NORTH ATLANTIC NETWORKS
YOUR CYBERSECURITY PARTNER

FORTIFYING YOUR CYBER DEFENSES

The Benefits of Managed Security Service Providers

With cyber threats lurking around every corner, Managed Security Service Providers help businesses fortify their cyber defenses and stay ahead of the curve. From risk assessment to compliance management, MSSPs provide a range of services that can help businesses manage their cyber risks with ease and peace of mind.

www.nan.com

16 Mason Ave., North Attleboro, MA 02760

Overview

In today's rapidly evolving cybersecurity landscape, businesses are under constant threat from cybercriminals seeking to exploit vulnerabilities in their systems. As a result, the need for robust and reliable security measures has never been more critical. However, maintaining a strong security posture is becoming increasingly challenging for organizations of all sizes, as threats continue to become more sophisticated, and security requirements grow more complex.

Managed Security Service Providers (MSSPs) have emerged as a valuable solution for businesses looking to strengthen their security defenses without the need for extensive in-house resources. MSSPs provide a comprehensive suite of security services and expertise, delivered through a managed service model, allowing businesses to focus on their core operations while leaving the security management to the experts.

In this white paper, we explore the unique benefits of MSSPs and how they can help organizations to overcome the challenges of maintaining a strong security posture. We will delve into the various types of MSSPs, the different security services they offer, and how they can be tailored to meet the specific needs of different organizations.

We will also examine the various advantages MSSPs offer, including access to specialized skills and knowledge, round-the-clock monitoring and support, and cost-effectiveness. We will also discuss the various considerations that businesses should take into account when selecting an MSSP, such as their track record, service level agreements, and compliance with relevant standards and regulations.

Overall, this white paper aims to provide a comprehensive overview of the unique benefits of MSSPs, highlighting why they are becoming an increasingly popular choice for organizations seeking to bolster their security defenses in the face of ever-evolving cyber threats.

MSSP Services

There are several types of MSSPs, each with different service offerings. The most common types include:

1. Pure-play MSSPs: These are companies that specialize in cybersecurity services and have no other business lines. Pure-play MSSPs offer a range of services, including threat detection, incident response, and compliance management.

2. Telecom MSSPs: These are telecommunications companies that have expanded their offerings to include cybersecurity services. Telecom MSSPs typically offer managed security services, such as firewall management and intrusion detection.

3. IT consulting firms: These are companies that provide IT consulting services and have expanded their offerings to include cybersecurity services. IT consulting firms typically offer a range of cybersecurity services, such as security assessments and vulnerability management.

4. Managed Service Providers (MSPs): These are companies that provide IT services, such as network management and cloud services, and have expanded their offerings to include cybersecurity services. MSPs typically offer a range of managed security services, such as antivirus and antimalware protection.

> Cybersecurity is a shared responsibility. We rely on banks, energy companies, and telecommunications providers to keep our daily lives on track. MSSPs play a critical role in helping these organizations to detect and respond to cyber threats, and ultimately protect our digital lives."
>
> Satya Nadella, CEO of Microsoft

MSSP Expertise

MSSPs possess specialized skills and knowledge in cybersecurity that many businesses lack. This expertise allows MSSPs to provide a range of services that help businesses manage their cyber risks effectively. The following are some of the specialized skills and knowledge that MSSPs can provide.

Threat intelligence is one of the specialized skills that MSSPs possess. MSSPs have access to the latest threat intelligence and can use this information to identify and respond to potential threats before they can cause harm. They are equipped with the tools and technologies to monitor and analyze the threat landscape, enabling them to detect and respond to cyber threats in real-time.

MSSPs can also provide incident response services. They have experience in responding to cybersecurity incidents and can help businesses minimize the impact of an attack. By having a well-defined incident response plan in place, MSSPs can help businesses quickly detect, analyze, and mitigate cyber threats. This enables businesses to reduce the time and costs associated with responding to a security incident.

Compliance management is another specialized skill that MSSPs possess. They can help businesses navigate complex regulatory environments by providing compliance management services, such as compliance assessments and regulatory reporting. With the increasing number of regulatory requirements, MSSPs can help businesses stay up-to-date with the latest regulations, ensuring that they remain compliant and avoid costly penalties.

MSSPs also hold a deep understanding of cybersecurity and can provide guidance and support to businesses on cybersecurity best practices. With the rapid evolution of cyber threats, businesses need to stay up-to-date with the latest cybersecurity trends and technologies. MSSPs can help businesses develop and implement effective cybersecurity strategies that align with their business objectives and risk tolerance.

MSSPs offer businesses the flexibility to tailor their services to meet their specific needs. This approach helps organizations manage their cyber risks more effectively and efficiently. MSSPs can customize their services in several ways, including through Service Level Agreements (SLAs), customized reporting, and scalability.

SLAs allow MSSPs to set expectations for the level of service and response times that businesses can expect. These agreements can be customized to meet the specific needs of different organizations. For example, some businesses may require 24/7 support, while others may only need support during business hours. MSSPs can tailor their SLAs to meet these different requirements, ensuring that businesses receive the level of service they need.

MSSPs can also provide customized reporting that is tailored to the needs of different organizations. This reporting can include metrics that are relevant to the specific business, such as the number of attempted attacks or the number of incidents detected. By providing this customized reporting, MSSPs can help businesses better understand their cyber risks and identify areas where they need to focus their efforts.

Finally, MSSPs can scale their services to meet the needs of businesses of different sizes. This allows businesses to start with a basic level of service and scale up as their needs change over time. For example, a small business may start with basic threat detection and incident response services, while a larger organization may require more advanced services, such as compliance management. MSSPs can provide these services as needed, allowing businesses to grow and adapt without having to change service providers.

The flexibility offered by MSSPs allows businesses to choose the services that are most relevant to their needs and helps them manage their cyber risks more effectively. Through customized SLAs, reporting, and scalability, MSSPs provide tailored services that meet the unique needs of any organization.

69%

of organizations are planning to increase their investment in managed security services over the next 12 months.

This suggests that more and more organizations are recognizing the value of MSSPs in managing their cybersecurity risks and are willing to invest in these services to enhance their security posture.

Source: https://www.accenture.com/us-en/insights/security/managed-security-services-2019

> Organizations are increasingly looking to MSSPs to help them manage the complexity of cybersecurity. With limited resources and a constantly evolving threat landscape, partnering with an MSSP can provide access to expertise and technology that would be difficult to achieve in-house."

Rob Clyde, Board Director of ISACA and Executive Chair of White Cloud Security,

Strengthening Security

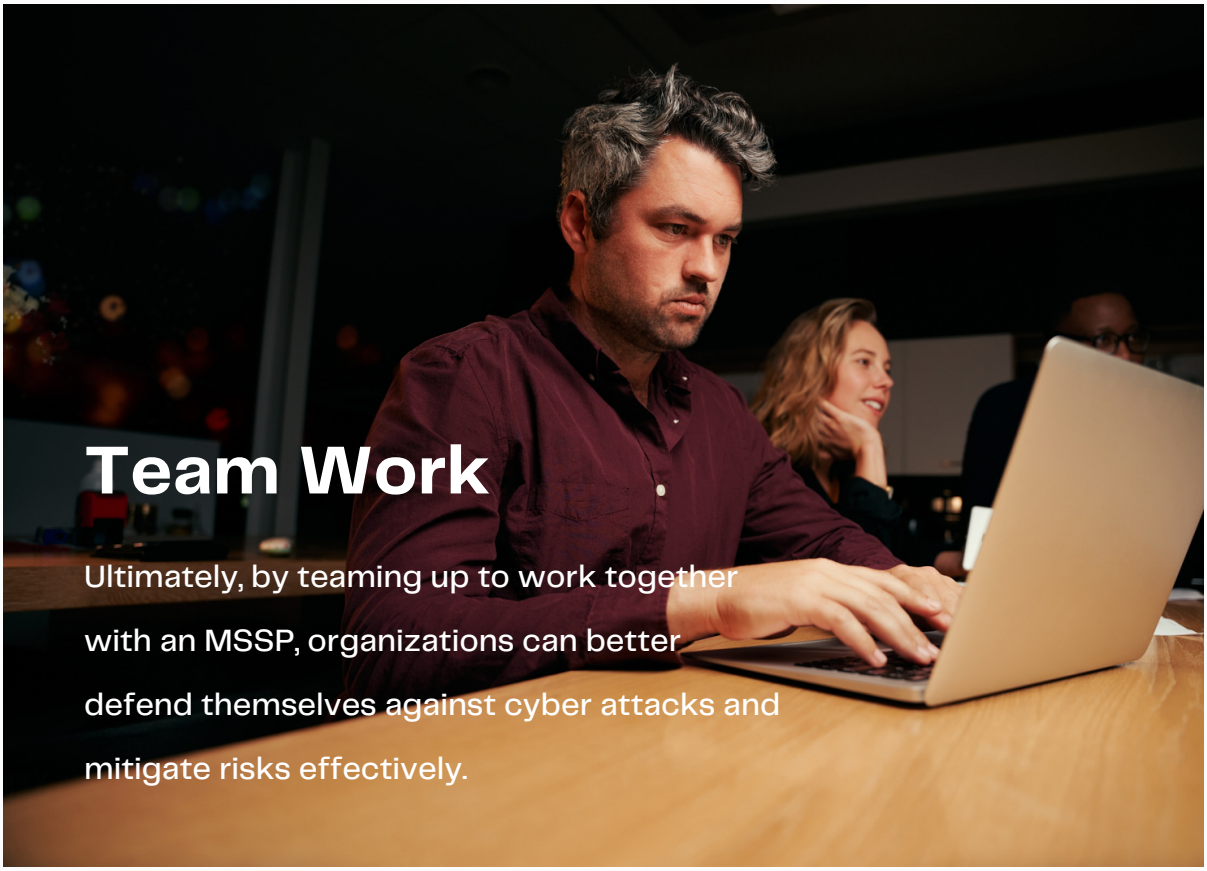
It's time to take action and ensure your security posture is strong enough to protect your business against the growing threat of cyber attacks. That's why we urge you to consider engaging with a Managed Security Service Provider (MSSP) to strengthen your defenses.

By engaging with an MSSP, you can proactively safeguard your organization's data, intellectual property, and reputation. Don't wait for a security breach to happen – take action now and engage with an MSSP to ensure your organization's security posture is as strong as possible.

By engaging with an MSSP, an organization can free up internal IT resources to focus on business-critical projects that drive innovation and growth. The MSSP can handle the day-to-day security tasks, allowing the other business to focus on developing new products, improving customer experiences, and expanding business.

Furthermore, an MSSP can also help a company comply with various regulatory requirements and standards, such as GDPR, HIPAA, and PCI-DSS. Compliance is essential for building customer trust, avoiding fines and penalties, and expanding into new markets.

In short, MSSPs not only provide a more secure business environment but also help drive growth and compliance. By partnering with an MSSP, an organization can achieve a competitive edge and gain long-term success.



MSSPs are becoming an increasingly popular choice for organizations seeking cybersecurity solutions due to their specialized expertise, cost-effectiveness, and ability to provide a comprehensive range of security services. By outsourcing their security needs to an MSSP, organizations can free up internal resources, reduce costs, and gain access to the latest security technologies and best practices.

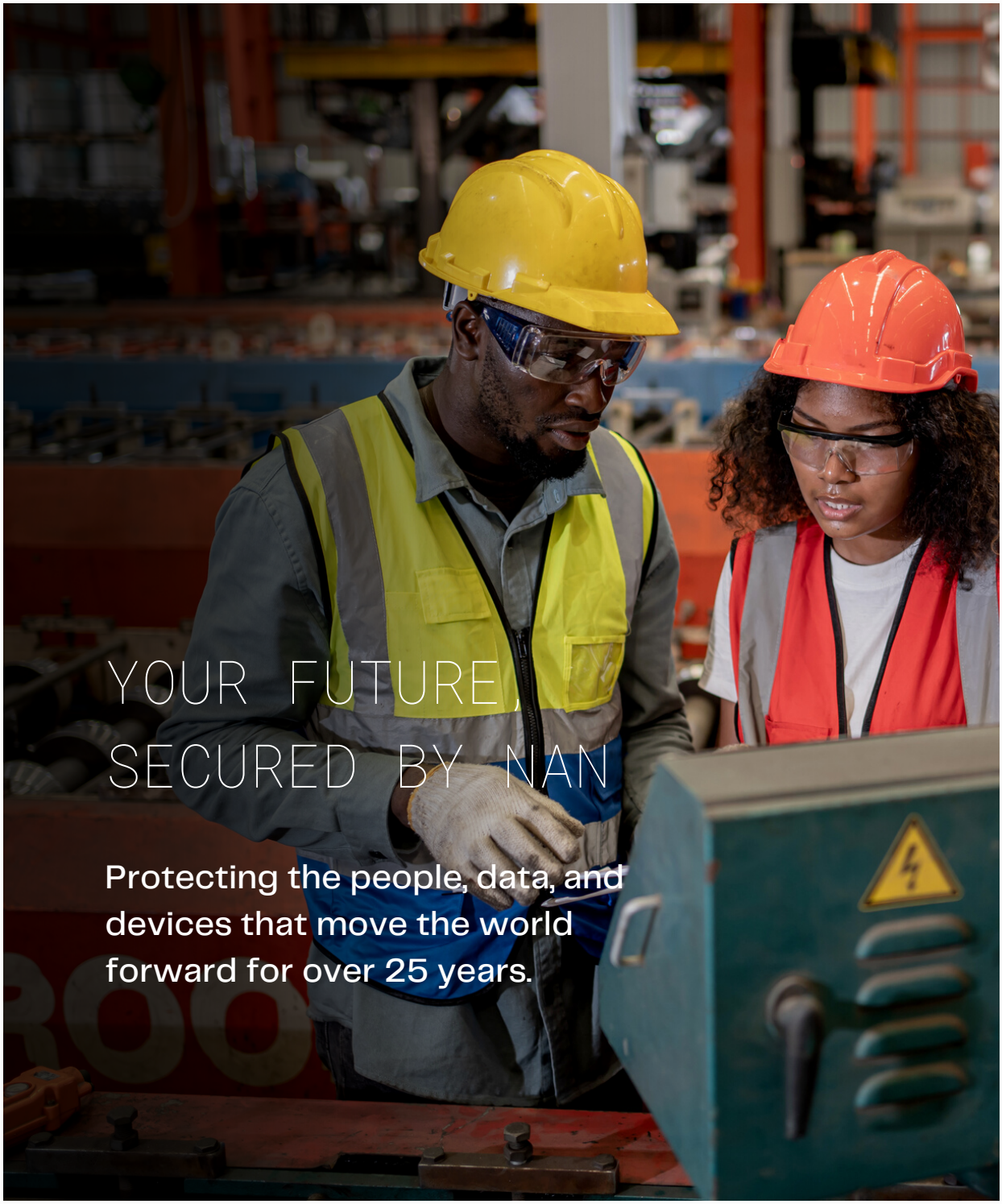
Therefore, we urge organizations to consider engaging with an MSSP to strengthen their security posture. By doing so, they can take advantage of the benefits of outsourced cybersecurity services and stay ahead of the ever-evolving threat landscape. With cyber attacks becoming more frequent and sophisticated, it is imperative that organizations take proactive steps to protect themselves, and partnering with an MSSP is an excellent way to achieve this goal.

Selecting the Right MSSP

Selecting the right partner is critical. With so many MSSPs in the market, it can be challenging to identify the best fit for an organization. When selecting an MSSP, businesses should look for the following:

- **Experience:** The MSSP should have extensive experience in providing cybersecurity services to organizations in your industry.
- **Service Offerings:** The MSSP should offer a range of services, including threat detection, vulnerability management, security device management, and incident response.
- **Expertise:** The MSSP should have highly trained security professionals with expertise in the latest threats and technologies.
- **Tailored Services:** The MSSP should be able to tailor its services to meet the specific needs of your organization.
- **24/7 Monitoring and Support:** The MSSP should provide round-the-clock monitoring and support to detect and respond to threats in real-time.
- **Cost-Effectiveness:** The MSSP's services should be cost-effective compared to building an in-house security team.
- **Service Level Agreements (SLAs):** The MSSP should offer SLAs that meet your organization's needs and define the level of service provided, including response times and the scope of services offered.
- **Compliance:** The MSSP should comply with relevant security standards and regulations, such as PCI, DSS, or HIPAA.
- **Track Record and Reputation:** The MSSP should have a strong track record of success and a positive reputation in the industry.
- **Communication:** The MSSP should have open communication channels to keep you informed of any security incidents and their response to them.
- **Flexibility:** The MSSP should be flexible and adaptable to changing security needs and requirements.
- **Partnership Approach:** The MSSP should take a partnership approach, working collaboratively with your organization to develop a customized security plan and ongoing security strategy.

NORTH ATLANTIC NETWORKS
YOUR CYBERSECURITY PARTNER



www.nan.com
16 Mason Ave., North Attleboro, MA 02760