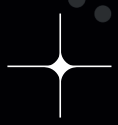
nedscaper

// WHITE PAPER

Strong Security, Satisfied Clients

How MSPs can better meet their clients' security expectations.



NEDSCAPER
MANAGED EXTENDED
DETECT AND RESPOND
SYSTEM AQUIRE

// Table of contents

// Strong Security, Satisfied Clients

Every Managed Service Provider (MSP) and their clients share the same dreaded nightmare: paying ransom to cybercriminals to regain access to their own files. The consequences are severe, and recovery can take weeks, if not months. But how do you ensure you have the right knowledge and resources to prevent this? More importantly, how do you ensure that your customers remain protected and satisfied, so they do not switch to the competition? Let us guide you through Nedscaper's vision on how your company can do just that.

Client security expectations

As an MSP, you are responsible for meeting your clients' expectations in the cybersecurity field. Although clients may not always explicitly state these expectations, they assume their systems and data are well-protected. They expect everything to be taken care of and rely on you to take on the responsibility for their digital security You often hear customers say, "My IT vendor manages my laptops and systems. They take care of everything, including security. But am I sufficiently protected against ransomware? I don't know..."

At the same time, clients are reading more about cyber threats such as malware, ransomware, CEO fraud, phishing attacks, and data breaches. This increasing flow of information forces them to seriously consider their organization's security measures. In addition, they must deal with legal obligations such as the General Data Protection Regulation (GDPR). However, for many clients, it is unclear which specific rules apply to them, such as the NIS2 Directive, what it entails, and the consequences of non-compliance.

Why MSPs need to be extra vigilant

As an MSP, you hold the key to your clients' IT environment, making you a prime target for cybercriminals. If a hacker breaches your systems, they can easily access the systems and data of all your clients through your network. This means that a successful attack on your company can have widespread effects, not only for you but also for all the organizations that rely on your services.

Cybercriminals increasingly target MSPs because they serve as "gateways" to multiple clients. By hacking one MSP, they gain access to data from dozens, if not hundreds, of organizations. This makes it crucial for MSPs to elevate their security measures to the highest level.

// 4 challenges that MSPs face

A robust cybersecurity approach is essential, but MSPs encounter several challenges that make it difficult to meet client expectations and comply with new regulations. Here are some of the main obstacles:

1 // Staff shortages and lack of expertise

The demand for cybersecurity professionals far exceeds the supply. This shortage makes it difficult for MSPs to maintain adequately staffed security teams. Existing employees become overburdened and often lack the time or focus to effectively manage security incidents, increasing the risk of errors.

2 // Complexity of modern cyber threats

Cyberattacks are becoming increasingly complex and sophisticated, requiring specialized knowledge and tools to quickly detect and neutralize new threats. Many MSPs lack the resources to keep up with these technologies, making them more vulnerable.

3 // Limited budget

Not all MSPs have the financial means to invest in comprehensive security infrastructure, software licenses, and staff training. This results in a lack of modern tools and expertise, which further increases the risk of security breaches. Additionally, training and certifications are often costly, leading MSPs to hesitate in making such investments.

4 // Compliance and regulations

With the arrival of the NIS2 Directive and other regulations, it is becoming increasingly difficult for MSPs to meet all the requirements. Obligations around risk assessments, incident reports, and implementing appropriate security measures require significant knowledge and effort. MSPs that fail to respond in time run the risk of sanctions or fines.

// What is NIS2 and why is it gaining attention?

In light of growing digital threats, the European Union has developed a strengthened directive for network and information systems: the NIS2 Directive. This directive aims to enhance the digital and economic resilience of European member states. For MSPs, this means they bear responsibilities not only for their own security but also for the security of their clients.

The NIS2 Directive is designed to boost digital resilience among European organizations and will be implemented in the Netherlands in 2025 as the Cybersecurity Act. This law imposes new obligations on organizations, including MSPs, such as risk assessments, implementing appropriate security measures, and a 24-hour incident reporting requirement. The Dutch government advises organizations to take proactive measures now, such as conducting a risk analysis, implementing suitable measures, and setting up incident management procedures to better prepare for this legislation and current threats.

NIS2 overview:

- European directive aimed at strengthening cybersecurity.
- Expands to broader sectors, including digital services.
- Increased cyber threats demand stricter security measures.
- Greater focus on risk management and incident response.
- Sanctions and obligations make compliance more critical for companies.

// 4 Steps to meet client security expectations

To meet the rising security expectations of clients and comply with regulations like NIS2, MSPs need to take strategic steps. This starts with understanding the risks their clients face and implementing appropriate security measures.

1 // Know your clients and their risks

To provide an effective security approach, you must understand your clients' specific needs and risks. This begins with a risk assessment. Ask yourself:

- What valuable data and systems need protection?
- What are the potential threats, and how does their current security compare?
- Which compliance requirements apply to this client?t?

A risk assessment allows you to tailor security measures to your client's needs, ensuring you offer solutions that are genuinely relevant.

2 // Build a strong cybersecurity foundation

Security starts with the basics. As an MSP, you need to ensure your clients have the right foundations for their security strategy. Here are some essential measures to implement:

- **Multi-Factor Authentication (MFA):** Implement MFA to make it significantly harder for unauthorized users to access sensitive data or systems.
- **Extended detection and Response (XDR):** mUse advanced security tools for automatic detection of suspicious activity and immediate countermeasures.
- **Security Service Edge (SSE):** Implement solutions for secure access to websites and applications, ensuring your clients remain protected even outside their own network.

3 // Continuously monitor your digital environment

Cyber threats are constantly evolving, so it's crucial to monitor client systems 24/7. Real-time monitoring allows security experts to respond immediately when a threat is detected, minimizing potential damage.

4 // Transparent communication on security

Clients want assurance that their data is safe, and their business continuity is secure. Clearly communicate the measures you're taking and explain why they're necessary. By being transparent, you build client trust and prevent misunderstandings.

// Partner with a security expert

If you lack the resources or expertise to offer comprehensive cybersecurity services on your own, consider partnering with a specialized security provider. Partnering with an expert like Nedscaper gives you access to advanced security solutions such as Managed Extended Detection and Response (MXDR). This ensures your clients are well-protected without the need for significant investment in your own security teams or infrastructure.

- **Direct Access to Expertise:** No need to hire or train expensive internal security experts. A skilled partner takes on this responsibility.
- **24/7 monitoring and response**: With a specialized partner, clients can rely on constant monitoring and rapid action in case of incidents.
- **Future-Proof Solutions:** Partners like Nedscaper leverage the latest technologies and methods, ensuring your clients stay protected against new threats.

Why Nedscaper's services meet MSPs' needs

In a world of increasingly complex cyber threats and growing regulatory pressure, MSPs need reliable, scalable solutions. The shortage of staff and expertise, combined with the complexity of modern threats, makes it challenging for many MSPs to meet client expectations. This is where Nedscaper comes in. With our Managed Extended Detection and Response (MXDR) solution, we provide the support and tools MSPs need to protect their clients and stay compliant.

Managed Extended Detection and Response by Nedscaper

Nedscaper offers MSPs and their clients a fully integrated cybersecurity solution powered by industry-leading Microsoft tools. Our Managed XDR platform provides 24/7 threat prevention, detection, and response, supported by AI and a team of over 80 security specialists. This allows you to continuously identify vulnerabilities and respond instantly when needed, keeping clients protected against ever-evolving cyber threats.

As the largest Microsoft-only Managed Security Services Provider (MSSP) in the Netherlands, we have a unique position. With our Microsoft Verified Managed XDR Solution status, we maximize Microsoft's capabilities. If you decide to end our partnership, you will retain access to your carefully managed Microsoft environment.

// Conclusion: Strengthen your security and protect your clients

As an MSP, you face the challenge of meeting ever-higher client security expectations while navigating increasing regulatory demands like the NIS2 directive. By taking proactive measures now, you can not only ensure optimal client protection but also future proof your own business. Whether you choose an in-house approach or partner with a specialized security provider, the key is to be prepared for the ever-evolving cyber threats.

Cybersecurity is no longer optional but essential. Investing in the right solutions and expertise is crucial to maintaining client trust and strengthening your competitive position.

// Want to learn more?

Ready to elevate your cybersecurity approach and provide even better protection for your clients? Nedscaper offers specialized security solutions and support to help you achieve this. Contact us today for a free consultation and discover how our Managed Extended Detection and Response (MXDR) can help you stay ahead.

+31 (0)20 299 9848

connect@nedscaper.com

// About Nedscaper

Nedscaper delivers pragmatic, accessible cybersecurity services across Europe and Africa. Its Managed XDR platform provides real-time threat detection, rapid response, and expert consulting, ensuring 24/7 protection for corporates and local governments, while SMBs are supported through a partner network.

Built around Microsoft's security tools, Nedscaper leverages software many organizations already trust, seamlessly integrating security into existing systems. This approach makes cybersecurity a natural extension of daily operations.

With offices in Amsterdam, Cape Town, and Johannesburg, and a growing global partner network, Nedscaper continues to expand, building trust in the digital world.