M365 + E5 Security

What is Baseline Security Plus?

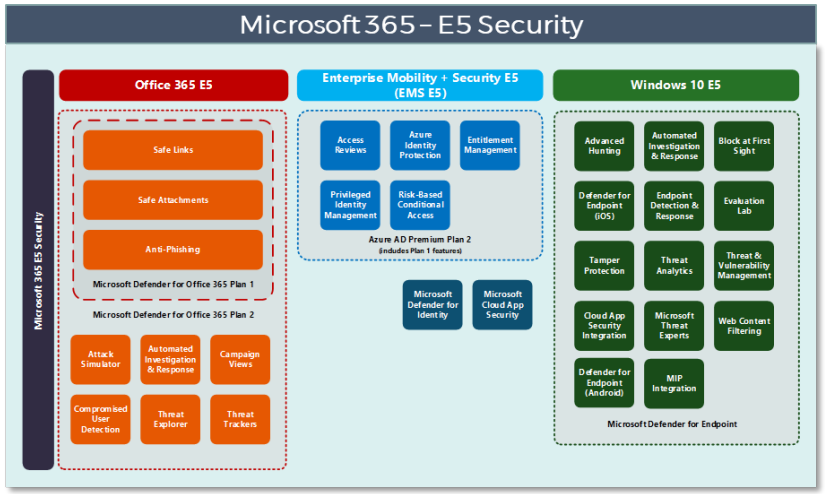
baseline
SOLUTIONS BY IT RELATION

What is
Baseline Security Plus

Baseline Security Plus enables you to protect your organization against more advanced attack with adaptive, built-in intelligence.

It is done by using products from the Microsoft 365 E5 Security bundle which contains several services which all have the common goal to protect against more advanced threats, compromised identities and malicious actions in both cloud-only and hybrid environments.

The common factor of all E5 features is that they use threat intelligence, machine learning and/or behavior analysis to create a more dynamic defense.



Products

- Azure Active Directory Premium P2
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Cloud App Security
- Microsoft Defender for Office 365 P2
- Password Filter

Integrated with ITR SOC

ITRelation

Why?
Microsoft 365 E5 Security

The key factor to implement Microsoft 365 E5 Security is *to create a more dynamic and self-protecting environment, across endpoint, identities and data to close gaps and mitigate risks.*

A really important factor regarding Microsoft 365 E5 Security is that all services work together to close gaps and ensure protection both across your on-premises and cloud environments.

This is for example by:

- *Protecting endpoints by using Microsoft Threat Intelligence and advanced security features to protect against more advanced attacks and harmful websites.*
- *Adding advanced identity protection by using behavior analysis and Microsoft Threat Intelligence to secure access and identities based on risks.*
- *Locate, get insight and block the usage of shadow IT and wrong data placement by using features from Cloud App Security & Microsoft Defender for Endpoint.*
- Implementing intelligent identity security based on risks and reputation - via Azure AD Premium & Microsoft Defender for Identity.

baseline
SOLUTIONS BY IT RELATION

Why Baseline Security?

Summary

Baseline Security Plus
Highlights

- ✓ Ensure an acceptable level of security based on known and integrated products.
- ✓ Continuous development and optimization based on changes in products and the overall threat picture.
- ✓ Focus on that users, devices and data, not only lives up to, but also maintain the desired level of security.
- ✓ Reporting based on current data.
- ✓ Monitoring and alerting based on security events identified by Microsoft Behavioral Analysis and Threat Intelligence.