SONICWALL®

Beyond EDR: How MSPs Win with 24/7 MDR Coverage

Let's Start

CONTENTS

1 Introduction

2 Why EDR Alone Isn't Enough

3 The 3 a.m. Threat Window

4 Identity: The Source of 83% of Security Alerts

5 Addressing Alert Overload

6 Build, Buy, or Partner: Choosing Your SOC Path

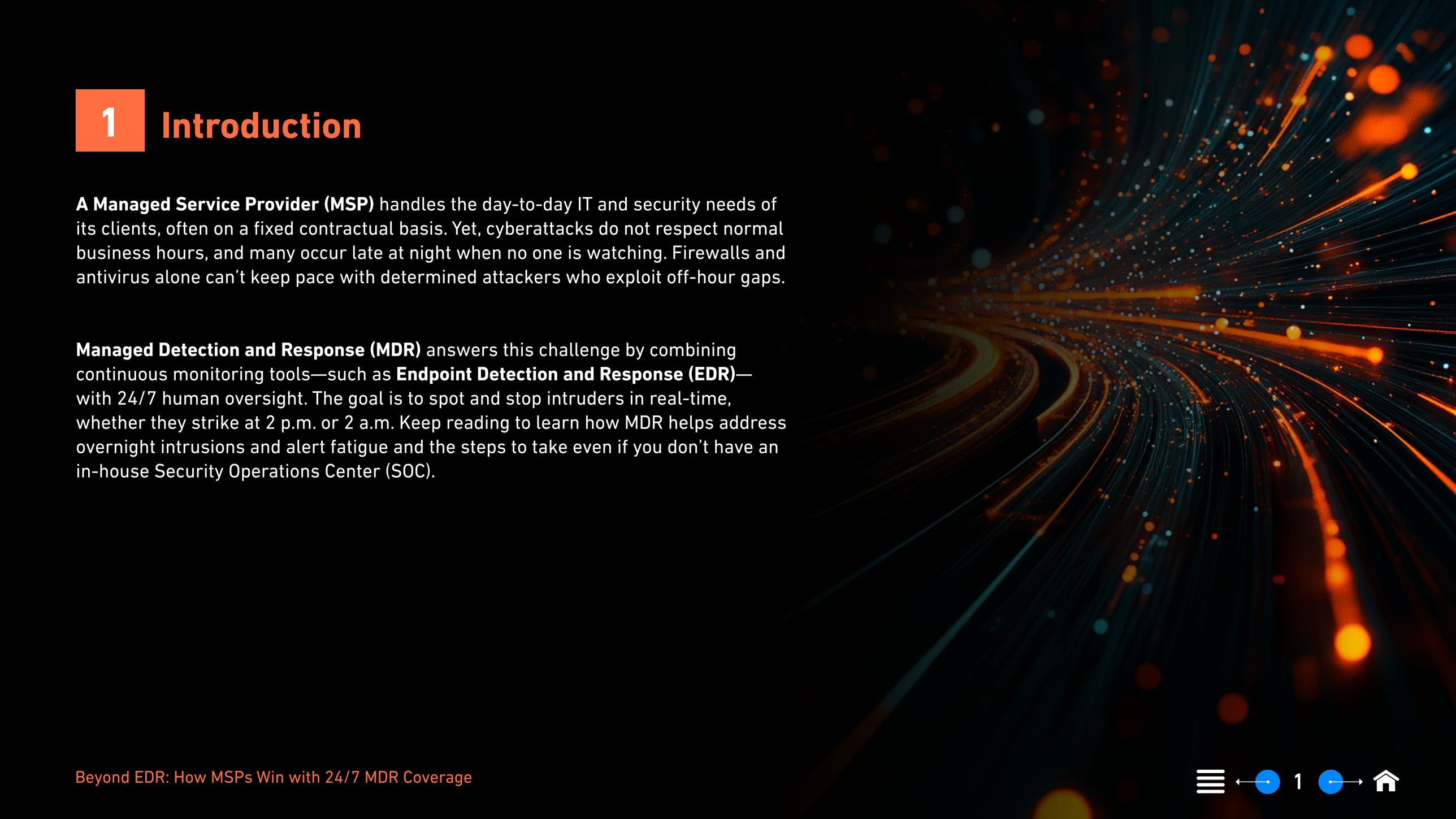
7 How to Launch MDR in Your Organization

8 Wrapping Up

1 Introduction

A Managed Service Provider (MSP) handles the day-to-day IT and security needs of its clients, often on a fixed contractual basis. Yet, cyberattacks do not respect normal business hours, and many occur late at night when no one is watching. Firewalls and antivirus alone can't keep pace with determined attackers who exploit off-hour gaps.

Managed Detection and Response (MDR) answers this challenge by combining continuous monitoring tools—such as **Endpoint Detection and Response (EDR)**—with 24/7 human oversight. The goal is to spot and stop intruders in real-time, whether they strike at 2 p.m. or 2 a.m. Keep reading to learn how MDR helps address overnight intrusions and alert fatigue and the steps to take even if you don't have an in-house Security Operations Center (SOC).



2 Why EDR Alone Isn't Enough

EDR in Brief

Endpoint Detection and Response (EDR) tools look for malicious or suspicious behaviors on endpoints (servers, laptops, workstations).
They often block or quarantine threats automatically, relying on up-to-date threat intelligence and behavioral analysis.

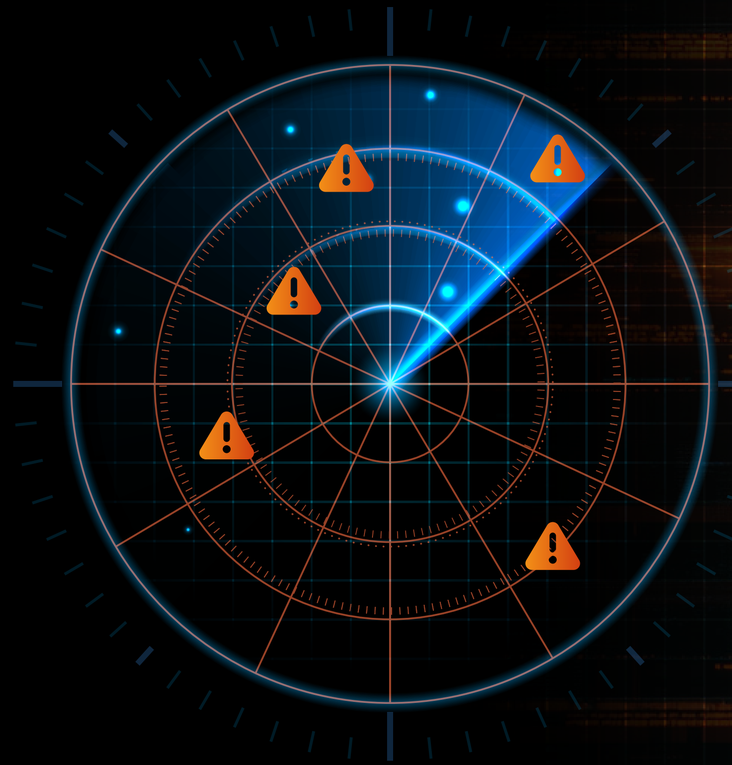
The Gap: Response

Even a top-tier EDR can't guarantee someone is there to investigate and contain an incident the moment it's detected. A real threat might go unaddressed for hours if your technicians are offline or overwhelmed.

MDR closes this gap by providing:

- ✓ Around-the-Clock Specialists: Trained analysts verify whether an alert is a false alarm or a real intrusion.
- ✓ Rapid Containment: Endpoints and user accounts can be isolated immediately if an attack is confirmed.

EDR sees an alert; MDR ensures it's acted upon immediately – even at odd hours or on weekends.



3 The 3 a.m. Threat Window

Late-Night Intrusions

Like multiple studies indicate, our SOC has found that many attacks begin between **3 a.m. and 6 a.m.** Attackers know it's the least monitored time. If your staff only sees an alert at 8 or 9 a.m., those extra hours can give hackers ample time to:

- Escalate privileges
- Move laterally to other systems
- Deploy ransomware or exfiltrate data

The "Volunteer Firefighter" Dilemma

Some MSPs have tried to handle 24/7 monitoring internally with minimal staff or on-call arrangements. It's comparable to a volunteer firefighter model—someone might wake up at any hour if their phone beeps. Realistically, that can't scale as you add more clients. Sooner or later, an alert will be missed, or staff will burn out.

Why MDR Helps:

- **Nonstop Oversight:** Dedicated teams watch alerts at all hours.
- **Reduced Dwell Time:** Immediate review and response shrink the window attackers have to roam your clients' networks.

4 Identity: The Source of 83% of Security Alerts

Why Identity Is Critical

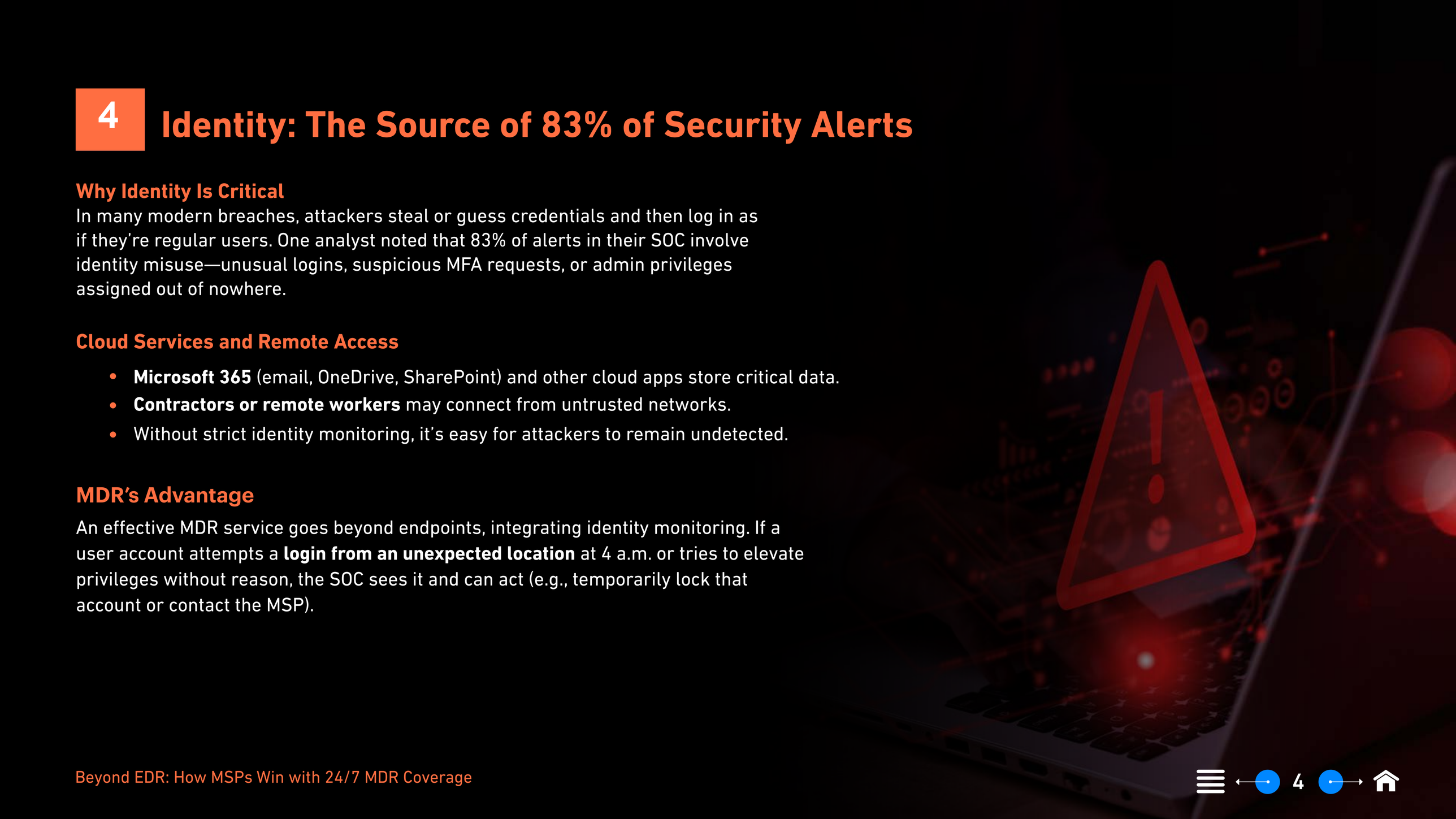
In many modern breaches, attackers steal or guess credentials and then log in as if they're regular users. One analyst noted that 83% of alerts in their SOC involve identity misuse—unusual logins, suspicious MFA requests, or admin privileges assigned out of nowhere.

Cloud Services and Remote Access

- **Microsoft 365** (email, OneDrive, SharePoint) and other cloud apps store critical data.
- **Contractors or remote workers** may connect from untrusted networks.
- Without strict identity monitoring, it's easy for attackers to remain undetected.

MDR's Advantage

An effective MDR service goes beyond endpoints, integrating identity monitoring. If a user account attempts a **login from an unexpected location** at 4 a.m. or tries to elevate privileges without reason, the SOC sees it and can act (e.g., temporarily lock that account or contact the MSP).



5 Addressing Alert Overload

Too Many Alarms, Too Little Time

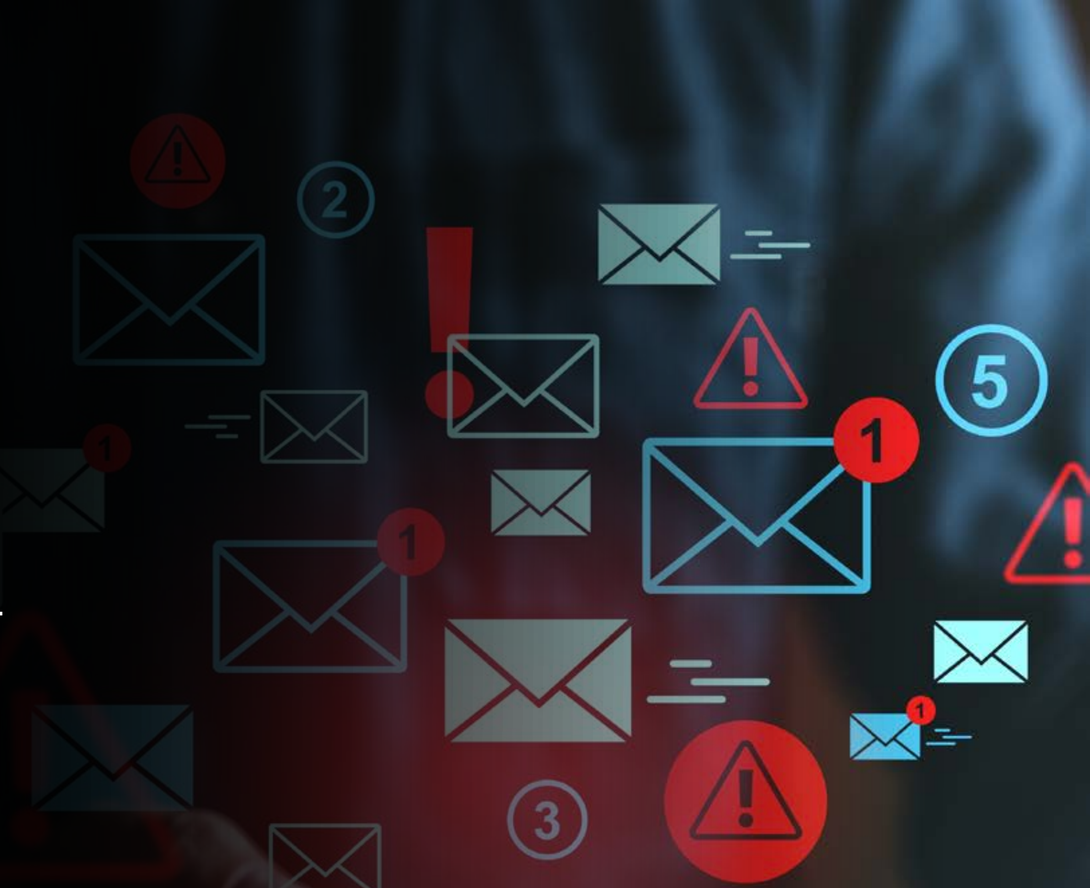
Security tools can produce an overwhelming volume of alerts. False positives—routine system behaviors flagged as suspicious—clutter dashboards and distract your team from serious threats.

Consequences of Overload

- **Missed Real Alerts:** Critical warnings might be buried in a sea of minor notifications.
- **Slow Response:** Manual triage takes time, giving attackers a bigger head start.

MDR's Advantage

- **Expert Triage:** SOC analysts filter out low-priority events.
- **Escalation:** Only genuine incidents require MSP intervention. You're free to handle other tasks until a validated risk emerges.



Result:

Fewer meaningless alerts land on your plate; dwell time for true threats is cut significantly.

6 Build, Buy, or Partner: Choosing Your SOC

Most MSPs agree on the importance of 24/7 monitoring. The question is how to achieve it:

Build Your Own SOC

- Requires hiring or training a round-the-clock team.
- Large financial and time investment.
- Might be suitable for larger MSPs with ample resources.

Buy a SOC (Acquisition)

- Involves acquiring a company that already operates a well-established SOC.
- Demands capital and integration effort.
- Works if you want full ownership right away.

Partner with an MDR Provider

- Typically the most feasible for small to mid-sized MSPs.
- Pay a per-endpoint or per-user fee with minimal upfront costs.
- Gain immediate 24/7 coverage without hiring a large staff.

Fastest Route:

Many MSPs find partnering the quickest and most cost-effective path to offering strong security services.
You keep your focus on delivering IT solutions while the MDR team specializes in continuous threat detection.

7 How to Launch MDR in Your Organization

Implement 24/7 Monitoring

- Many attacks happen between **3 a.m. and 6 a.m.**, when your staff is likely offline.
- Ensure that someone is always on call. This can be an in-house team or an external Security Operations Center (SOC) partner.

Protect Every Endpoint

- Threats can enter through any device—desktops, laptops, or remote user systems—not just your servers.
- Equip all endpoints with Endpoint Detection and Response (EDR), then link them to a 24/7 MDR service for immediate human oversight.

Prioritize Identity and Cloud Security

- About **83% of security alerts** stem from identity misuse (e.g., stolen credentials, abnormal logins).
- Use multi-factor authentication (MFA) and keep an eye on unusual login activity, especially for cloud apps like Microsoft 365 or Google Workspace.

Strengthen Email Defenses

- Phishing remains a top entry point for malware and ransomware.
- Adopt email scanning or API-based solutions that inspect links and attachments. Feed those alerts into your MDR system to catch attacks early.

Define Your Incident Workflow

- If a threat is detected at 3 a.m., who should the SOC call first?
- Clarify immediate actions: Should infected endpoints be isolated? Should staff passwords be reset right away?

Decide on a SOC Approach

- **Build** an in-house SOC if you can hire, train, and equip a 24/7 security team.
- **Buy** (acquire) an existing SOC if you want complete control and have the necessary budget.
- **Partner** with an MDR provider for quicker, more cost-effective coverage without expanding staff.

Recognize the Value of MDR's 24/7 Service

- MDR is not just another tool. It provides continuous monitoring, real-time detection, and immediate intervention—day or night.
- With experts on watch, threats have less time to spread, reducing damage and downtime.

Following these steps helps you reduce false alarms, stop attacks faster, and maintain trust in your security posture—even during off hours when most breaches begin.

8 Wrapping Up

MDR addresses the **blind spots** that basic antivirus or even advanced EDR alone cannot cover. With **real-time monitoring, identity checks, and immediate response**, you reduce the window of opportunity that attackers count on—especially overnight.
For MSPs looking to improve client protection without building a full SOC from scratch, MDR is both cost-effective and practical. It handles:

- **Off-Hours Incidents:** No more waiting until morning to investigate critical alerts.
- **Identity Threats:** The top source of breaches, especially in cloud environments.
- **Alert Fatigue:** Filtering thousands of possible issues down to genuine threats.
- **Client Confidence:** People want proof they're protected 24/7.

By integrating MDR, you give your clients a robust security net while freeing your team to focus on strategic projects. Whether you're planning to build, buy, or simply partner with an established MDR provider, these steps provide a framework to move forward quickly and confidently. Contact us today to learn more about SonicSentry MXDR!

About SonicSentry MXDR

Services: MDR for Endpoint, MDR for Cloud and MDR for Network

Website: SonicSentry MXDR - SonicWall

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®