

optimum.business

Cybersecurity for Every Stage of Growth

**A Buyer's Guide from DNS Filtering to
Managed Detection and Response**



Executive Summary

Every October, Cybersecurity Awareness Month prompts a familiar round of reminders about strong passwords and phishing emails. But the harder question most organizations actually face isn't awareness; it's architecture. Given a finite budget and a finite security team (sometimes a team of one, sometimes no dedicated team at all), which controls should be in place, in what order, and at what point does it make sense to bring in outside help?

This paper maps the modern security stack, starting with **DNS-level filtering**, moving through **endpoint detection and response (EDR)**, through **cloud and access security (SWG, CASB, ZTNA)**, and up to fully **managed detection and response (MDR)**, against the realities of organizations from a five-person shop to a multinational enterprise. The goal is to provide a shared framework that business owners, IT managers, and security leaders can use to answer the same question: What do we actually need, and when?

The harder question most organizations actually face isn't awareness; it's architecture.

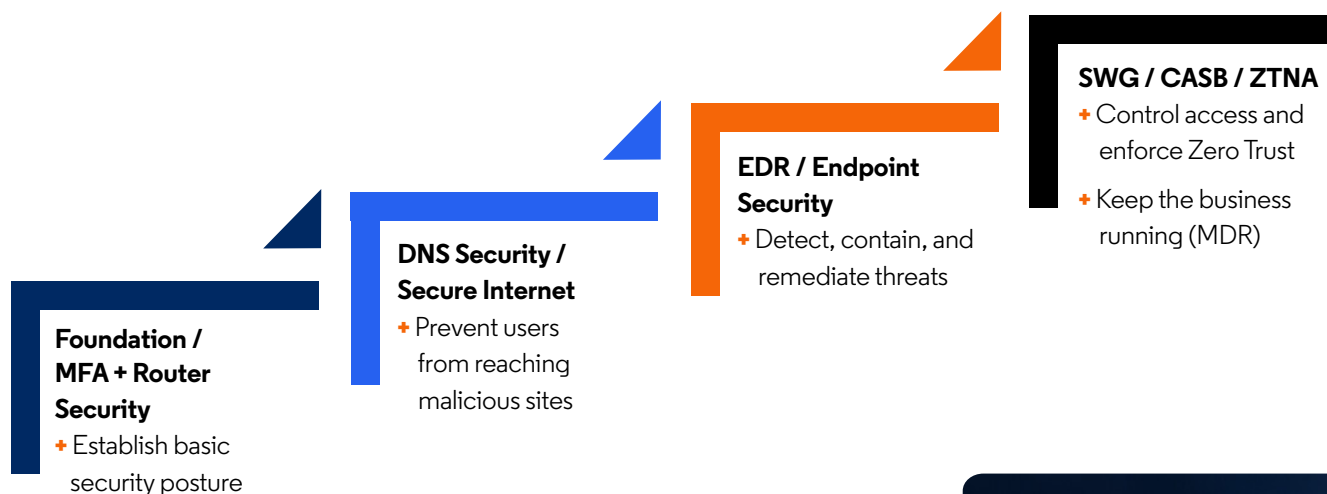
The Threat Reality Facing Businesses Today

Attackers no longer reserve their effort for the largest targets. Automated scanning, commodity ransomware kits, and phishing-as-a-service have made it economical to target organizations of every size, and several structural shifts have widened the exposure for all of them.

- + **Ransomware and extortion have become industrialized**, and smaller organizations are frequently targeted precisely because they are assumed to have weaker defenses and limited ability to withstand downtime.
- + **Phishing and business email compromise** remain the most common way attackers gain an initial foothold, regardless of how sophisticated the rest of an organization's defenses are.
- + **Remote and hybrid work** has dissolved the traditional network perimeter. Employees, contractors, and devices now connect from everywhere, which means protecting the office network alone is no longer a sufficient strategy.
- + **SaaS and cloud sprawl mean sensitive data** increasingly lives outside any network the organization directly controls, in dozens of applications that were often adopted without security review.
- + **Third-party and supply chain risk** means an organization's exposure now depends partly on the security posture of its vendors and partners, not just its own.
- + **Cyber insurance underwriting has tightened**, and carriers increasingly ask organizations to demonstrate controls such as MFA, EDR, and documented incident response when evaluating coverage and pricing.
- + **The security talent shortage** means most small and midsize organizations, and even some large ones, cannot realistically staff a 24/7 security operations center on their own.

None of this means every organization needs the same stack. It means every organization needs a deliberate stack sized to its actual risk, data sensitivity, and ability to operate and respond, not one modeled on what a much larger or smaller peer happens to run.





Understanding the Security Stack

The options covered in this paper are not competing alternatives so much as layers that build on one another. Most organizations don't choose one; they choose how far up the stack to go and how much of the operational burden to keep in-house versus hand to a managed provider.

DNS-Level Security and Web Filtering

DNS-level security inspects and controls the domain name lookups a device makes before a connection is ever established, blocking known malicious domains, phishing sites, and malware command-and-control destinations at the earliest possible point. Because it operates at the DNS layer rather than inside the device or the network traffic itself, it is lightweight to deploy (often a simple resolver change or a small agent), and it protects a device anywhere it connects, not just on the corporate network.

It is among the highest-leverage, lowest-cost controls available, but it is a prevention layer only. It stops known bad destinations, not threats that arrive through other means or that are already present on a device. It is a strong foundational layer for organizations of every size.



Endpoint Security (From Antivirus to EDR)

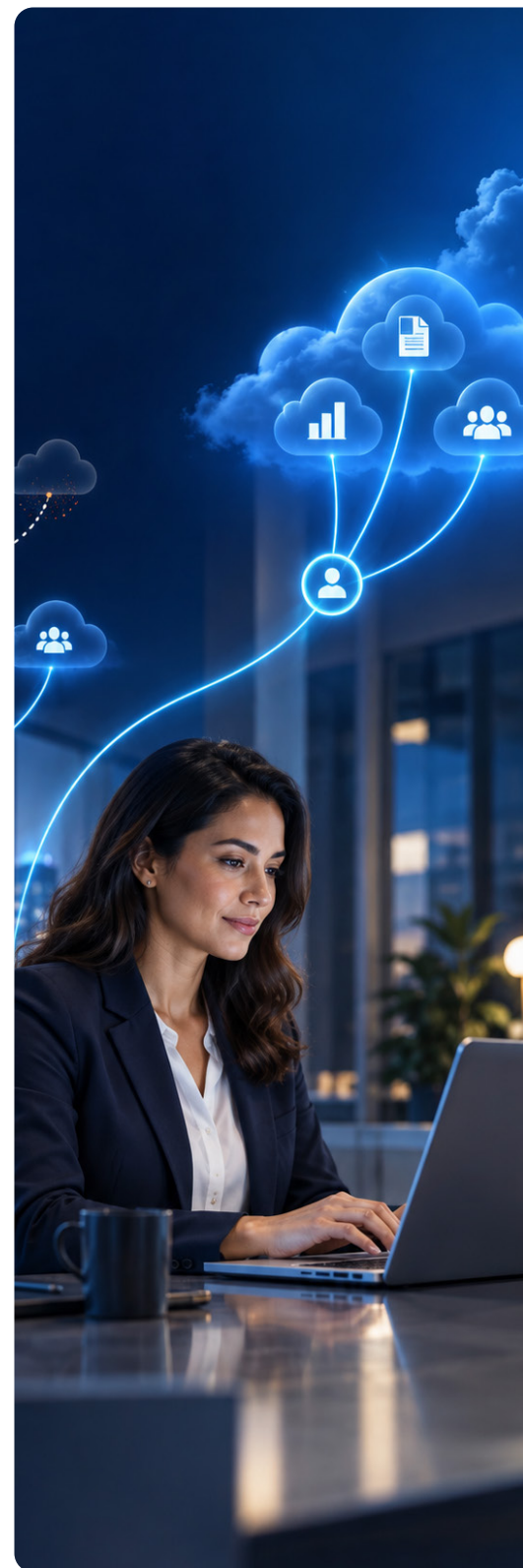
Traditional antivirus and endpoint protection platforms (EPP) look for known malware signatures on a device. Endpoint Detection and Response (EDR) goes further. It continuously monitors process behavior on laptops, servers, and workstations, looking for the patterns of an active compromise (privilege escalation, unusual lateral movement, ransomware-style file encryption) even when the specific malware has never been seen before.

EDR's real value is not just detection but response, including the ability to isolate a compromised device from the network in seconds before an incident spreads. That value depends on someone being available to review alerts and act on them; EDR generates signal, but without a triage process behind it, that signal often goes unused.

Cloud and Access Security (SWG, CASB, and ZTNA)

As work has moved off the traditional office network and onto SaaS applications accessed from anywhere, a family of cloud-delivered controls (often grouped under the umbrella of Secure Access Service Edge, or SASE) has emerged to secure that reality. A **Secure Web Gateway (SWG)** inspects and filters web traffic wherever a user is working. A **Cloud Access Security Broker (CASB)** extends visibility and policy enforcement into SaaS applications themselves, flagging risky sharing, shadow IT, or data leaving through unsanctioned apps. **Zero Trust Network Access (ZTNA)** replaces the older model of a VPN granting broad network access with narrow, identity-verified access to specific internal applications only.

Together, these tools answer a question DNS filtering and EDR do not: not just whether a device is compromised, but whether a person, using a particular device and location, should be allowed to access a specific application or data. They matter most once an organization has meaningful remote work, multiple SaaS applications, or third parties who need limited access.



Security Architecture Must Reflect How Modern Organizations Operate

Cybersecurity discussions often focus on tools, but the effectiveness of those tools depends on how people, applications, and data interact across the organization. As businesses adopt hybrid work, cloud applications, distributed offices, and third-party collaboration, security becomes increasingly tied to the underlying infrastructure that connects them.

Organizations evaluating cybersecurity investments should consider not only which controls to deploy, but also how those controls support users across different locations, devices, and applications. A security strategy that works well within a single office may look very different from one designed for a distributed workforce or a multi-site enterprise.

As environments become more complex, visibility, access control, and operational consistency become just as important as threat prevention. The most effective security programs are built around an understanding of how data moves through the organization and where the greatest business risks exist. For distributed enterprises, that often requires coordinating security policies across users, locations, applications, and cloud environments rather than treating each as a separate challenge.

The most effective security programs are built around an understanding of how data moves through the organization and where the greatest business risks exist.



Managed Detection and Response (MDR) and Managed Security Services

MDR and broader managed security service provider (MSSP) offerings layer expertise and around-the-clock monitoring on top of the tools above, rather than replacing them. A provider's analysts watch alerts from EDR, network, identity, and cloud sources continuously, correlate them into a coherent picture, and take or recommend action, typically under a contractual response-time SLA.

This is the option that most directly solves the talent shortage problem. It gives an organization the outcome of a 24/7 security operations center without the cost and difficulty of building and staffing one internally. For organizations with a strong internal team, a similar service can be used selectively (for after-hours coverage or first-line alert triage) rather than as a full replacement.

Technical Comparison

The table below summarizes how these four building blocks differ in what they protect, how they're deployed, and what they demand from the organization running them.

Dimension	DNS-Level Security & Web Filtering	EDR (Endpoint Detection & Response)	Cloud & Access Security (SWG / CASB / ZTNA)	MDR / Managed Security (MSSP)
What It Protects	Blocks access to known malicious domains, phishing sites, and malware command and control traffic before a connection is even made	The device itself (laptops, servers, and workstations), protected by watching process behavior for signs of compromise	Data and application access as users connect to the web and to SaaS/cloud apps, wherever they are working from	The organization's overall security posture, by continuously watching alerts across tools and acting on them
Deployment Model	DNS resolver setting or lightweight agent; typically live in under a day	Lightweight agent installed on each endpoint, reporting to a cloud console	Cloud proxy/gateway plus lightweight client agent; policies enforced regardless of network location	Layered on top of existing tools (EDR, firewall, cloud logs); a service, not a product install
Threat Coverage	Broad but shallow. Stops known bad destinations, phishing links, and basic malware callbacks, but blind to threats already inside a device	Deep but narrow. Catches novel and fileless malware, ransomware behavior, and lateral movement, but only on covered devices	Broad. Covers data exfiltration, risky SaaS usage, unmanaged device access, and enforces least privilege access to internal apps	Broadest. Correlates signals across endpoint, network, identity, and cloud to catch what any single tool would miss alone
Requires In-House Expertise?	Minimal. Mostly configuration, then it runs passively	Moderate. Someone needs to triage alerts and respond, or false positives and real incidents both go unaddressed	Moderate. Policy design and ongoing tuning of access rules	Low. The point of the service is to supply the expertise and around-the-clock monitoring the buyer doesn't have in-house
Response Capability	Prevention only. Blocks before the fact, with no investigation or response function	Detects and can automatically contain a single device, but a human still needs to investigate and decide next steps	Prevention and access control. Blocks or limits risky actions, but not built for incident investigation	Full detection, investigation, and response cycle, typically with a contractual response-time SLA
Typical Relative Cost	Low	Moderate	Moderate to High	Highest
Best Entry Point For	Every organization, regardless of size, given the strong return per dollar spent	Any organization with company-managed devices and sensitive data to protect	Organizations with remote/hybrid staff, multiple SaaS apps, or contractors needing limited access	Organizations that lack a 24/7 internal security team but face real, present risk

Economic Comparison

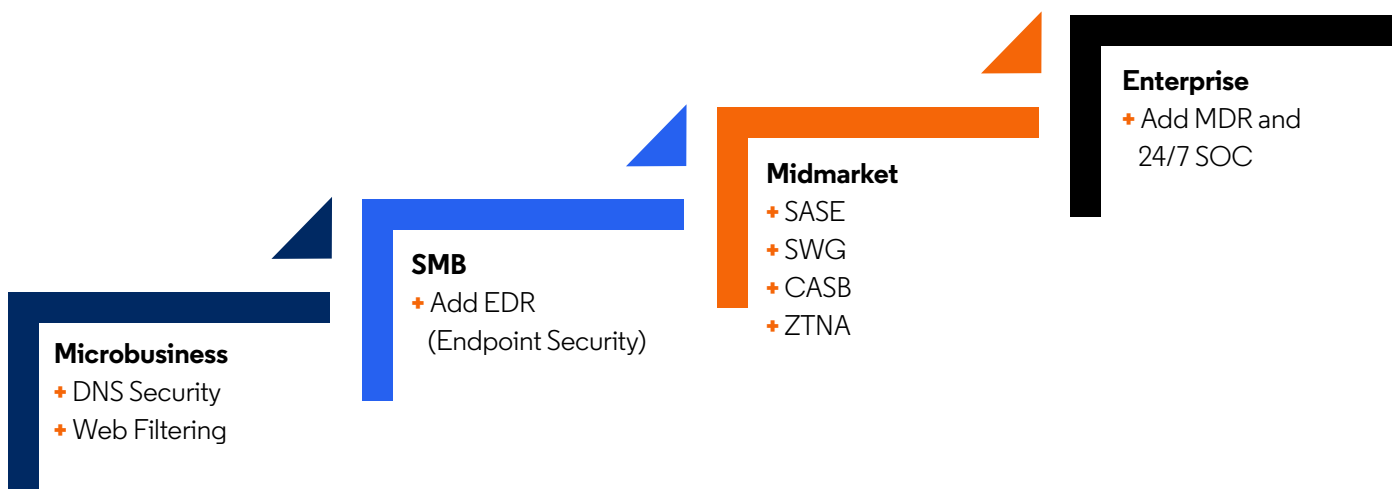
Security spending is frequently evaluated against the wrong baseline: the cost of the tool rather than the cost of the incident it prevents or shortens. The table below lays out the cost structure of each layer alongside what happens when it's skipped.

Cost Element	DNS Filtering	EDR	SASE (SWG/CASB/ZTNA)	MDR / MSSP
Pricing model	Per user or per device, monthly	Per endpoint, monthly	Per user, monthly, sometimes bundled per app/policy	Per endpoint or per user, monthly, often with tiered response SLAs
Implementation effort	Minimal. Change a DNS setting or push a small agent	Low to moderate. Agent deployment across the fleet	Moderate. Requires access and app policy mapping	Low for the buyer. The provider absorbs most onboarding work
Ongoing staffing burden	Near zero	Real. Someone must watch and act on alerts, or value is lost	Moderate. Periodic policy review as apps and staff change	Minimal. That burden is what's being outsourced
Cost of doing nothing	High. This is typically one of the lowest-cost, highest-return controls available, so skipping it is rarely justified	High. A single unmonitored, uncontained endpoint compromise can cascade into a full breach	Rising. Unmanaged SaaS and remote access are now leading breach vectors	High. Without 24/7 coverage, dwell time before detection lengthens materially
Insurance / compliance impact	Often a baseline expectation in cyber insurance questionnaires	Frequently a named requirement for favorable premiums or coverage at all	Increasingly requested for remote access and cloud data questions	Can materially improve insurability and shorten breach notification timelines



The Staffing Question Is Often the Real Cost

The sticker price of a security tool is rarely the deciding factor. The deciding factor is whether the organization has someone available to act on what that tool surfaces. An EDR platform that generates alerts no one reviews provides very little real protection despite a real monthly cost. This is precisely the gap MDR and managed security services are built to close, and it's why many organizations of every size find that a smaller number of well-monitored controls outperforms a larger number of unmonitored ones.



Decision Framework: A Maturity Ladder by Business Size

Rather than a single recommendation, most organizations benefit from thinking in terms of a maturity ladder, considering which controls are foundational at a given size, which are worth adding next, and which typically only make sense once the organization has grown further. The table below is a starting point. Actual risk profile, industry, and data sensitivity can move any organization up or down this ladder.

Business Size	DNS Filtering	EDR	SASE (SWG/CASB/ZTNA)	MDR / MSSP
Microbusiness	Foundational. Start here, as the first dollar spent	Recommended once budget allows; bundled EPP/AV is a minimum	Not typically necessary yet unless handling sensitive client data	Rarely justified on its own; consider a bundled offering from an IT provider
Small Business	Foundational. Should already be in place	Core requirement, especially for any device touching customer or financial data	Worth adding once remote work, contractors, or multiple SaaS apps are in play	Strong candidate if there is no dedicated IT security role in-house
Midmarket	Table stakes, integrated with broader DNS/network policy	Core requirement across the fleet, feeding into a broader detection strategy	Core requirement. Hybrid work and SaaS sprawl are the norm at this size	Common and often cost-effective versus building an internal 24/7 SOC
Large Enterprise	Baseline control, usually one part of a larger secure access strategy	Core requirement, frequently paired with a broader XDR strategy	Core requirement, usually as part of a full SASE/zero-trust architecture	Used selectively to extend an internal SOC's coverage (nights/weekends, tier-one triage) rather than replace it

Key Principle

Layer in order, not all at once. DNS filtering is often one of the first security investments because it can prevent a broad range of threats with relatively low cost and operational effort. Every layer above it should be added when the organization's risk, headcount, or regulatory exposure outgrows what the layer below it can cover, not simply because a larger peer has it.

Use Case Deep Dives



Microbusiness

At this size, there is rarely a dedicated IT or security role, and every dollar of security spend competes directly with core operating costs. The priority is maximum protection for minimum operational burden. DNS-level filtering and a bundled endpoint protection/antivirus package, both configured once and left to run passively, address many of the most common risks. A password manager and multifactor authentication (MFA) on email and financial accounts round out the essentials. Full EDR, SASE components, or MDR are usually premature here unless the business handles unusually sensitive data (health records, payment data, legal files) or is contractually required to meet a client's security standards.



Small Business

This is typically the point where the business has enough devices, enough customer or financial data, and enough attack surface that DNS filtering and basic antivirus are no longer sufficient on their own. EDR becomes a core requirement, particularly for any device that touches customer or payment data. If the business has remote employees or contractors, or has adopted several SaaS applications, a lightweight SASE offering, particularly ZTNA in place of a traditional VPN, is worth prioritizing next. Because a dedicated security hire is rarely justified at this size, a managed offering that bundles EDR monitoring with the underlying tools is often the most practical way to get real detection and response coverage without building a team.



Midmarket

Midmarket organizations typically have enough scale to justify a real security budget and often at least one dedicated security or IT security hybrid role, but rarely enough to staff detection and response around the clock. DNS filtering, EDR, and SASE components are all core requirements at this size, since hybrid work and environments with multiple SaaS applications are the norm, not the exception. MDR is frequently the most cost-effective way to close the 24/7 coverage gap. It is usually far less expensive than building an internal SOC, while still providing continuous monitoring and a documented response process that satisfies both customers and cyber insurance underwriters.



Large Enterprise

Large enterprises generally have all four layers in place already, often as part of a broader zero-trust or XDR (extended detection and response) architecture with a dedicated internal security team. The open question at this size is usually not which layers to adopt but how to extend and optimize them, using managed services selectively to cover after-hours monitoring, first-line alert triage, or specialized threat hunting capacity that would be inefficient to build and retain in-house. The economics shift from build versus buy wholesale to a more surgical question of which specific gaps a managed partner should fill.

Large enterprises also face challenges less common in smaller organizations, including security-tool sprawl, complex compliance requirements, distributed operations, third-party ecosystems, and growing volumes of security telemetry. At this scale, success often depends less on adding tools than on improving visibility, integration, and operational efficiency across existing investments. Controls, processes, and response capabilities must remain aligned across business units, locations, users, and applications as the organization grows.

A Buyer's Checklist

Before adding to or building out a security stack, decision-makers should be able to answer the following questions:

- ☒ **What is our most sensitive data**, and where does it actually live today, on managed devices, in SaaS applications, or both?
- ☒ **Do we have anyone who can review and act** on security alerts today, and how quickly?
- ☒ **Are our devices and users ever outside** the traditional office network, and if so, how are they currently protected there?
- ☒ **Has a customer contract**, a cyber insurance application, or a regulator specifically required any of these controls?
- ☒ **If a device were compromised right now**, how would we find out, and how long would that take?
- ☒ **Is our next security dollar better spent on a new tool**, or on monitoring and response for the tools we already have?
- ☒ **As we grow**, at what size or milestone will we revisit this stack rather than letting it grow by default?

Answering these honestly and revisiting them as the organization grows, does more to close real security gaps than adopting any single tool in isolation.

Conclusion

There is no single correct security stack; there are only the right layers for an organization's actual size, data, and ability to monitor and respond. DNS-level filtering is a strong foundational step. EDR becomes increasingly important once an organization has sensitive data on managed devices. Cloud and access security controls become increasingly important once work has moved off the traditional network. Managed detection and response exists specifically to close the gap between the tools an organization has and the 24/7 attention those tools require to be effective.

Cybersecurity Awareness Month is a useful annual prompt to ask the harder architectural question, not just the awareness one. Given where the organization is today and where it's headed, does its current security stack match its actual risk, or is it simply what accumulated along the way?

Next Steps

Connect with the Optimum Business Enterprise team to assess your cybersecurity needs and build a security strategy that fits your organization today and as it grows.

Learn more at: optimum.com/business/west/enterprise