Cyber security as a managed service

Protecting critical data throughout the enterprise—from your core systems to your partner ecosystems

Facing sophisticated, rapidly evolving threats from both inside and outside the corporate network, many small and mid-sized organisations struggle to maintain the skills and resources required for a comprehensive approach to cyber security.

While it may seem easy enough to deploy point solutions to address perceived vulnerabilities, a patchwork approach inevitably leaves gaps that attackers can exploit. Truly effective defence only comes from a coordinated, holistic approach to cyber security—but that's hard to achieve without dedicated in-house security expertise.

Northdoor's unique cyber security managed service helps small and mid-sized organisations design, implement, run, and govern the appropriate security policies and technologies – and extend them from their core systems all the way out to their ecosystems of partners and customers.

Combining deep expertise in cyber security with world-class technology, Northdoor offers a single-source service that protects critical data and systems, freeing our clients to focus on their business objectives.

northdoor
Store IT · Protect IT · Use IT

Rising risks for SMEs

The cyber attacks and data breaches that hit the headlines naturally tend to involve large, high-profile organisations. This can lull smaller organisations into a false sense of security. The reality is that small- and medium-sized enterprises (SMEs) are an increasingly common target for cyber-criminals.

SMEs are less likely to have dedicated cyber security resources and may assume that criminals will seek richer pickings from bigger, better-known targets. But relying on security through obscurity is a high-risk strategy. Given the largely automated nature of many cyber attacks, criminals can afford to probe the defences of thousands of companies at once. And they are likely to have more success targeting under-prepared SMEs than larger, better-protected enterprises.

According to RiskRecon, data breaches at small businesses jumped by 152% in 2020-21. This was more than double the rise in data breaches at larger companies over the same period.[1]

Growing complexity and scale

A key reason for the increase in cyber security risk is the proliferation of new applications, devices, and data sources both inside and outside the typical organisation. Today's IT teams must not only protect their organisations from ever more frequent cyber threats, but also maintain security across a much more complex and distributed infrastructure. And with global annual expenditure on digital transformation set to hit US$2.8 trillion by 2025, the attack surface will continue to grow in both complexity and scale.

While the need to secure information systems and assets against threats is a constant, the challenge has grown exponentially since the global pandemic, which supercharged the adoption of remote working models. SMEs now face a significant challenge in protecting existing data, systems, devices, and users across networks that blur the boundaries between office and non-office locations. At the same time, they must continue their digital transformation without opening up new vulnerabilities. Furthermore, they need to achieve both these objectives against a backdrop of increasing regulatory scrutiny and compliance expectations.

[1] https://blog.riskrecon.com/company/media-coverage/small-business-mighty-attack-surface

Taking a holistic view

Given the scale of the challenges and the pace of change, a piecemeal approach to cyber security will not provide adequate protection. Entire business models now rely on digital capabilities, so any disruption to processes or exposure of data could cause significant financial, reputational, and regulatory damage. A correspondingly comprehensive approach to cyber security is vital, including close alignment between cyber security practices and the overall business strategy.

In particular for SMEs, it has always been challenging to hit the moving target of cyber security. It is hard to find the time, people, budget, skills, and experience to design the optimal information security strategy, put in place the corresponding organisational structures and software solutions, and manage this security infrastructure over time.

Moreover, given constrained IT budgets, it is likely that many organisations will be reining in capital investments and trying to extend the useful life of their existing systems – putting more pressure on existing IT personnel to keep the lights on.

Even where an organisation has the budget to expand its team to include security experts, the current UK recession is combined with an extremely tight labour market, making it hard to find and retain the right talent at any price.

Striking the right balance

Beyond skills, there is potentially a bigger issue in play: effective cyber security is a challenge not just for technologists, but also for businesspeople. After all, if total data security was your only concern, the easiest way to achieve it would be to switch off all your devices, shutter all your offices, and give all your employees a leave of absence.

In the real world, companies clearly need to strike a balance between security on the one hand and ability to do business on the other. IT security and business teams must work together to identify cyber security risks and decide whether they can be mitigated, accepted, or deferred.

Achieving and maintaining alignment between IT security and business teams requires skills and experience that smaller organisations lack. SMEs will therefore benefit from working with a service provider that can draw on past experience to create a joined-up cyber security capability based on well-defined roles and policies.

Cyber security as a managed service

Organisations must accept that the risk of a cyber attack can never be reduced to zero. An effective approach to cyber security must therefore not only implement practical defences, but also set up and maintain the appropriate policies and capabilities to respond appropriately when a security breach occurs.

That means cyber security isn't a one-and-done exercise; it's something that organisations must think about constantly. That can be especially taxing for SMEs, who are unlikely to have the resources to dedicate to a comprehensive cyber security programme.

To help small and mid-sized organisations access vital cyber security skills and experience – and to enable larger organisations to outsource some or all of their cyber security workload – Northdoor offers cyber security as a fully managed service. Our approach provides comprehensive protection for critical data assets from core systems all the way out to the extended web of relationships with partners and customers.

> *Cyber security isn't a one-and-done exercise; it's something that organisations must think about constantly... To help small and mid-sized organisations access vital cyber security skills and experience – and to enable larger organisations to outsource some or all of their cyber security workload – Northdoor offers cyber security as a fully managed service.*

Flexible, tailored, cost-effective

Building on decades of experience serving blue-chip clients, Northdoor experts take the time to understand each organisation's unique strategy, requirements, and appetite for risk. We then design a tailored service that addresses the cyber risks cost-effectively.

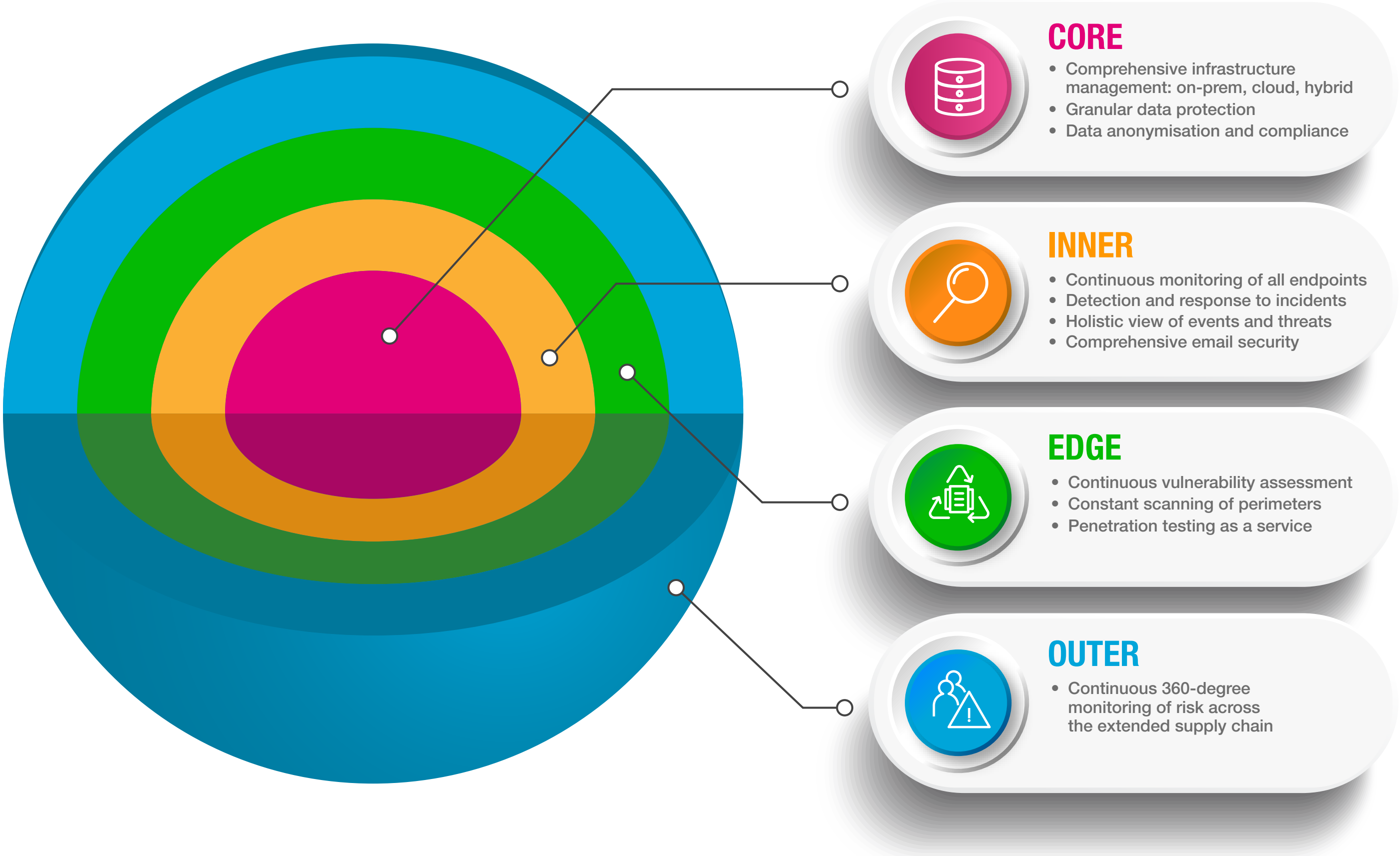
Northdoor can handle as much or as little of the cyber security role as required: from infrastructure management and endpoint monitoring to continuous vulnerability scanning and supply-chain risk assessments, and everything in between.

By engaging Northdoor to manage cyber security, organisations can cost-effectively access deep skills and experience, freeing up in-house IT employees to work on value-add projects. Our managed service for cyber security is delivered by a team of experts that spreads its time over multiple client environments, so that each client gets the appropriate level of support and attention without the high cost of a dedicated internal team.

Northdoor's economies of scale reduce the cost below what any individual SME could achieve on its own. The managed service approach also removes concerns about key staff going on holiday, taking sick leave, or becoming de-skilled from not having enough to keep them busy.

Northdoor begins the process of protecting critical information systems and assets by performing an objective assessment of the current state of readiness. We compare this to the targeted future state of readiness, then set out a programme of improvements to enable the transformation. We design and execute the appropriate strategy, including the organisational and governance structures, and deploy the technology solutions to protect critical data from the core out.

Northdoor's managed service for cyber security provides defence in depth across Core, Inner, Edge and Outer layers.



CORE

- Comprehensive infrastructure management: on-prem, cloud, hybrid
- Granular data protection
- Data anonymisation and compliance

INNER

- Continuous monitoring of all endpoints
- Detection and response to incidents
- Holistic view of events and threats
- Comprehensive email security

EDGE

- Continuous vulnerability assessment
- Constant scanning of perimeters
- Penetration testing as a service

OUTER

- Continuous 360-degree monitoring of risk across the extended supply chain

In the **Core** layer, Northdoor protects data at rest and in motion across databases and other stores wherever they are located: on-premises, in the cloud, or a hybrid of the two. We define and apply granular data protection, and we establish robust, highly automated anonymisation capabilities.

In the **Inner** layer, Northdoor protects users and their applications, deploying advanced technologies for detecting, diagnosing, reporting on, and responding to emerging security threats. Our email security solutions intelligently defend against the accidental or deliberate exfiltration of sensitive data and are backed by ongoing user training.

In the **Edge** layer, Northdoor monitors and probes all the points at which the organisation's systems and data come into contact with the outside world. We set up and manage continuous assessment and remediation of software vulnerabilities, and we provide penetration testing as a service to reassure both internal management and external auditors.

In the **Outer** layer, Northdoor provides 360-degree monitoring of extended cyber security risks across the extended chain of connected partners, suppliers, and clients. With real-time intelligence on vulnerabilities across the entire supply chain attack surface, clients can evaluate the security stance of corporate suppliers and business partners far beyond organisational boundaries.

northdoor
◦ Store IT ◦ Protect IT ◦ Use IT ◦

A comprehensive service to add business value

The Northdoor managed service for cyber security works to align cyber security policies and practices with strategic business objectives. Our stance is highly pragmatic: we understand the importance of striking the right balance between security and usability. With our expertise, we can help you minimise the friction on your business processes without introducing unacceptable risk.

Our comprehensive managed service covers both technological and organisational aspects, helping clients develop the appropriate IT policies, procedures and best practices while establishing a strong internal culture around cyber security. Northdoor's managed service includes comprehensive monitoring and reporting capabilities, making it easier to comply with internal and external audit requirements.

In addition to mitigating internal and external threats, and ensuring rapid and effective response to security incidents, we help organisations understand their evolving risk profile and gain end-to-end visibility of their data assets – wherever they are. As each organisation undertakes new data-related projects, we help them to understand the cyber security implications so that they can deliver the projects faster and at lower risk.

With the Northdoor managed service for cyber security, organisations can redeploy internal IT resources to focus on transformational value-add projects, safe in the knowledge that expert eyes and world-class tools are protecting their core data assets.

Take the next step

Contact Northdoor for more information or to arrange a free review of your existing cyber security practices.