

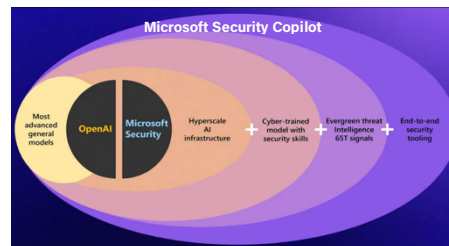
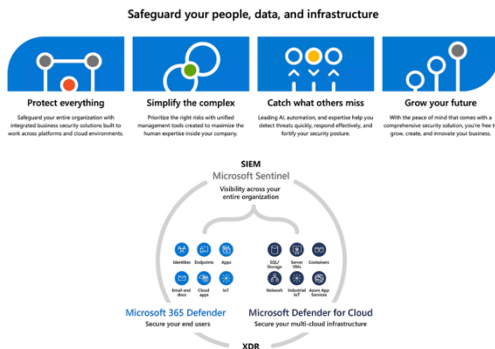
## Protecting a digitally connected workforce

Microsoft 365 is the cloud-first platform for all the ways people work today—whenever, wherever, however. Simply put, it's a better way to work.

Microsoft believe that energized, empowered employees are the key to a durable, competitive advantage for every organization. The Microsoft Work Trend Index shows that leaders today need to end productivity paranoia, embrace the fact that people come into the office for each other, and re-recruit everyone.<sup>1</sup>

### Protect your productivity

Microsoft continually develop technologies that prevent, detect, and respond to attacks with built-in unified experiences and end-to-end XDR and AI capabilities.



### Microsoft (and others) under the spotlight

March 2023, the Biden Administration released a new [National Cybersecurity Strategy](#); it puts more responsibility on private industry and tech firms to follow best security practices. Dig into the new document and you'll find that because the new strategy is only a policy document, it doesn't have the bite of law behind it. But that doesn't help organizations that need assurances that their operations can withstand the multiple cyber vectors deployed by cyber criminals in the pursuit of operational disruption and data compromise.

### Microsoft defending against never ending attacks

*"The cybersecurity threat landscape has never been more challenging or more complicated, costing the world \$6 Trillion annually", Satya Nadella, Microsoft Chairman and CEO <sup>2</sup>.*

Microsoft back-level support continues to be a major differentiator and advantage for businesses, but everyday Microsoft is [indirectly] in the news as cyber criminals continually innovate their attacks against the Microsoft platform. Recent **BlackLotus** (UEFI bootkit) deployments circumvent Secure Boot; **BlackMamba** key logging capability to steal sensitive information; **Remcos** bypasses Microsoft Windows's UAC security to deploy malware; **Web Servers Malicious URL Directory Traversal** allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server, as well as an ever increasing list of refreshed and new vectors. Microsoft relentlessly fights their customers cause with the regular Patch Tuesday which fix active zero-day vulnerabilities and flaws.

<sup>1</sup> [Hybrid Work Is Just Work. Are We Doing it Wrong?](#) Work Trend Index Pulse Report, WorkLab, Microsoft. September 22, 2022.

<sup>2</sup> <https://tinyurl.com/mszbp7y> - Satya Nadella, Chairman and CEO, Microsoft Secure March 28, 2023

## Value of Collaboration

Microsoft security offerings help drive organizations protection and response capability, but it is clear to see that the ingenuity of cyber criminals are managing to evade these defenses. Microsoft productivity, AI and Copilot platforms need to be supported with complementary “better together<sup>3</sup>” data and device solutions that protect before and during the successful evasion of security tools.






## NeuShield Strengthens Microsoft

Recognizing these unending attacks on businesses and individuals and embracing Satya Nadella’s strategy to adopt a Zero Trust architecture, NeuShield prioritized their efforts to protect all devices and data on Microsoft Windows Platform.

Seamlessly aligning to the Microsoft Security Copilot technologies that prevent, detect, and respond to attacks, NeuShield adds an additional level of cyber resilience not available from any other technology.

When Microsoft and other vendors security tools are bypassed, that organization is open to compromise and the cybercriminal will affect the maximum intended damage.

NeuShield Data Sentinel features such as Mirror-Shield™, Data Engrams™, One-Click Restore and Boot Protection prevent any cyber vector (known or unknown) from compromising data and mitigate the effects of data deletion. Equally critical, NeuShield ensures that the devices (servers and workstations) are secure and protected from zero day threats and malware intent on destroying operating system capability.

 <p><b>Mirror Shielding™</b></p> <p>Patented technology that adds a barrier to protected files preventing them from being modified. <b>Mirror Shielding™</b> makes an attacker believe they have access to a computer's original data files, but they are in fact only seeing a mirror image of them.</p>	 <p><b>Data Engrams™</b></p> <p>Leverages <b>Mirror Shielding™</b> to create copies of modified data at different points in time. <b>Data Engrams™</b> work like file revision history, allowing files to be restored to previous versions.</p>	 <p><b>One-Click Restore</b></p> <p>Restores operating system files and settings back to a known good state allowing you to quickly regain access to your computer after a ransomware attack. <b>One-Click Restore</b> also removes both known and unknown malware.</p>	 <p><b>Boot Protection</b></p> <p>Protects the boot portion of a drive to prevent aggressive types of ransomware from taking over the boot process and preventing applications from writing to the boot record.</p>	
--	--	--	--	--

## NeuShield delivers value without any dependency for traditional backups and network connectivity, ensuring recovery speeds are in minutes and hours, not days or months.

Data and devices can be critically dependent on many other technologies to deliver businesses operational agility. Where a cyber incident or internal oversight compromises Active Directory (AD), Domain Name Server(s) (DNS), backup & recovery catalogs, and Active SQL databases that are located on a Windows Server, these critical elements of infrastructure will be protected and experience the recovery speeds noted previously.

## Protecting Partnerships

Microsoft business ethos is about partnerships. Businesses agility has recognized the value of outsourcing the management and security of their Microsoft platforms via Managed Services and Security partners. NeuShield Data Sentinel allows these MSP/MSSPs to continually maintain their contractual service level agreements (SLAs), delivering an enhanced service that does not depreciate the existing value of Microsoft offerings.

NeuShield Data Sentinel Business & Datacenter Editions support all Microsoft cloud, on-premise and hybrid implementations as single and multi-tenant environments.

## System Requirements

OS: Windows 7, 8.1, 10, 11

OS: Windows Server 2008 R2, 2012, 2016, 2019, 2022

<sup>3</sup> <https://tinyurl.com/mszbp7y> - Charlie Bell, EVP Microsoft Security - Microsoft Secure March 28, 2023