



Fast and effective threat response

Identify, detect, and respond to attacks and threats in your network
with Onevinn MXDR, Microsoft Sentinel, and Microsoft 365 Defender



Contents

- 2 What is your security plan to defend against growing cyberthreats?
- 4 Bridge the cybersecurity skill gap
- 5 Proactively remediate vulnerabilities
- 6 Strengthen your security posture
- 7 Case study: Greenfood Group
- 8 Identify threats early and develop a real-time incident response

What is your security plan to defend against growing cyberthreats?

As attackers become more sophisticated, organizations need to strengthen their defenses

There's a reason why so many organizations are increasingly moving their operations to the cloud – digital transformation opens doors to new opportunities, from introducing greater agility to increasing scalability, productivity, and innovation. Unfortunately, though, the more we expand our digital perimeters, the harder it is to see and combat incoming attacks that seek to exploit our sprawling IT ecosystem.

95%

95% of surveyed cybersecurity professionals stated the cybersecurity skills shortage and its associated impacts have not improved over the past few years.¹

277

In 2022, it took an average of 277 days to identify and contain a breach.²

\$4.35M

The average cost of a data breach in 2022 was \$4.35 million.²

Onevinn's Managed Extended Detection and Response (MXDR) service helps companies shift from a reactive state of cybersecurity into a proactive state of security and protection. With the ever-evolving threat landscape, some attacks are unavoidable. But you can prepare your company to narrow the window of vulnerability with the combined support of security operations experts who are trained to manage and extend the Microsoft Security product portfolio. Onevinn is powered by Microsoft 365 Defender and Microsoft Sentinel, providing users with a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Take the offense – never be blindsided by a cyberattack again



Bridge the cybersecurity skill gap

Combat the cybersecurity skill shortage that is affecting most organizations today.

[LEARN MORE](#)

Proactively remediate vulnerabilities

Spot threats before they become a full-scale attack and remediate immediately.

[LEARN MORE](#)

Strengthen your security posture

Consolidate your tools with an integrated security platform and extend those capabilities for maximum protection.

[LEARN MORE](#)

Bridge the cybersecurity skill gap

Finally access the resources you need to fortify your security operations and introduce new skills to your IT team

There is a strong demand for cybersecurity professionals among US employers. Finding top-notch analysts with decades of experience is no easy task. Yet the evolution of cyberthreats clearly spells out a need for highly trained, knowledgeable resources. There must be a solution to the problem of finding the right personnel, budget, and time to act on critical incidents 24/7.

Onevinn MXDR offers a new way forward. Companies are invited to outsource the entire spectrum of security work to an external Security Operations Center – freeing up your IT team to focus on other challenges. The opportunity is twofold: Companies benefit from adding an additional human layer of skilled analysts to their IT team, doubling their resources and capacity to continuously detect and eliminate incoming cyberattacks. Then there is the additional advantage of integrating the Microsoft Security product portfolio with Onevinn MXDR services, creating the perfect symbiotic system that accelerates the time it takes to proactively identify and remediate any potential security gaps while taking appropriate measures to intrusions.

Onevinn + Microsoft

Onevinn's MXDR service is powered by the Microsoft 365 Defender product suite, a unified extended detection and response solution portfolio that integrates with Microsoft Sentinel. This integration gives both IT teams and Onevinn cybersecurity experts access to the advanced capabilities of Microsoft's cloud-native Security Information Event Manager (SIEM) and Security Orchestration Automated Response (SOAR). Intelligent security analytics and threat intelligence combine to simplify alert detection, threat visibility, proactive hunting, and threat response.



Proactively remediate vulnerabilities

Automate your incident response and address threats before they turn into full-blown attacks

Identifying and remediating every threat can be a time-consuming and daunting task – IT teams are already overwhelmed and understaffed. However, in the current threat landscape, being agile, vigilant, and constantly monitoring your IT environment is crucial to avoid data falling into the wrong hands.

Offload security pressure by letting an external party both manage the day-to-day threats and illuminate flaws in the security posture. Through smart and advanced technology, MXDR offers a much faster and more efficient incident response system compared to traditional security services. Onevinn adds even greater value by streamlining communications, introducing helpful cadences like monthly governance meetings where companies receive recommended lists of vulnerabilities that require immediate remediation for continued protection. Onevinn delivers a simplified and more reliable infrastructure as a service, creating a more integrated Microsoft Security platform that's easy to manage while enabling higher efficiency and smarter security.

Onevinn MXDR value add

- Continuous proactive monitoring and remediation from a trusted partner
- Expedient response time all hours and days of the year
- 24/7 experienced security analysts available, just one message away
- Threat hunting and automated detection with reduced noise
- Global threat intelligence and continuous monitoring of current trends and developments

Onevinn's Managed XDR Solution

Onevinn MDR a Microsoft Verified Managed XDR Solution Status

onevinn

Number one in intelligent security
Security Partner of the Year

Microsoft Intelligent Security Association



Strengthen your security posture

Speed isn't everything – be thorough in your threat investigation and adopt a holistic security strategy

There is too much noise in the threat landscape today and it can be difficult to determine what's real and what's not. In order to effectively address real threats, security teams need to sift out the false positives when addressing security alerts.

With Microsoft Sentinel, you can automate the process of consolidating threats. And then with the added human layer of Onevinn, you can extend that functionality – distill the noise even more and get to the bottom of each threat. Onevinn MXDR works with organizations to narrow the window of vulnerability. This is done through the detection and response capabilities of at-risk identities, endpoints, and threats. An MXDR solution helps reduce risk, vulnerability, and threat exposure through detection and response. Onevinn MXDR is operated 24/7 by a dedicated team of experienced cybersecurity analysts. The service contains adapted detection and response playbooks for accelerated containment against modern attacks and threats, ensuring your business, data, and assets are secured around the clock.

Continue to proactively remediate vulnerabilities with Onevinn MXDR

- 24/7 monitoring of your IT environment
- Rapid response to attacks
- Experienced and skilled analysts specializing in the Microsoft Security product portfolio
- A proactive delivery and working methodology for continuous security improvements

CASE STUDY

Greenfood Group

Situation

Greenfood Group is one of northern Europe's leading groups in healthy convenience food, employing around 1,500 people. The company is known for distributing fresh fruit, vegetables, and even a self-serve salad bar that elevates the convenience store experience. The salad bar, a much-loved add-on to the company, is almost an entirely separate component that goes by a different brand name: Picadeli.

Challenge

The digital processes that made the Picadeli salad bar so successful varied significantly from the other lines of business at Greenfood Group. Seeing how the differences impacted critical operations like managing supply chains, the IT department that was already using hybrid-connected cloud services and was familiar with DevSecOps-way of working saw an opportunity to extend Picadeli's technological maturity to other areas of the business. The IT manager already understood that an IT infrastructure is vital for convenience store products to get through the logistic chain on time. But he also knew he would need to introduce the right skillset to ensure that the implemented infrastructure is suitable to support fresh produce deliveries – especially because fresh products leave little room for production delays. To guarantee the success of updating internal systems, Greenfood sought to find an operating partner to audit and improve their existing IT operations.

Result

Onevinn are now fully integrated into Greenfood's security operations end-to-end, introducing the right security protocols and awareness needed to scale into the future. The company can ensure round-the-clock staffing to monitor security alarms, successfully defending against threats that could otherwise disrupt critical business processes and lead to production delays.

Solution

The collaboration to secure Greenfood's IT environment has unlocked a range of new services for implementation. Onevinn's MXDR services built on Microsoft Sentinel alongside Microsoft 365 Defender now monitor all Greenfood's clients, servers, networks, and cloud services.

Identify threats early and develop a real-time incident response

The current threat landscape is filled with bad actors and fast-moving attacks. It is critical for businesses to find solutions that are effective at protecting against these threats. With Onevinn MXDR and Microsoft Sentinel, organizations can shift from a reactive to a proactive state of security and defend against threats with a trusted partner and tools they already use.

**Find Onevinn on the Microsoft
Commercial Marketplace**

LEARN MORE

¹ Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment | ISSA

² Cost of a data breach 2022 | IBM



 Microsoft Security



onevinn