EXTRAHOP®

Expand Network Visibility and Security with Modern IDS

Introduction

As the modern threat landscape continues to evolve, security tools must adapt to stay ahead of emerging threats. Simple firewalls, antivirus software, and legacy IDS (Intrusion Detection Systems) are no longer sufficient to defend organizations against attacks.

As attention has shifted from perimeter defense toward zero trust models, tools to detect suspicious activity within the network have risen to the forefront. Tools such as modern IDS combined with an NDR (Network Detection and Response) solution are needed to gain network visibility.

Since its inception, IDS has had an essential place in security programs and even in compliance mandates. However, legacy IDS solutions no longer deliver the visibility needed to address modern threats. Instead, a modern IDS that complements and integrates seamlessly with other security tools is required. By integrating with NDR, modern IDS can provide additional context and visibility to detect east-west threats and stop intruders post-compromise. Together these solutions can close compliance gaps introduced by cloud initiatives and eliminate blind spots created by encryption.

> “According to the 2023 Verizon Data Breach Investigations Report, external actors were responsible for 83% of breaches.”[1]

[1] “Data Breach Investigations Report,” Verizon, 2023.

A Brief History of IDS

The Emergence of IDS

Building from the ideas of an academic paper entitled, “An Intrusion-Detection Model,” published in 1987, IDS gained popularity in the 1990s and even greater traction in the 2000s. Early systems such as the IDES built by SRI International combined rule-based detection leveraging known vulnerabilities with statistical anomaly detection to identify suspicious behavior. These systems were designed to secure the network perimeter from attacks such as port scanning, SQL injections, and buffer overflows.[2]

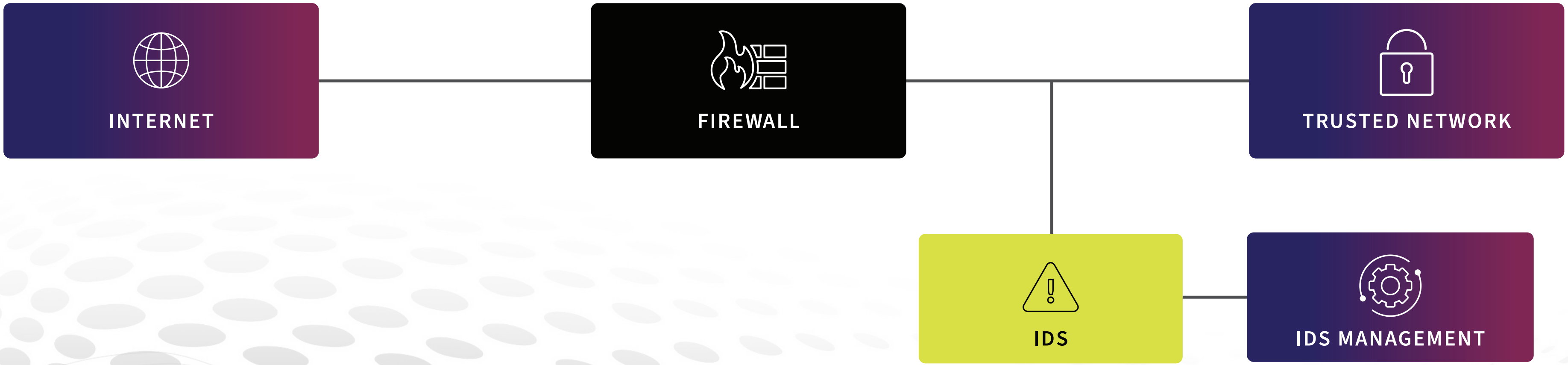
The Role of IDS in Compliance

IDS was quickly hailed as a significant addition to previous technologies and was adopted and promoted by various security frameworks and compliance standards, including the SANS Top 20 (now the CIS Controls), PCI DSS (which mandated use of IDS by covered organizations), and NIST (which included guidance in publication 800-31 as early as 2001, and updated guidance in publication 800-94). IDS now has a long-standing place in security compliance.

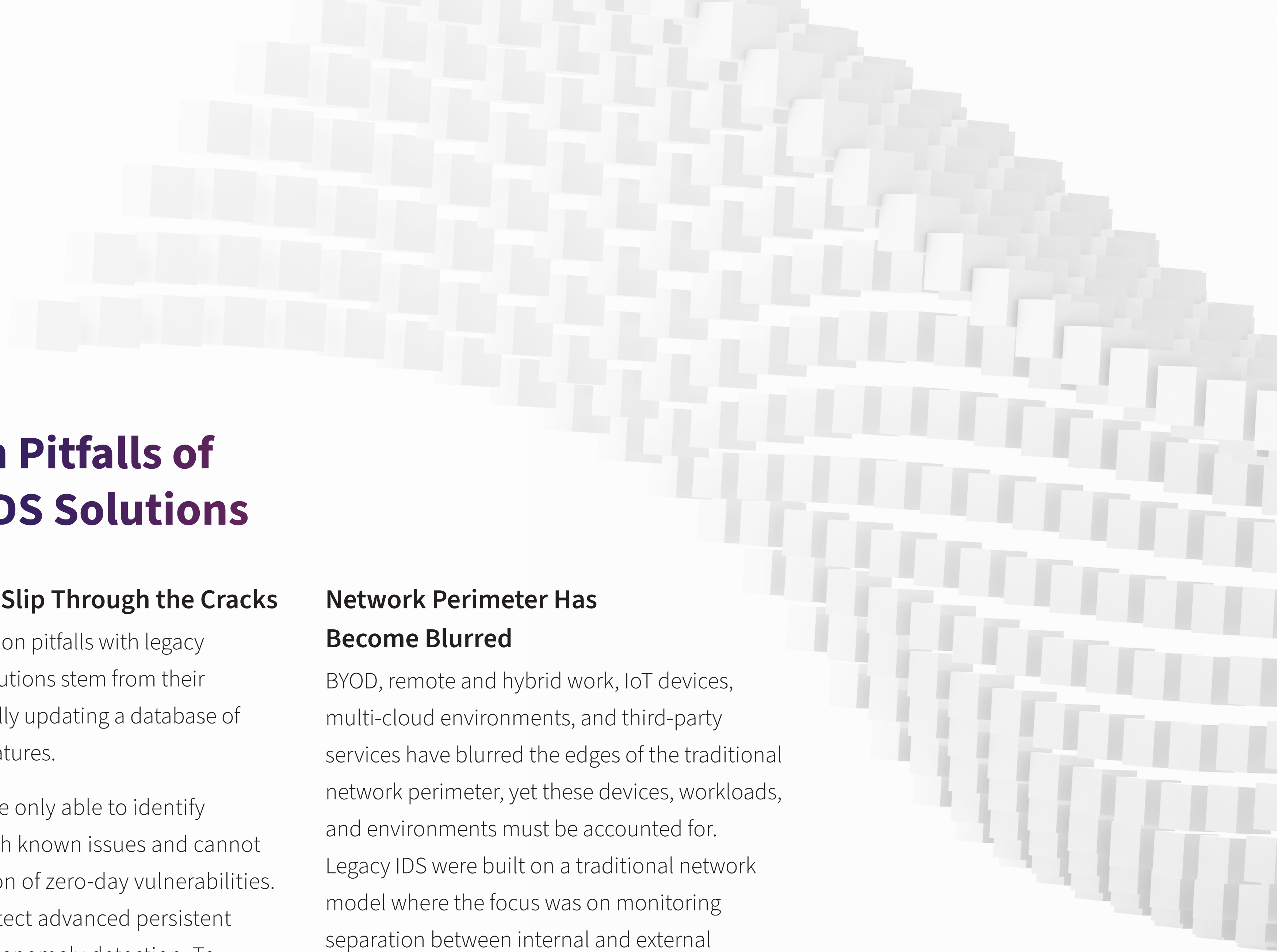
The Functionality of IDS

IDS, at its core, relies on a database of known attack methods and vulnerabilities–and the signatures and patterns of these attacks. IDS technologies use rule- or signature-based packet evaluation–attempting to match packets against known malicious patterns.

The primary focus of these solutions is on reactive alert generation for perimeter defense, enabling action to remediate potential issues. Typically, the alerts must be prioritized, investigated, and remediated by the SOC team.



[2] Gilham, Fred, Jr. et al., “A Real-time Intrusion Detection Expert System (IDES),” SRI International, Feb. 8, 1992.



Common Pitfalls of Legacy IDS Solutions

Zero-Day Risks Slip Through the Cracks

Some of the common pitfalls with legacy standalone IDS solutions stem from their reliance on manually updating a database of known attack signatures.

These solutions are only able to identify patterns that match known issues and cannot prevent exploitation of zero-day vulnerabilities. They also can't detect advanced persistent threats that evade anomaly detection. To address zero-day threats, IDS should be fully integrated with NDR.

Network Perimeter Has Become Blurred

BYOD, remote and hybrid work, IoT devices, multi-cloud environments, and third-party services have blurred the edges of the traditional network perimeter, yet these devices, workloads, and environments must be accounted for. Legacy IDS were built on a traditional network model where the focus was on monitoring separation between internal and external networks. However, in today's fluid virtual networking model, there is no longer a clear distinction between internal and external.

Encrypted Traffic Creates Blind Spots

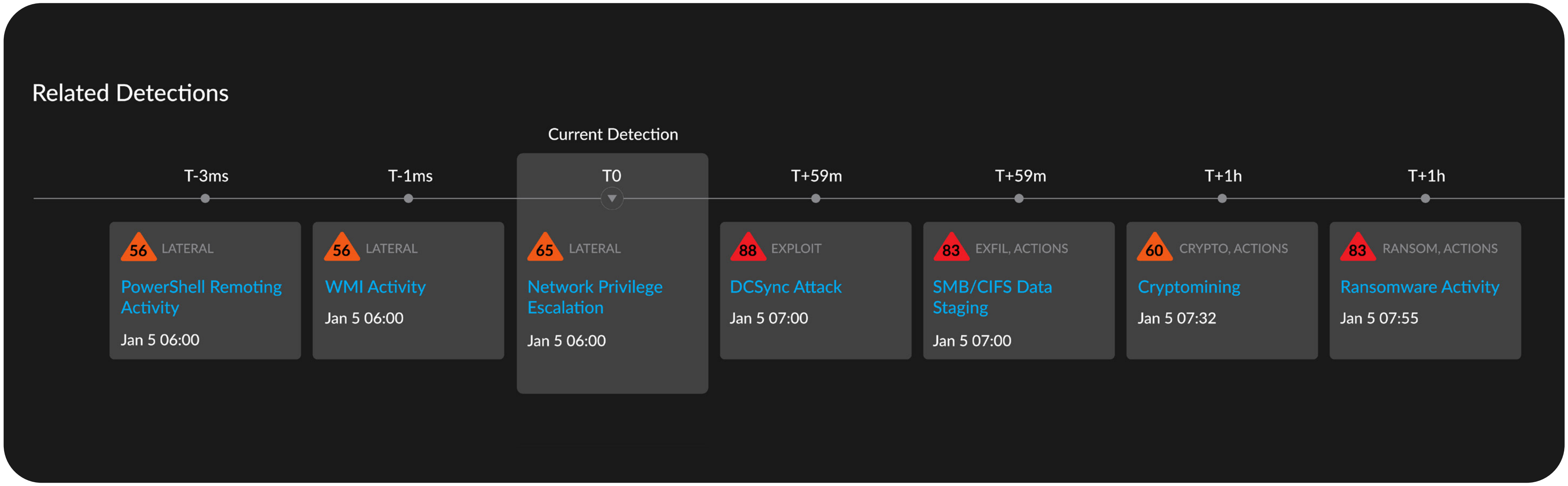
Legacy IDS solutions can only evaluate traffic it can monitor. The rise of encrypted traffic in recent years has created significant blind spots for legacy IDS solutions. In fact, it has been reported that more than 85% of attacks now use encrypted channels to attempt to evade detection.[3]

Narrow Focus Provides Limited Visibility

Legacy IDS primarily focuses on north-south traffic and detecting threats at the perimeter. Internal network traffic escapes detection so these solutions fail to detect lateral movement within the network. This can leave a huge visibility gap once an attacker has made an initial entry undetected and turns their focus to reaching additional targets.

False Alerts Create Fatigue

Logs or notifications are triggered by traffic deemed suspicious, but legacy IDS solutions often generate many false positive alerts if not properly tuned. Proper tuning requires a great deal of time and knowledge of network systems and devices, and usually requires ongoing effort to maintain. Standalone IDS solutions lack the context and integrated investigation workflows needed to take action on these alerts, leaving organizations vulnerable to attackers.



Related Detections

Current Detection

T-3ms	T-1ms	T0	T+59m	T+59m	T+1h	T+1h
56 LATERAL	56 LATERAL	65 LATERAL	88 EXPLOIT	83 EXFIL, ACTIONS	60 CRYPTO, ACTIONS	83 RANSOM, ACTIONS
PowerShell Remoting Activity	WMI Activity	Network Privilege Escalation	DCSync Attack	SMB/CIFS Data Staging	Cryptomining	Ransomware Activity
Jan 5 06:00	Jan 5 06:00	Jan 5 06:00	Jan 5 07:00	Jan 5 07:00	Jan 5 07:32	Jan 5 07:55

[3] "State of Encrypted Attacks 2022," Zscaler, 2022.

Modern IDS

Hallmarks of Modern IDS Solutions

- Modern solutions allow cloud-based deployment and automated cloud-based rule updates to stay up to date.
- Seamless coverage across cloud and on-premises environments ensures all areas of a modern network are monitored.
- Automated workflows and integration with other security products, including NDR provide deeper insight and speed response.
- Efficient integrations for faster detections of malware.

The Benefits of Modern IDS

- Detect an attacker's movement early in the kill chain before they do significant damage.
- Close compliance gaps caused by blind spots without weakening encryption.
- Account for cloud initiatives without impeding the business.
- Utilize flexible deployment models, including virtual and physical sensors based on an organization's needs.
- Gain visibility into security hygiene to reduce potential attack surfaces.
- Understand what happened leading up to and after an event, including the relationship between the breached host and other systems.

Critical Capability	ExtraHop IDS	Legacy IDS
Critical CVE exploit detection	✓	✓
Protocol abuse	✓	✓
Static threshold rules	✓	✓
Application ID	✓	✓
File detection	✓	✓
Custom rule import	✓	✓
Decryption	✓	x
Insider threat detection	✓	x
East-west visibility	✓	x
Cloud enabled	✓	x
Full spectrum investigation	✓	x
Virtual sensors	✓	x

Pairing Modern IDS with NDR for a Winning Combination

While EDR and SIEM have played significant roles in improving SOC visibility, these solutions alone leave significant gaps:

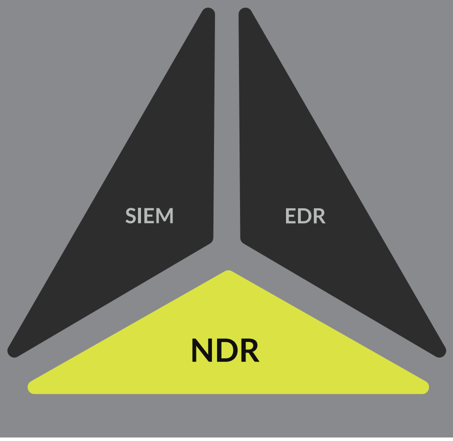
- SIEM reliance on log data limits visibility into east-west attacks and produces frequent false positives, which creates investigation work for the SOC and compounds alert fatigue.
- Attackers routinely turn off or modify logs to cover their tracks.
- EDR relies on agents, which organizations may not be able to deploy on every endpoint and which attackers find ways to disable or evade.

NDR combined with modern IDS provides high-fidelity detections, real-time visibility, and can improve SOC efficiency:

- Machine learning provides the foundation for behavioral, anomaly, peer group, and rules-based pattern detections.
- Monitoring network traffic enables organizations to detect sophisticated attacks such as advanced persistent threats and threats that evade logs.
- Integrated risk scoring, smart triage, correlation, and investigative workflows can improve response time and help prioritize the most pressing issues.

When added to EDR and SIEM, NDR with integrated modern IDS can strengthen organizations' security posture and provide the SOC comprehensive visibility. Together, these technologies build on each other's strengths and mitigate the weaknesses of isolated solutions. For example:

- NDR may catch traffic missed by an EDR where an agent is not available.
- NDR may illuminate end-to-end encrypted network connections the SIEM may not have visibility into.



About ExtraHop IDS

ExtraHop IDS offers critical capabilities to streamline workflows and more effectively stop threats:

- Automated, high-fidelity signature-based detections.
- Rapid CVE detection with tens of thousands of signatures from leading threat rule sets.
- Automated cloud updates to sensors within minutes of rules being published.
- Integrated security technologies to reduce overhead, simplify management, and improve response time.

By combining ExtraHop RevealX™ with ExtraHop IDS, customers looking to retire legacy IDS systems will be able to make the leap to modern NDR defense capabilities without weakening their compliance posture or losing the capabilities IDS has provided over the years.

RevealX NDR Workflow Powered with IDS

Securiuty Hygiene	Detection	Incident Response	Forensics
Passive Asset Inventory Discover Weak and Expired Cypher	Known Threats Unknown Threats	30, 90, 180, or 365 Days of Traffic Lookback Correlated Attacker Timeline Threat Briefings	Continuous PCAP Evidence Repository

Legacy IDS

Securiuty Hygiene	Detection	Incident Response	Forensics
✗	Known Threats	✗	✗

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at **extrahop.com**.

EXTRAHOP®