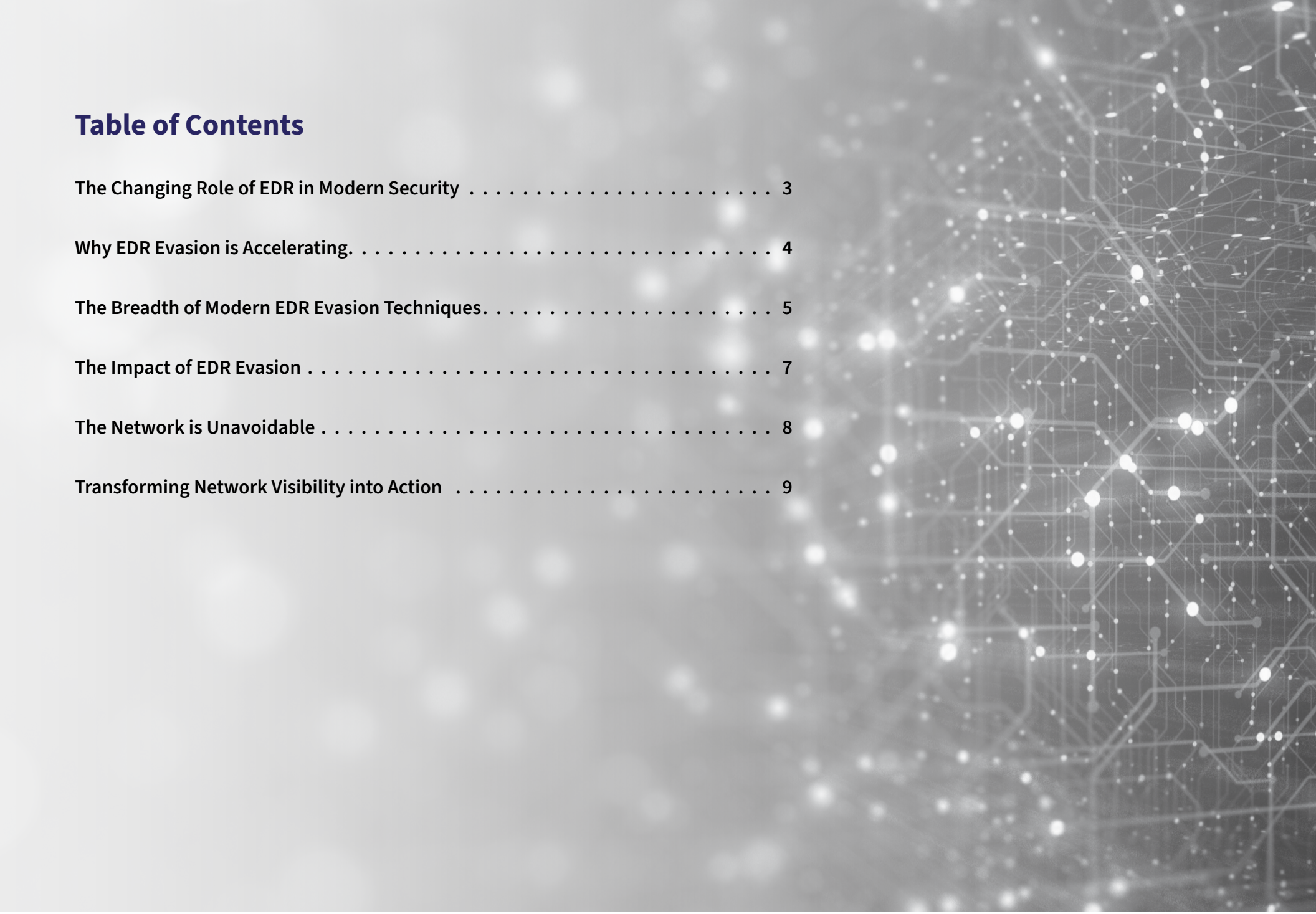
Why EDR Evasion is Accelerating. 4

The Breadth of Modern EDR Evasion Techniques. 5

The Impact of EDR Evasion 7

The Network is Unavoidable 8

Transforming Network Visibility into Action 9



THE CHANGING ROLE OF EDR IN MODERN SECURITY

EDR is often considered the frontline defense, monitoring endpoints for suspicious activity. However, attackers are adapting their tactics to anticipate, evade, and bypass these protections.

When successful, attackers gain the freedom to operate under the radar, generating few, if any, observable events for endpoint defenses to act on. As a result, EDR alone is no longer enough to secure modern environments.

WHY EDR EVASION IS ACCELERATING

EDR evasion was once an extremely specialized skill, but it's becoming more widely accessible via automated tools and services. Today, even low-skill attackers can leverage bypass techniques to avoid advanced defenses using open-source red teaming tools, AI-assisted malware obfuscation techniques, and other "publicly" available exploits.

What once required expert knowledge now requires only a GitHub account, basic technical literacy, and the use of widely available LLM models. In turn, attackers are able to increase the volume and speed of breaches. Consider the volume and magnitude of what threat actor groups like **Scattered Spider** are doing, manipulating help desks and bypassing MFA to gain "authorized" access and evade traditional endpoint controls.

Proof-of-concept exploits like EDR-Freeze bypass security by tricking the operating system into suspending EDR agents, rendering agents blind while they falsely appear active, helping attackers avoid triggering alerts.

THE BREADTH OF MODERN EDR EVASION TECHNIQUES

Attackers no longer rely on a single evasion method. They have a wide range of options to choose from. These techniques span multiple layers of the operating system and execution lifecycle.

Kernel-level control

Manipulates the operating system core to remove, disable, or bypass security monitoring, allowing malware to run undetected.

Examples:

01 **Spyboy "Terminator"**

02 **Crypto 24**

03 **RealBlindingEDR**

04 **Daxin**

In-memory execution

Runs code directly in system memory, avoiding disk-based detection and leaving fewer traces for traditional EDR tools to pick up on.

Examples:

05 **Silver**

06 **KyloRen**

07 **Process Injection (Mapped Sections)**

08 **MSSQL CLR Abuse**

Telemetry suppression

Disables or alters the signal that EDR relies on, effectively "blinding" the EDR agent.

Examples:

09 **AMSI patch kits**

10 **EDR-Freeze**

11 **EDRKillShifter**

12 **EDR-Killer Market**

THE BREADTH OF MODERN EDR EVASION TECHNIQUES

File system & policy manipulation

Uses operating system features to hide or block security controls, allowing attackers to persist and evade remediation.

Examples:

13 NTFS Junctions

14 PendingFileRename

15 Weaponizing WDAC

16 EDR-Redir V2

17 AnonKiller V2

C2 & evasion frameworks

Manages command-and-control operations while bypassing detection hooks.

Examples:

18 Brute Ratel

19 Cobalt Strike

20 Havoc C2

21 Bulwark Packer

22 BestEDROfTheMarket Lab

Non-Windows/IoT pivots

Exploits Linux, IoT, or unmanaged devices to move laterally or access environments that EDR cannot monitor.

Examples:

23 RingReaper

24 Agenda/Qilin Linux Pivot

25 Akira IoT Pivot

Fileless propagation

Executes malicious code entirely through native system tools and scripting environments without ever writing a payload to disk, leaving traditional file-scanning defenses with nothing to detect.

Examples:

26 PowerShell Empire

27 SliverC2 (PowerShell Stager)

28 Invoke-Obfuscation

29 WMImplant

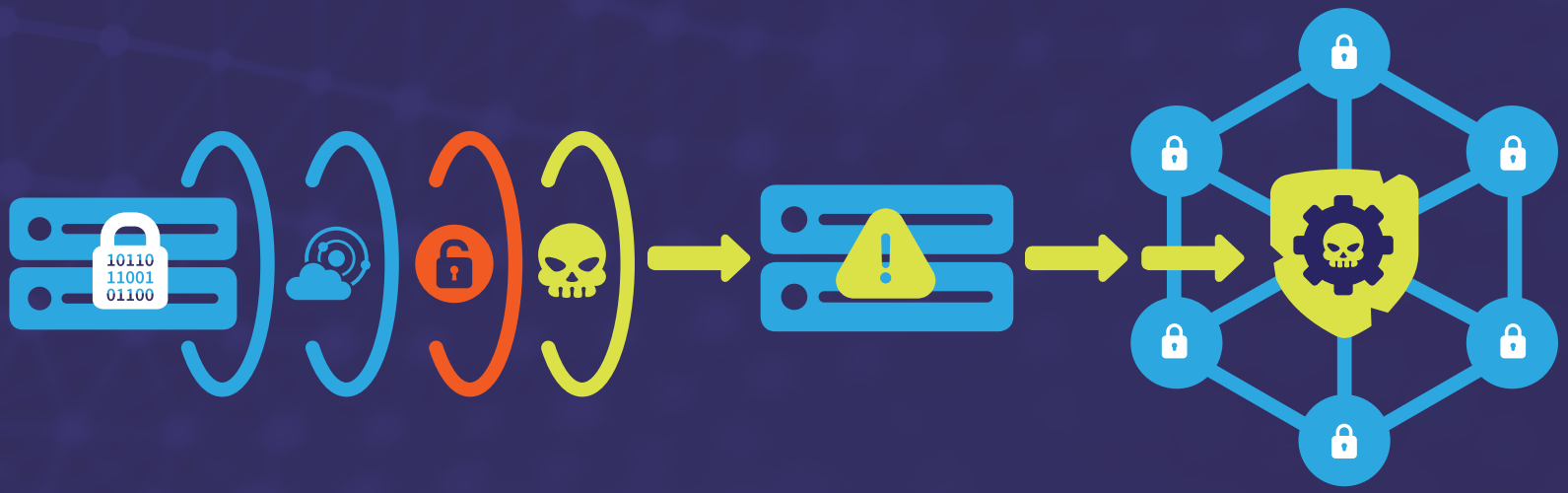
THE IMPACT OF EDR EVASION

Evasion extends **dwell time**, giving attackers freedom to map networks, harvest credentials, and exfiltrate sensitive data. Presently, attackers maintain access for **an average of two weeks** before deploying ransomware.

In some sectors, like education and government, that window extends for an average of 5-7 weeks. During this time, attackers escalate privileges and prepare for attacks, increasing potential impact.

Extended dwell time often causes disruption, with organizations experiencing an average of 37 hours of downtime following a cybersecurity incident.

After bypassing Change Healthcare's endpoint defenses with stolen credentials, ALPHV/BlackCat was in the company's corporate network for nine days, enabling the exfiltration of 6TB of data and a $22 million ransom.



THE NETWORK IS UNAVOIDABLE

Regardless of whether EDR detects a threat or whether EDR is evaded entirely, network activity remains a constant and reliable source of truth.

The network provides immutable evidence. The network cannot be deleted or altered by attackers, creating a permanent record of all activity — even when EDR agents are blind.

The network also picks up behavioral anomalies. Protocol-aware analysis reveals lateral movement, credential misuse, and exfiltration, while telemetry of encrypted traffic exposes hidden command-and-control activity.

This network-centric perspective enables faster detection, more accurate investigation, and earlier response, before attackers can escalate or exfiltrate sensitive data.

TRANSFORMING NETWORK VISIBILITY INTO ACTION

To stay ahead of evasive threats, organizations must look beyond the endpoint. Detection strategies should combine network-level telemetry and behavioral analysis to identify threats before they escalate, accounting for attacker speed and stealth.

Learn how ExtraHop uncovers evasive threats with network detection and response (NDR).

ABOUT EXTRAHOP

ExtraHop turns the network — the enterprise's ultimate source of truth — into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that "thinks," analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit **extrahop.com** or follow us on **LinkedIn**.

EXTRAHOP®