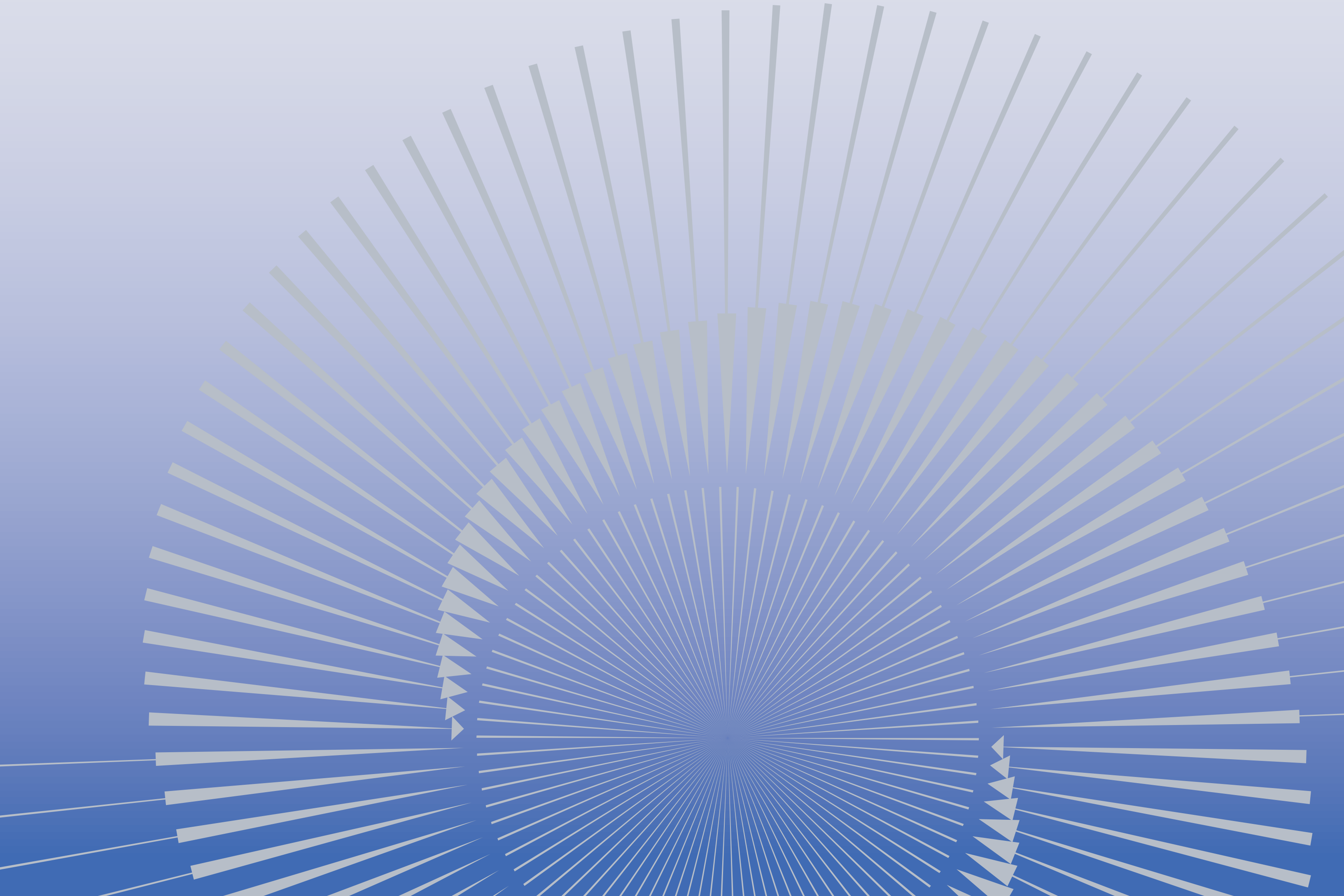
Reduce Risk & Build Cyber Resilience

Continuous security assessment, remediation and security posture improvement



Introduction

Reducing security risk is a challenge in the dynamic landscape of code changes, threats, and new vulnerabilities. New CVEs or zero-day attacks appear every day, so patch work is never fully complete. Microsoft and Synack joined forces to implement a Zero-Trust framework (“the program”) that prioritizes resilience. At a high level, Synack assesses cyber gaps, while Microsoft Security Enterprises Services addresses corresponding security posture improvements.

Synack’s premier on-demand security testing platform harnesses a talented, vetted community of security researchers and smart technology to deliver continuous penetration testing and vulnerability management, with actionable results. We are committed to making the world more secure by closing the cybersecurity skills gap, giving organizations on-demand access to the most trusted security researchers in the world.

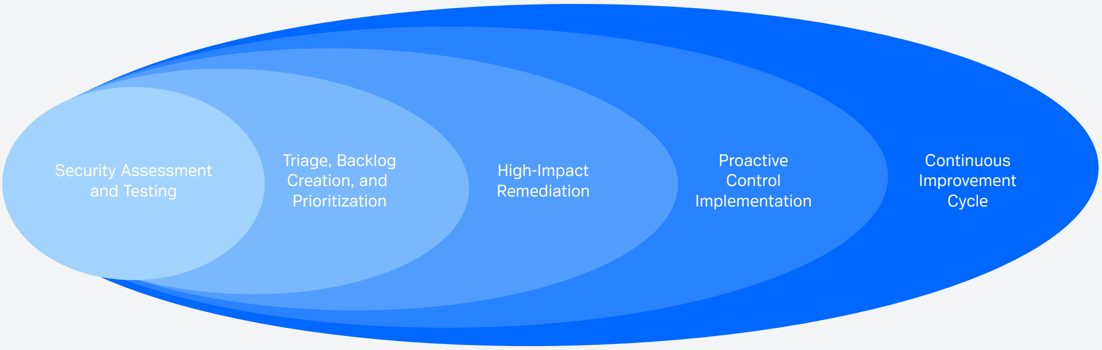
Microsoft Security Enterprise Services works with Microsoft’s most valued customers across the threat, regulatory, and security risk management landscape to strengthen and advance their security posture. Security Enterprise Services provides hands-on consulting services designed for customers that use Microsoft and other third-party security solutions, best practices, and know-how as they embrace modern security capabilities. Security Enterprise Services utilizes extensive cybersecurity knowledge and industry expertise gathered over decades to keep businesses secure.

Status Quo—Reactive

Traditional approaches to security testing, such as a yearly, compliance-driven penetration test, fall short because they fail to keep pace with the changing threat landscape. Meanwhile, automated scanning, while a useful tool for alerting to suspected vulnerabilities, does not specifically validate exploitable and actionable vulnerabilities present in a specific environment. Current testing methodologies often treat all assets the same despite varied levels of risk. Furthermore, note that compliance standards such as NIST 800-171 specify more proactive security assessments.

A Better Way—Proactive

A better and more agile approach supplements routine vulnerability scans with a human-driven continuous security assessment cycle throughout the year, to test for new vulnerabilities. These new vulnerabilities are then put into a work backlog to prioritize the remediation of critical vulnerabilities quickly. Root causes and patterns are analyzed for opportunities to put proactive controls in place, which improves the security posture because similar vulnerabilities are prevented from being exploited in the future. The result: strategic changes to operational process and tooling are implemented to build cyber resilience.


Security Assessment and Testing
Triage, Backlog Creation, and Prioritization
High-Impact Remediation
Proactive Control Implementation
Continuous Improvement Cycle

BUILDING CYBER RESILIENCE

Security Assessment & Testing

Baseline Current Risk Posture

At the start of each engagement, digital reconnaissance is conducted to establish a baseline and get an understanding of the state of cyber risk in the customer's environment. Automated scanning tools are deployed at this stage to identify suspected vulnerabilities and to identify assets which are candidates for in-depth security testing. The baseline phase is also when the maturity of security operations center (SOC) monitoring and processes are evaluated for improvement opportunities, such as leveraging security assessment results in development lifecycle workflows.

When following Microsoft's Zero Trust approach in conjunction with Synack's current risk posture assessment, Security Enterprise Services can help provide a modern cyber security strategy to support the organizational vision and mission statements and address the cyber security threat landscape. Microsoft can also help create a prioritized and actionable cyber security architecture roadmap and transformation plan that is derived from the cyber security strategy and aligned with the market trends and recommendations found by Synack.

Microsoft's Zero Trust Principles for Cyber Resilience + Synack

Verify Explicitly

- Always authenticate and authorize based on all available data points including user identity, location, device health, service or workload, data classification, and anomalies.
- Incorporate Synack testing to validate that authentication and authorization controls are deployed securely.
- Validate remediation of any discovered exploitable vulnerabilities.

Use Least-Privilege Access

- Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies and data protection to help secure both data and productivity. workloads
- Test for access/escalation exploits via Synack open vulnerability discovery and for specific attack vectors through Synack Missions.

Assume Breach

- Minimize blast radius and segment access.
- Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.
- Leverage the Synack Platform to perform authenticated and internal testing to identify and remediate security risks assuming environment compromise.

Test for Exploitable Vulnerabilities

Taking a thoughtful, proactive approach to security testing based on asset-level risk can help your organization craft a testing strategy that will keep it compliant and help the organization to properly manage risk across a growing attack surface. The spectrum of testing supported includes everything from Synack continuous open vulnerability discovery (OVD) to confirmation of which vulnerabilities are exploitable.

The key to confirming exploitable vulnerabilities is human-led testing. Traditionally, such testing has been performed by an internal red team or penetration testers brought on site once a year. Unfortunately, neither approach is nimble or scalable enough to meet the dynamic and constantly evolving threat landscape facing customers today, much of which is enabled by common IT solutions such as the adoption of cloud computing and artificial intelligence, plus other factors such as organized cyber-criminal networks.

Hiring security experts to meet unpredictable testing demands is impractical. Instead, the program provides on-demand access to a community of more than 1,500 expert security researchers (the Synack Red Team) who have been through a rigorous vetting process. Access to the program's global community of financially incentivized security researchers allows for diversity of thought and skills that improves assessment efficacy, allowing you to stay ahead of the latest threats. In addition, Security Enterprise Services offers highly skilled experts with extensive knowledge in a wide range of security services to provide long term cyber resilience, uniquely positioned with a modular, integrated, and agile approach to help you manage the information lifecycle and ensure legal discoverability.

Vulnerability Reporting

Traditional penetration testing reports are descriptions of what was done during testing, what was found and what might be done about it. Without responsive analytics and trend analysis, the report and analytics are useful for just a moment in time, lacking context of what happened before or since. Conversely, the program offers changes to your security testing methodology by centralizing and standardizing vulnerability reports and creating a flexible menu to improve test efficacy and leverage vulnerability data strategically.

Synack Reporting Includes:

- Dashboard at a glance, including new findings, status, patch verification and historical findings.
- Clear descriptions of found exploitable vulnerabilities, including statistics, steps to reproduce, screenshots and suggested remediations to patch.
- Each test comes with a human-written summary based on expert analysis of the testing data.
- Attacker Resistance Score quantifies and tracks cyber resilience over time. Organization and specific test scores change over time and are compared to key industries.

Triage, Backlog Creation and Prioritization

The program ensures that highlighted exploitable vulnerabilities are high impact and actionable to allow for quicker remediation. Synack triage eliminates duplicate or low quality submissions. The most critical vulnerabilities are captured and prioritized with the help of Security Enterprise Services consultants and architects. They are then documented in a DevOps backlog that will be used to track remediation activities. Unlike traditional vulnerability management, which can produce an overwhelming volume of alerts, the program's security assessments provide lower volume and higher value recommendations.

Root Cause Analysis

The program's reports go beyond identifying vulnerabilities by providing expert human analysis to advise on what caused the vulnerability in the first place. Exploitable vulnerabilities are identified, and Synack security researchers document the steps needed to reproduce the exploit. Knowing how something is exploited is part of a robust root cause analysis. Furthermore, Security Enterprise Services provides advanced threat hunting capabilities to validate Synack findings, actively looking for signs of real threat actor activity. The program correlates historical insights from across security assessments, and threat hunting, looking for trends and patterns that can optimize analysis utility.

High-Impact Remediation

The program's process of triage, root cause analysis, and prioritization targets the most important exploitable vulnerabilities for remediation on assets that are critical to the business.

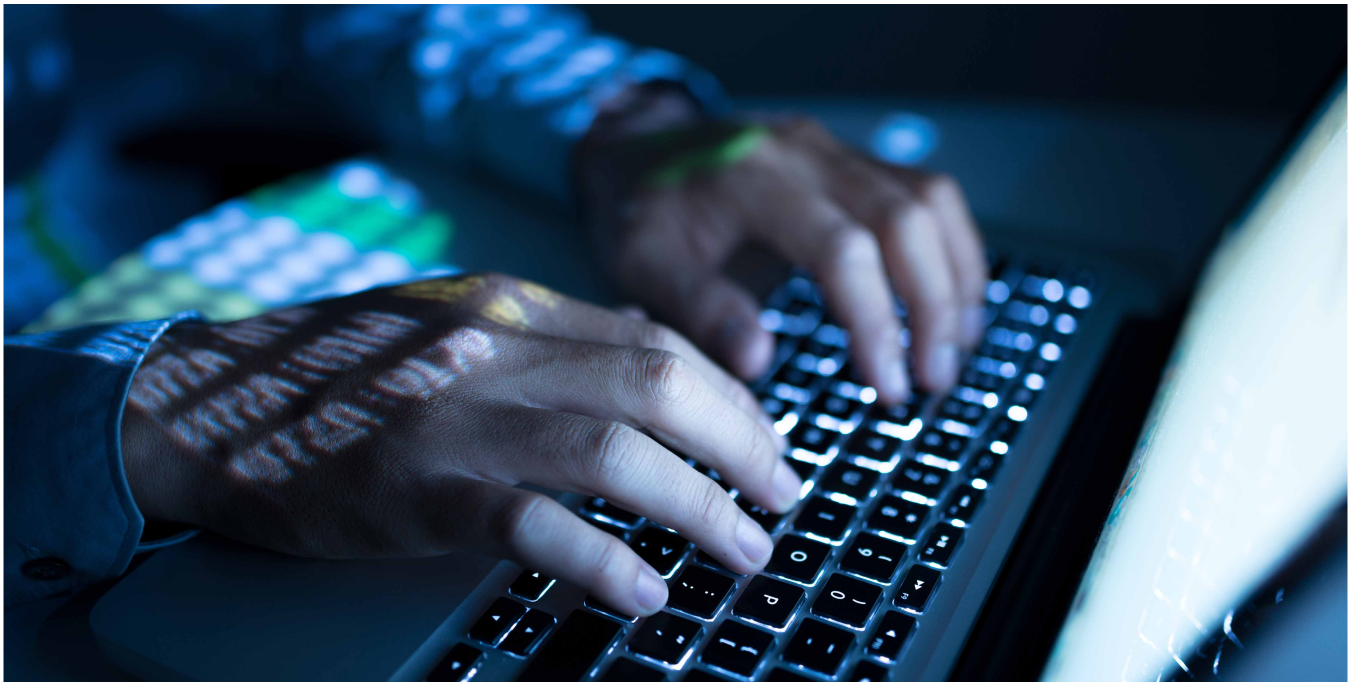
Provide Recommendations

Each Synack vulnerability report provides detailed recommendations about how to remediate the security gaps that allowed the vulnerability to be exploited by security researchers. Tooling recommendations are also provided to improve future detection and remediation efforts. Your team can then use these recommendations to close security gaps in your environment.

The combination of Microsoft Security Enterprise Services and Synack, helps solve business challenges—providing rapid, efficient technology adoption strategies with effective change management to help your organization thrive and grow.

Close Exploitable Security Gaps

There are many stories in the security world of organizations that are breached by previously identified vulnerabilities that were never addressed. One benefit of the program is that after Synack security researchers find exploitable vulnerabilities, Security Enterprise Services offers end-to-end security solutions that help enable customers to modernize and secure their digital estate including identities, data, applications, devices and across multi-cloud environments. Not only helping ensure recommendations are implemented but also proactively helping carry out security controls and prevent recurrence. This greatly reduces opportunities for bad actors to exploit vulnerabilities in the future.



Proactive Control Implementation

Patch Verification

Once recommendations to close security gaps are implemented, the security researchers re-test to verify that the patch was effective. If the security gap still exists, this information is communicated back, and the cycle is repeated until the vulnerability is no longer exploitable and security monitoring has been updated to reduce the risk of recurrence.

Improved Security Tooling

Security Enterprise Services leverages Synack test findings to help enterprises proactively optimize the operationalization of their Microsoft security stack. Exploitable vulnerability findings are integrated into your Microsoft security workflows and tools, reducing operational friction, improving responsiveness, reducing alert noise, and validating security posture. Security testing results from Synack inform enhanced detection in the Microsoft Sentinel and the Microsoft Defender suite, as well as inform improvements in Azure Policy, Patching Solutions, and other tooling.

Continuous Improvement

On-Going Strategic Testing

The program provides a transparent view of security assessment performance, including exploitable vulnerabilities, real-time analytics and testing history, as well as patch verification. Your continuous lifecycle is managed from discovery to remediation, helping your developers and security operations staff resolve issues earlier so that you can rest assured that your vulnerabilities are thoroughly addressed.

Extended Detection and Response with Microsoft Security

Extended Detection and Response (XDR) brings the entire lifecycle of threats together within one unified experience and set of capabilities—enabling your organization to prevent, protect, detect and respond to threats of all kinds across your entire digital estate—including email, endpoints, identities, cloud apps and workloads. By bringing all these signals together, we can enable capabilities that are otherwise impossible_such as a full unified view of entities, managed services support across domains, centralized vulnerability management that crosses security layers, advanced cross-product detection engines powered by global Threat Intelligence and more. Security Enterprise Services can help define the detections, drive policy configurations, and accelerate any vulnerability management and configuration changes.

Security Posture Trends

When done properly, security assessment can transform vulnerability management through both tactical and strategic methods. Tactically, exploitable vulnerabilities are fixed. Strategically, trends of root causes are identified and remediated across asset type and at scale. The program's reporting also allows you to track improvements in security posture over time.

With the program's security assessment portal, you can see security trends across vulnerabilities, allowing you to focus on the areas that need the most remediation. For example, one customer learned that 80% of vulnerabilities found in their applications and infrastructure were related to authentication. After they built an internal education program to retrain their teams on secure authentication, they cut their authentication vulnerability rate in half.

Proactive Risk Reduction

Synack continuous security assessment helps identify recurring risks that point-in-time testing fails to catch. This can be used to drive technical and process changes at an organizational level to mitigate future risk associated with similar vulnerabilities. Security Enterprise Services will create an actionable remediation roadmap to ensure high impact findings are fully understood, addressed and proactively prevented in the future.

Scaling Faster with Microsoft Security Enterprise Services + Synack

By harnessing the power of Microsoft's cloud and grounding our strategy in Zero Trust principles, we offer world class platform solutions and a world class team of security experts. with an end-to-end experience that empowers security teams to:

- Protect everything: Safeguard your entire organization with integrated security, compliance, and identity solutions built to work across platforms and cloud environments. We believe anything less than comprehensive security is no security at all. We secure devices, identities, apps, clouds—the fundamental fabric of our customers' lives—with the full scale of our comprehensive multi-cloud, multi-platform solutions.
- Simplify the complex: See the entire picture, prioritize the right risks, and remediate entire attack chains with a fully integrated toolset and strategic guidance created to increase the human expertise inside your company.
- Catch what others miss: Leading artificial intelligence (AI), automation, and expertise help you detect threats quickly, respond effectively, and fortify your security posture. Because you can't stop what you can't see. We have a unique outside-in and inside-out approach that helps customers scale faster.
- Grow your future: With the peace of mind that comes with a comprehensive security solution, you're free to grow, create, and innovate your business. We believe security should enable you to go further, quickly. And as we innovate products across all the markets and technology spaces that Microsoft is a part of, we're uniquely positioned to meet the security needs of the future. We know just how mission critical this work is—and we're your allies in this journey.

Embracing the Zero Trust philosophy of moving from assumption to explicit verification and that every element of your system can be breached, we provide a framework to manage the complexity of today's organization across the entire digital estate quicker, and to a scale that can only be provided from Microsoft Security Enterprise Services and Synack.

Improve Cyber Resilience

Agile reporting on vulnerability trends, success of risk mitigation strategies and the improvement of process and tooling is key to building cyber resilience. Continuous security assessment, remediation and posture improvement, offered by Microsoft in conjunction with Synack, achieves the goal of building cyber resilience and is a key component of a sound Zero Trust framework. Please contact us to learn more at microsoft@synack.com.