

SECURE+

 Microsoft 365

ARO Technology.
Only better.

aro.tech | 0333 240 9880 | info@aro.tech

Introduction

Why Secure+

Getting your hands on Microsoft licenses is like opening a door to a world of possibilities—a toolkit packed with tools and services that run the show in your digital domain. But here's the thing: just buying the licenses is where it all begins. It's like having a massive library of resources, loaded with features that can rev up efficiency, beef up security, and spark innovation in your setup. Yet, these licenses hold more potential than meets the eye, waiting for you to explore and make the most of them.

See, it's not about the purchase; it's about what happens next. It's about diving in, figuring out what these licenses can truly do for you. It's tweaking, fine-tuning, and tapping into the real power packed into your Microsoft investment. It's not a one-off deal—it's about using them smartly, making the most of every feature, and uncovering the multitude of opportunities waiting within your Microsoft setup.



What is Secure+

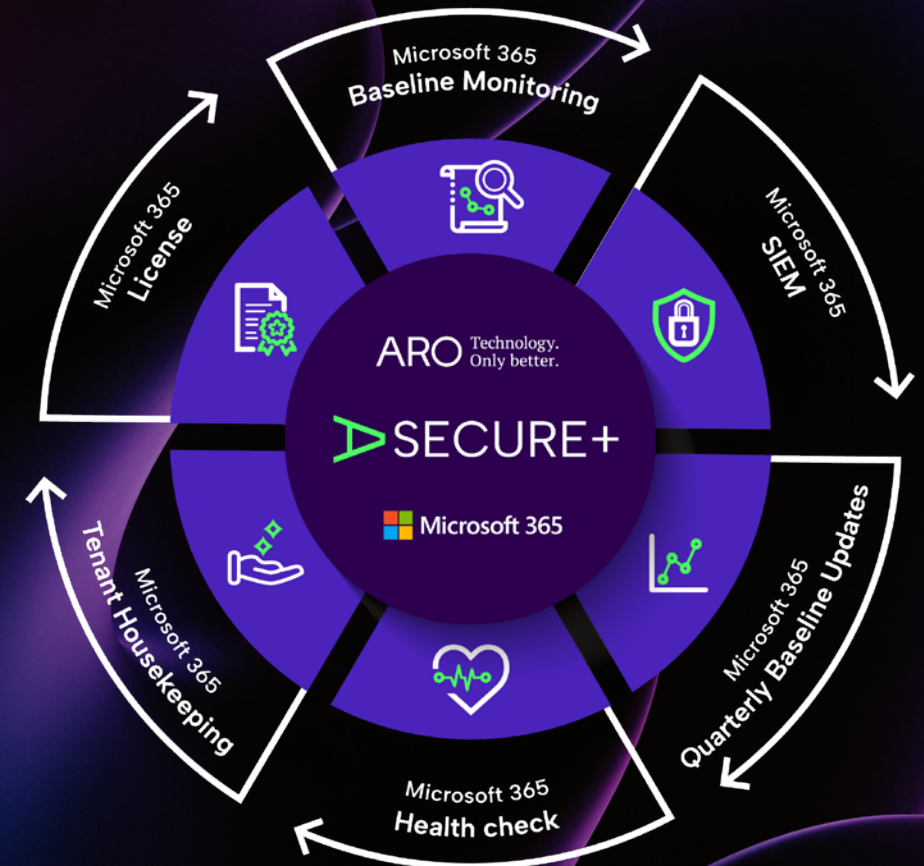
Secure+ represents a holistic approach to safeguarding and enhancing your Microsoft environment through a suite of interconnected services.

After an initial audit, Secure+ covers six essential elements:

- 01 Quarterly Baseline Updates
- 02 Baseline Monitoring
- 03 Security Information and Event Management (SIEM)
- 04 Health Check
- 05 Tenant Housekeeping
- 06 License Management

Secure+ offers a proactive and comprehensive solution.

It ensures continuous monitoring of configurations, optimisation of licenses, regular health assessments, and vigilant security oversight. By embracing Secure+, organisations benefit from a strategic blend of proactive measures and meticulous management, fortifying their Microsoft landscape against vulnerabilities, ensuring compliance, optimising cost and fostering a resilient digital infrastructure for sustained operational excellence.



Audit

Think of the first step in the Secure+ journey as a thorough check-up, using powerful Microsoft tools to examine configurations and security posture.

The audit provides a Secure Score across Identity, Device Security, Data Security, Application Security and an overall position, with the aim of achieving as close to 100% as possible.

We have ourselves recently surveyed 500 companies across these criteria, many of whom assumed their environment was up to date and well managed. The results opposite aren't comfortable reading.

We would be delighted to carry out the audit for your company with no charge. Even if Secure+ is not the right product for you, it will certainly flag up areas to focus on internally.

The number of companies, out of the 500, achieving below **50%** secure score in each category:

313 / 500 Companies had a **Total Secure Score** below 50%

212 / 500 Companies had an **Identity Secure Score** below 50%

466 / 500 Companies had a **Device Security Secure Score** below 50%

448 / 500 Companies had a **Data Security Secure Score** below 50%

449 / 500 Companies had an **Application Security Secure Score** below 50%

69% of businesses
do not apply software
security updates within
the recommended 14 days

Source: The 2023 Cyber Security
Breaches Survey, gov.uk

...But we've got
you covered.

 SECURE+

01

Baseline Updates



Quarterly Baseline Updates represent a strategic approach to maintaining the robustness, security, and efficiency of your Microsoft environment.

In essence, these updates encompass a scheduled and systematic process of reviewing and implementing foundational configurations and settings within your systems and applications every quarter.

The digital landscape constantly evolves, introducing new security threats, performance enhancements, and operational efficiencies. Quarterly Baseline Updates are designed to keep your Microsoft environment aligned with these advancements. They encompass essential updates to configurations, policies, and settings, ensuring they remain in sync with the latest best practices and security protocols.

By adhering to a regular quarterly update cycle, your systems are fortified against emerging threats, equipped with the latest security patches, and optimised for performance. This proactive approach minimizes vulnerabilities, mitigates

risks, and ensures that your Microsoft environment operates at its most secure and efficient state.

In summary, Quarterly Baseline Updates serve as a proactive measure, aligning your Microsoft environment with the latest industry standards and security protocols. By staying current with these updates, you ensure that your systems are fortified, optimised, and resilient, providing a stable and secure foundation for your organisation's digital operations.

Examples

- Review your current configuration and continually improve the security posture of your environment to reduce internal and external threats through implementing good defensive mechanisms.
- Ensures you deploy newly released methods to protect your users/devices and data within a reasonable timeframe after release.
- Uncover configurations that don't comply with industry standards or regulatory requirements, that would otherwise pose a compliance risk.

Only **1 in 3** security breaches are identified by a business' own security team or tools

Source: The 2023 Cyber Security Breaches Survey, gov.uk

...But we've got you covered.

 SECURE+

02

Baseline Monitoring

Baseline monitoring serves as the backbone for maintaining the optimal security, and compliance of your Microsoft 365 environment. Essentially, it establishes a benchmark—a reference point—for the ideal configuration and behaviour within your Microsoft 365 environment.

The monitoring continuously observes and evaluates your Microsoft 365 environment against this established baseline. It scrutinises key parameters, settings, and configurations, identifying any deviations or anomalies from the standard expected configuration.

By meticulously tracking these configurations, baseline monitoring ensures that your Microsoft 365 environment consistently operates within predefined parameters. It acts as an early warning system, promptly detecting any drifts from the established norms, thereby enabling swift corrective actions to maintain operational efficiency, security, and compliance.

In essence, baseline monitoring becomes your proactive guardian, tirelessly watching over your systems, anticipating potential issues, and allowing for proactive adjustments to ensure your Microsoft 365 environment operates at its peak, delivering optimal security.

Examples

- Detects that Microsoft 365 configurations have drifted from the predefined standards, potentially due to manual changes or unauthorised modifications
- Detects what Microsoft 365 configurations have drifted from the predefined standards, potentially due to IT System admin changes, either authorised or unauthorised.
- Identify missing security updates and service packs across Microsoft software installed on your system, allowing you to prioritize and apply necessary patches.



79% of businesses
do not have formal
incident response
processes



...But we've got
you covered.

 SECURE+

Source: The 2023 Cyber Security
Breaches Survey gov.uk

Customers who introduce a zero trust security approach with solutions such as Secure+ Reduced the number of security and IAM-related help desk calls by **50%**

Source: The Total Economic Impact™ Of Zero Trust Solutions From Microsoft



03

SIEM

Think of SIEM as a vigilant guard that tirelessly watches over your network, applications, and systems, collecting and scrutinising vast amounts of security-related data in real-time. This includes logs, alerts, and events generated by various users, devices and applications across your Microsoft 365 ecosystem.

By consolidating this wealth of information into a centralised platform, SIEM enables our security team to detect and respond to potential threats swiftly. It identifies suspicious patterns, anomalies, or potential breaches by correlating data from multiple sources, providing a comprehensive view of your security posture. SIEM then leverages Machine Learning (ML) and Artificial Intelligence (AI) to learn from past incidents, further strengthening your organization's security measures.

SIEM doesn't just stop at detection; it empowers your team with actionable insights and automated responses. It assists in streamlining incident response, facilitating compliance adherence, and bolstering your organisation's resilience against cyber threats.

In essence, SIEM acts as an intelligent guardian, offering a panoramic view of your Microsoft 365 security landscape and enabling proactive measures to safeguard your Microsoft 365 environment. It's a vital tool in the arsenal against cyber threats, ensuring that your organisation's digital assets remain protected, compliant, and resilient in the face of evolving security challenges.

Examples

- Detects multiple failed login attempts originating from an unfamiliar IP address trying to access sensitive Microsoft 365 accounts.
- Identifies a sudden and abnormal transfer of a large volume of files from an internal Microsoft SharePoint site to an external location.
- Assists with incident response activities through providing the incident response team with a vast amount of information relating to sign-in logs and access logs.

Your logs are
showing activity in
Russia but you've
got no users there...

...We've got
you covered.

 SECURE+

Health Check

Microsoft Health Check is an ongoing, comprehensive evaluation and diagnostic process designed to assess the overall health, performance, and security of your Microsoft 365 environment. It serves as a proactive measure to ensure that your environment and configurations are optimised and operating at their peak efficiency and security.

This evaluation involves a systematic analysis of various facets of your Microsoft 365 ecosystem, including security settings, and configurations. The goal is to identify potential vulnerabilities, inefficiencies, or areas that require improvement within your environment.

Meticulously compiled and comprehensive reports are presented monthly, illustrating the overall health of the Microsoft 365 ecosystem and adopted services, including, identity security, device security, application security and data security, ensuring that everything is operating as expected.

Consistent monitoring of the health status of the Microsoft 365 tenant ensures ongoing visibility into the wider environment, allowing for the timely identification and resolution of any identified issues or non-compliance.

Regular monitoring of the Microsoft 365 adoption score helps to maximise return on investment, further increase utilisation of unadopted Microsoft 365 services, and inform future IT strategies and roadmaps.

62% of businesses spend up to 7 hours tracking and analysing regulatory compliance developments each week, highlighting a need for automated reporting

Source: 2023 Cost of Compliance
Thomson Reuters



The average
time to contain
an insider threat
incident is
85 days



...But we've got
you covered.

 SECURE+

Source: 2022 Cost of Insider Threats
Global Report, Ponemon Institute

05

Tenant Housekeeping



Tenant Housekeeping is the meticulous maintenance and organisation of your Microsoft 365 Identities, configurations and settings. It involves the ongoing management for stale users and devices within your Microsoft 365 tenancy.

Much like maintaining a clutter-free and well-organised physical workspace, Tenant Housekeeping ensures your digital 'tenant' remains efficient, optimised, and secure. This process involves regular checks and actions to tidy up and streamline your Microsoft 365 environment, removing redundant, outdated, or unnecessary users and devices and associated assets where applicable.

By conducting routine housekeeping tasks, such as, removing redundant accounts, inactive devices or legacy configurations, Tenant Housekeeping ensures that your Microsoft 365 tenancy operates smoothly. This not only enhances performance but also contributes to security by minimising potential vulnerabilities stemming from neglected or outdated user accounts, devices or configurations.

In essence, Tenant Housekeeping acts as a custodian for your digital space, maintaining order, efficiency, and security within your Microsoft 365 tenancy. By regularly cleaning these items, ensuring an optimised digital workspace for your organisation's smooth operations.

Examples

- Identifies several user accounts that have been inactive for an extended period, indicating unused or abandoned accounts.
- Identifies devices that have been inactive for an extended period, indicating unused or abandoned devices.
- Identifies configurations that have been superseded within your Microsoft 365 tenant and removing/replacing them as necessary.

54% of Microsoft 365
licenses are inactive,
underutilised, oversized
or unassigned

...But we've got
you covered.

 SECURE+

Source: Global Office 365 Report:
License Optimization, CoreView

06

License Management

Microsoft 365 License Management is the systematic oversight and optimisation of your organisation's Microsoft 365 licenses. It involves the strategic monitoring and notification of these licenses to ensure cost efficiency, compliance, and optimal utilisation across your Microsoft 365 environment.

54% of Microsoft 365 licenses are inactive, underutilised, oversized or unassigned. Moreover, nearly 60% of organisations reportedly overspend on software licenses, either by purchasing more licenses than needed or acquiring licenses with features that surpass their actual requirements.

Effective Microsoft 365 License Management aims to mitigate these challenges by conducting regular audits, aligning licenses with actual usage patterns, and by informing you of the optimal license allocation based on organisational needs. It involves tracking license usage, identifying inactive or underutilised licenses, and reallocating resources to maximise value and reduce unnecessary expenses.

In summary, Microsoft 365 License Management is a strategic approach that helps organisations optimise their investment in Microsoft software, ensuring that licenses are aligned with actual usage, costs are minimised, and compliance is maintained within the dynamic landscape of software licensing so that you can procure the correct number of licenses upon your renewal date.

Examples

- Detects a significant number of Microsoft 365 licenses that have remained unused or underutilised for an extended period.
- Highlights instances where departments or individuals are subscribed to Microsoft 365 plans that exceed their actual requirements, leading to unnecessary expenditure.
- Identifies instances where certain users or departments are using Microsoft software beyond the terms specified in the license agreement, potentially violating compliance regulations.



The Ongoing Journey

Secure+ isn't just a final stop; it's an ongoing commitment. It's about staying alert and evolving alongside the ever-changing digital world. With Microsoft's features growing and cyber threats always shifting, Secure+ is there as your guardian, adapting and keeping watch over your Microsoft setup. It's not just a one-time deal; it's a promise to constantly shield and strengthen your system. Think of it as an ongoing journey—a continuous effort towards building a better, stronger Microsoft environment that grows and evolves with your needs.

With Secure+, your journey towards a fortified, optimised Microsoft environment isn't a destination—it's an ongoing pursuit of excellence, driven for you by ARO, one of the UK's leading Microsoft Centres of Excellence.

Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Data & AI
Azure



➤ BOOK YOUR AUDIT NOW



Cloud

Microsoft and Cloud Services

Office 365, Dynamics, Power Platform, Teams

Hybrid Cloud Infrastructure

Full Hybrid Capabilities, Public, Private, Hyper Converged

Next Generation Networking

Campus and DC, large scale indoor/outdoor

IPAM, Network access, WAN, LAN

Backup and Protection

Immutable, Offsite, Data Replication, DR

Cyber Security

Next Generation Firewalls, DDI Security, SIEM, SOC



Collaboration

Unified Communications

Unified Communications
In-house Mitel Cloud platform
In-house Microsoft Teams Cloud Voice Platform

Contact Centre

Full AI and workforce management options

Business Mobiles

ISP for O2 and Vodafone, Strategic Partner for EE

Connectivity

Broadband, Leased Line, SD-WAN

SIP and Business Voice

AV and Meeting Room Solutions



Data Centre Services

Public and Private Sector

Private Cloud
SaaS
TRE
Secure Storage / Retrieval
Managed Data Centre Services
Managed Connectivity
Managed Firewalls
24/7 Operations Centre
Co-Managed Services
WAN Design and Implementation



Sustainability

Net Zero Journey

Carbon and consumption reduction plan to Net-Zero

POD Energy and Carbon Management Software

In house, bespoke reporting portal and EMS

Energy Procurement and Tenders

Independent tender driven purchasing for fixed or flexible energy trading solutions

Energy Optimisation

Consultancy to help optimise facility consumption

Energy Compliance

Assistance with government energy legislation

Total Account Management

All aspects of daily energy management

ARO Technology. Only better.

Your enterprise performance partner for Cloud, Collaboration,
Data Centre Services and Sustainability

aro.tech

0333 240 9880

info@aro.tech

