Why Should Businesses Invest in Security?

Because they experience these common

Pain Points



Panic and Frustration from not knowing what to do in an event there is a cyber attack and its potential short-term and long-term impacts



Worried that a cyber attack would jeopardize the business and its reputation, which can cause damaged customer relationships and financial loss



Invasion of privacy of valuable and sensitive information about customers who have put trust in the organization



Overwhelmed with too much information about how to prevent cyberthreats



Stressed from the lack of inhouse cybersecurity skills and staffs



Fear of losing Intellectual Property, proprietary and personal information

Why Should Businesses Invest in Security?

Because they want to reap these desirable

Business Outcomes



Understand the cyber threat trends and best practices



Ensure your business continuity even after a cyber attack



Protect your reputation and instill trust in your customers



Optimally prepared (not over or under prepared) for potential cyberthreats in a proactive manner



Have qualified security
experts providing advice and
helping with security issues at
the tip of your fingers



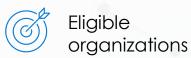
Detect if hackers have already compromised your environment



Threat Landscape Assessment









1 Week+

Business Outcome



Asses the current security state at the user and Microsoft 365 tenant level



Understand existing vulnerabilities and gaps



Prioritize security enhancement based on identified risks

Engagement Deliverables



Data ingestion & visualization of Microsoft 365 within ProServelT's Microsoft Sentinel workbook.



30-minute remote output review with ProServelT



Specific use cases scenarios developed



Complimentary Threat Landscape Assessment

A threat landscape assessment can be completed in days and will focus on 5 key areas of insight into your environment's cybersecurity.

01. Sign-In Information

Overview of successful and failed login attempts across the globe.

02. Dark Web Scan

The credentials or sensitive information that are sold or exposed.

03. Multi-Factor Authentication

Breakdown of MFA enabled and disabled accounts.

04. Spoof Protection

Attempts at impersonation targeting your organization.

05. Privileged Role Exposure

At-risk accounts with elevated permissions.

