XDR explained: A strategic approach to threat management

Barracuda

Defense is difficult

Defending business systems is growing more complex every day. There is no longer a clearly defined edge to your network. Business IT infrastructure is constantly evolving and expanding, often without the oversight of IT or security teams. By their very nature, cloud and hybrid systems are flexible and instantly changeable, often by business and not IT teams.

Barracuda

Attacks are easier

The bar for launching attacks has also been lowered. Attackers no longer need to know how to operate hacking tools or a botnet — they can just subscribe to a ransomware-as-a-service platform and simply specify a target. Some of these hacking platforms are even available with zero upfront costs in exchange for a share of ransomware profits extorted from successful attacks.

Attackers don't depend on a single tool or strategy to attack their targets. Typical attacks now come in various forms, testing defenses not only at the perimeter but also throughout and outside of an organization.

Bad actors use automation to constantly browse systems for vulnerabilities. Attacks are increasingly intelligent, multifaceted, targeted, and sophisticated. They use AI to turbocharge phishing and social media attacks to steal the credentials needed to access systems. Organized gangs will not necessarily act immediately once inside a network. They may take their time to observe and plan their next steps. They can wait as they are often well-funded both by the success of previous attacks and, in some cases, by nation-states.

Security skills remain in short supply

There remains a worldwide shortage of trained and skilled cybersecurity professionals. Finding and keeping the right people is expensive and time-consuming for any IT manager or director. And the number of unfilled cybersecurity posts continues to grow.

Research from ISC2 (PDF), the membership association for cybersecurity professionals, found a huge shortfall in cybersecurity professionals around the world. “We estimate the size of the global cybersecurity workforce at 5.5 million — a 9% increase from 2022, and the highest we’ve ever recorded. Conversely, the global workforce gap continues to grow even faster: The gap grew by 13% from 2022, which means that in 2023 there are roughly 4 million cybersecurity professionals needed worldwide. The profession needs to almost double to be at full capacity.”

Alert overload and fatigue

While cybersecurity tools and defenses are also increasingly sophisticated, this brings its own challenges. Whereas once security teams had a handful of defensive systems to maintain and monitor, they are now dealing with multiple sources of information. And that means more alerts to assess and more decisions to make. Teams decide dozens of times a day whether an alert requires immediate action or is a false positive that can be safely ignored. This is exhausting your staff and can lead to errors. It can also exacerbate problems with staff turnover.

This also means more work for security teams and less time for them to think strategically about the business and how to keep it secure. It turns your highly paid staff into responders — they are fighting fires, not thinking ahead.

Barracuda.

What is extended detection and response?

Extended detection and response (XDR) offers a single repository for security data and telemetry as well as an analytic capability to make sense of this data and accelerate threat detection. Specifics of the definition vary slightly according to which analyst house or vendor you ask, but that's it in a nutshell. XDR also provides automated responses to incidents based on previously agreed-upon playbooks and plans.

Another way of thinking about XDR is to see it as an evolution of endpoint detection and response (EDR) — the system that checks in on laptops, desktops, and servers, and gathers security data from them to look for indicators of compromise.

Alongside this, network detection and response systems check and gather logs from network devices and analyze traffic entering, leaving, and traversing the corporate network.

XDR takes security data generated from each of these sources, and potentially others too, and helps security analysts make sense of that data. This allows better insights and helps separate real threats from false alarms.

Barracuda

What are the benefits of XDR?

Because XDR brings all your security instrumentation into one place and automates analysis, detection, and response, it means that detections happen earlier, and your teams can respond faster in the case of a genuine attack.

XDR can save you money and time. ESG Research shows that XDR can do the work of eight full-time staff. In a world where recruiting and retaining security staff is a challenge, this gives your team a boost.

It helps turn the mass of unstructured security data and telemetry into a useful and informative resource.

XDR exploits the fact that attacks are now made on many different fronts — it is no longer just a phishing attack on your finance department. Because attackers are looking across your organization, you need defensive systems that do the same. Well-connected XDR platforms exploit what should be the strength of a multipronged attack and turn it into a weakness. By spotting anomalies across systems, they can react more quickly and contain attacks faster.

Barracuda

What does XDR actually do?

Precise capabilities vary, but most XDR systems offer the same broad functionality. They bring all your security data into one place, offer some analysis of that data for rapid detection, and automate responses if an incident requires intervention.

Firstly, they offer endpoint security monitoring, network traffic analysis, and system logs together and spot connections, links, and correlations that can indicate an attack or other unusual activity. Crucially, this includes telemetry from the cloud, not just your local network. But XDR will also bring in telemetry from email systems, firewalls, and network traffic. This means rapid detection and faster response to incidents with less time logging into disparate systems for instrumentation and to check alerts.

Secondly, XDR will also offer a degree of intelligent analysis of the data it brings together. It might consider user behavior against a predefined norm, for instance. It might spot anomalous user access or escalated privileges, which could point to an account takeover. It will examine network traffic to see if data is being exfiltrated.

Finally, XDR systems are capable of automatically responding to attacks. Usually, this takes the form of following an agreed incident response playbook. This might include blocking suspect IP addresses.

This automation helps ensure your response is as rapid and effective as possible. It also ensures that staff are free to look at the bigger picture during an incident and are not bogged down in manual tasks required to lock down and secure systems.

But, perhaps the biggest benefit of XDR is visibility.

A properly configured XDR system provides a single pane of glass into your organization's security status in real time. Staff are not spending time checking access logs, network telemetry, and firewall alerts — it is all in one place, on one screen.

This allows security teams to get ahead of the unending torrent of alerts — to give them the time and mental bandwidth to think and escape the lockstep of incident response.

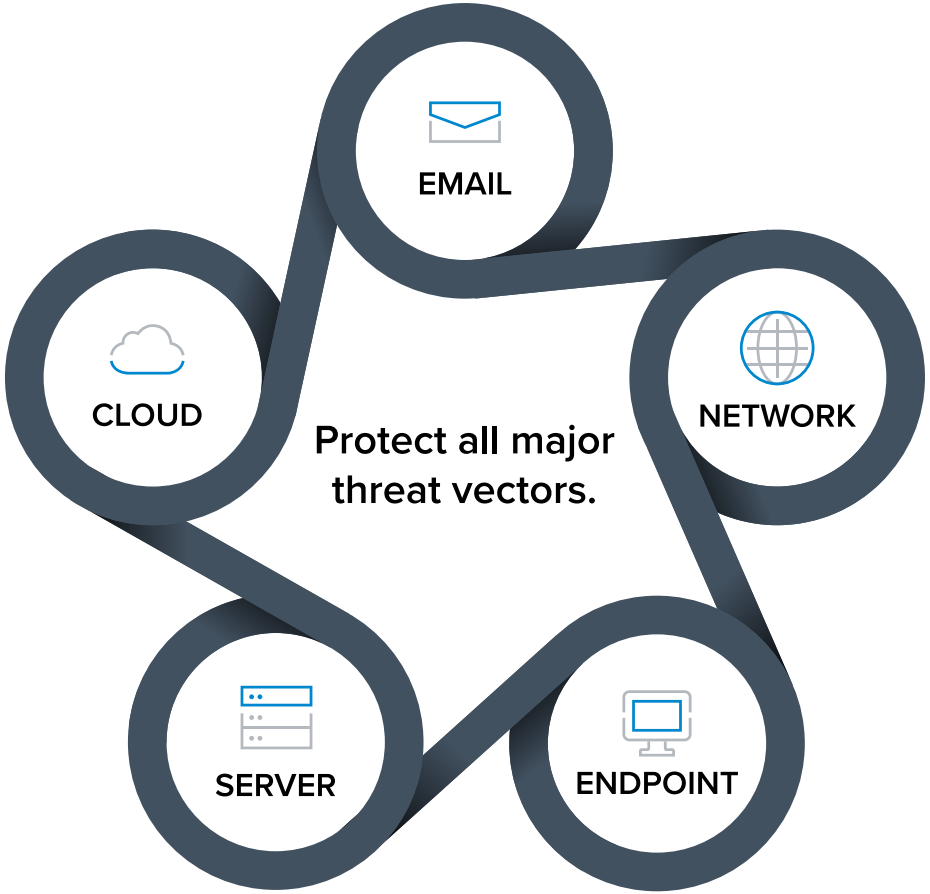
Choosing an XDR provider

The most important factor is that XDR should not be just another add-on to your security arsenal. It must be central and fully integrated with all the key components you use.

The most noteworthy advantage of XDR is that it provides your security team with a whole view of your entire digital estate. So you need to verify that it works with what you've got.

But, it must also be able to easily link with other data sources and third-party systems now and in the future. This means it must also be supported and have a development path mapped out so that you can properly and strategically plan for a secure future.

With an ever-changing threat landscape and the evolving technologies and data sources needed to counter those threats, your XDR provider must have the right skills to keep up with a rapidly changing world.



Barracuda

Conclusion

XDR is not a magic bullet. But it is a vital tool to help your security teams get ahead of attackers and make the best use of existing security controls. It means they can make rapid use of data that you are already generating, and also add new sources of telemetry quickly and painlessly. It gives them greater real-time visibility into the true security status of systems and accelerates threat detection and response.

Unlike other XDR platform vendors, Barracuda Managed XDR offers this with the support of a team of security analysts staffing its security operations center 24/7. They're constantly analyzing events from over 40 data sources and mapping them to threat detection rules to keep you and your infrastructure safe.

Learn more about Barracuda XDR.

Barracuda

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. Hundreds of thousands of organizations worldwide trust Barracuda to protect and support them so they can focus on taking their business to the next level. For more information, visit barracuda.com.