

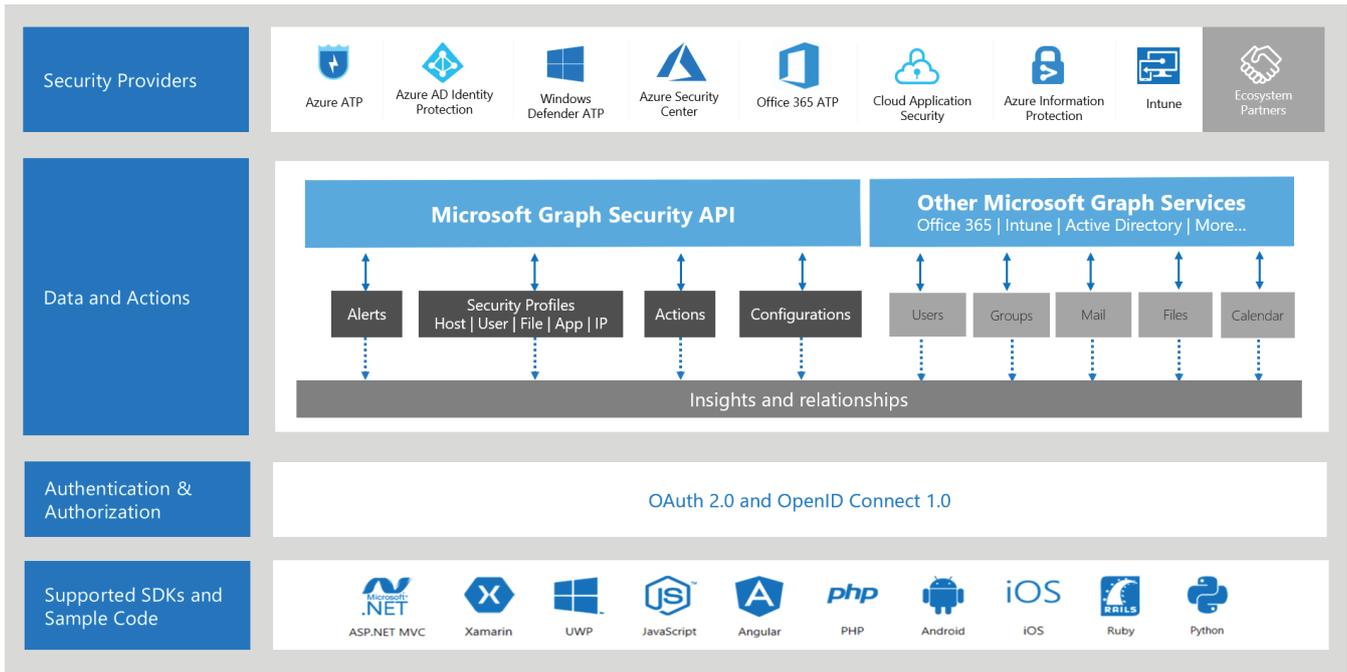


# Microsoft Managed Security Service

# HPT MANAGED SECURITY MONITORING SERVICE

Today, many security monitoring and alerting solutions deployed in network environment consume the big cost of license but only have efficiency when the organization has a skilled and experienced security monitoring team. Therefore, optimal equipping with security monitoring solution, effective self-operation and self-monitoring, with minimized cost are always impossible investment solution for organizations nowadays. For that reason, HPT provides Managed Security Monitoring Service (MSMS) to help organizations not only meet the Management - Safety - Cost criteria, but also catch up with the effective and necessary trend of investment in information security.

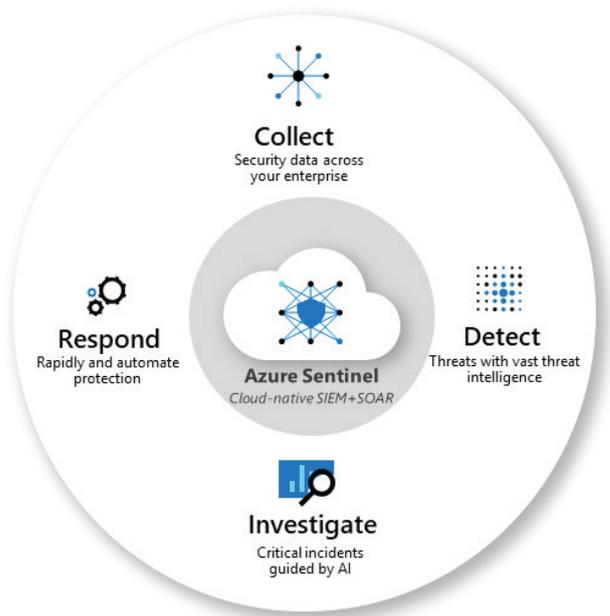
**HPT Managed Security Monitoring Service (MSMS)** designed and operated on the basis of Microsoft Graph that is the gateway to data and intelligence in Microsoft 365. It provides a unified programmability model that you can use to access the tremendous amount of data in Office 365, Windows 10, and Enterprise Mobility + Security. Use the wealth of data in Microsoft Graph to build apps for organizations and consumers that interact with millions of users.

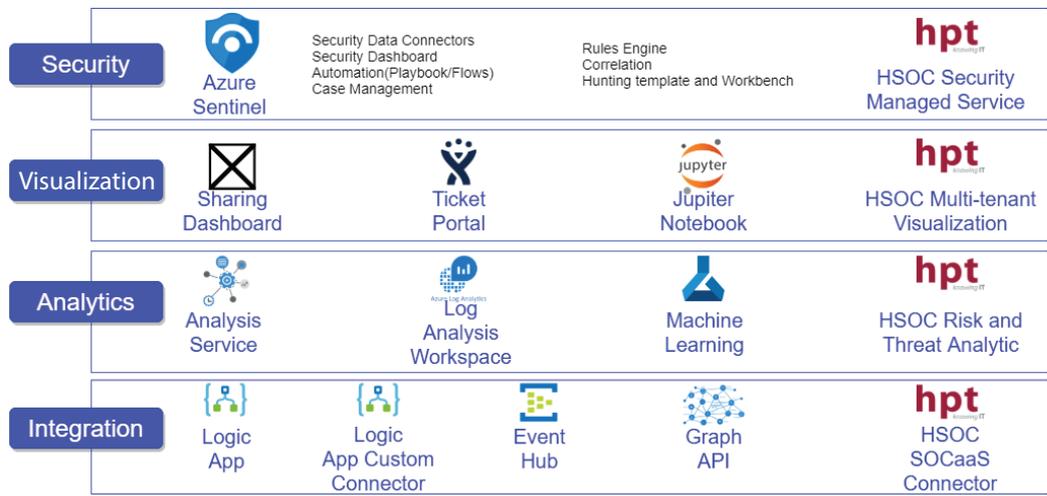


## Managed Security Information & Event Monitoring

Building protective cloud security measures to stop threats before they disrupt your business, and quickly detecting and responding to new threats, are the HPT SOC mission. With years of experience building and managing SIEMs, HPT recognizes that Azure Sentinel addresses many of the issues that plague traditional SIEMs – cost and time associated with deploying hardware or virtual data collection appliances, speed of connectivity to security logs and visibility into risk and threats across multi-cloud and hybrid environments. Sentinel provides efficient data queries, built-in analytics and strong security orchestration automation and response (SOAR) engine.

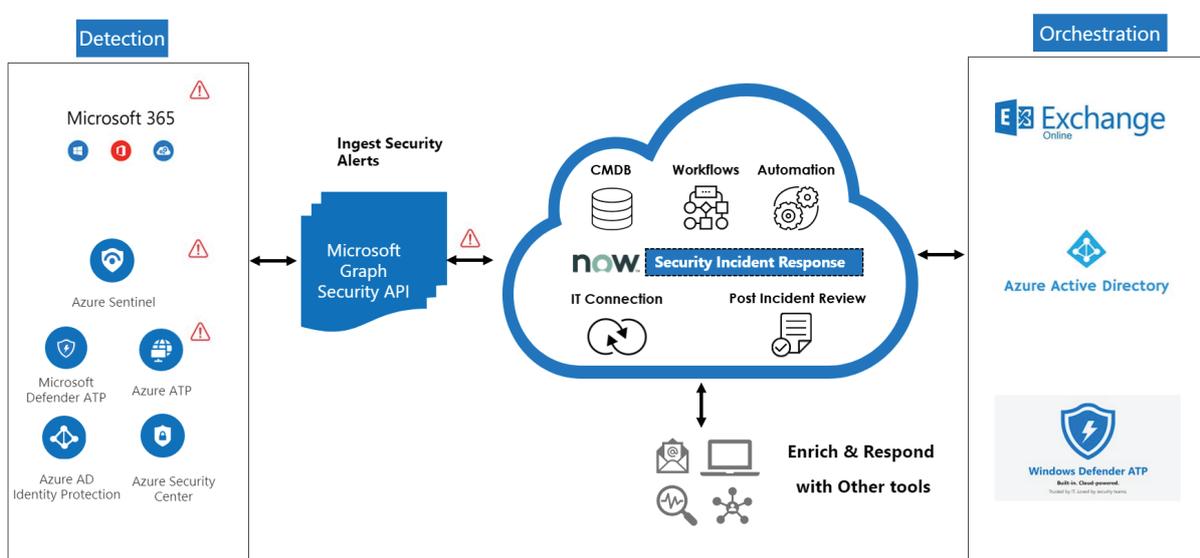
Azure Sentinel is a cloud-native SIEM platform that aggregates data from multiple sources, including users, applications, servers and devices running on-premises or in any cloud, letting you analyze millions of records in a few seconds. Azure Sentinel includes built-in connectors for easily onboarding of popular security solutions and can collect data from any source using open standards like CEF and Syslog.





Azure Sentinel is your view across the enterprise and HSOC's team of cloud security experts will be there each step of the way to design, configure and optimize Sentinel for your environment. We also offer the custom playbooks for detection and response automatically:

- Handling Ransomware/Crypto Locker Infection.
- Unauthorized Domain Admin Access.
- Handling Malware Infection.
- Remediating Website Defacement.
- Multiple Simultaneous Logins.



## **BENEFITS:**

Managed Security Monitoring Service becomes a trend of enterprise in security investment while threats are increasing, and security self-defense is still not effective. There are clear benefits associated with cyber security outsourcing as proposed to handle the challenges:

- Bring simplicity and convenience in deployment, flexibility in expanding the scope of monitoring by integration of extended security services.
- Reduce investment costs for information security experts
- Ensure 24x7 system monitoring, help to detect early and mitigate security risks
- Enhance system security based on recommendations

## **WHAT WE WORK**

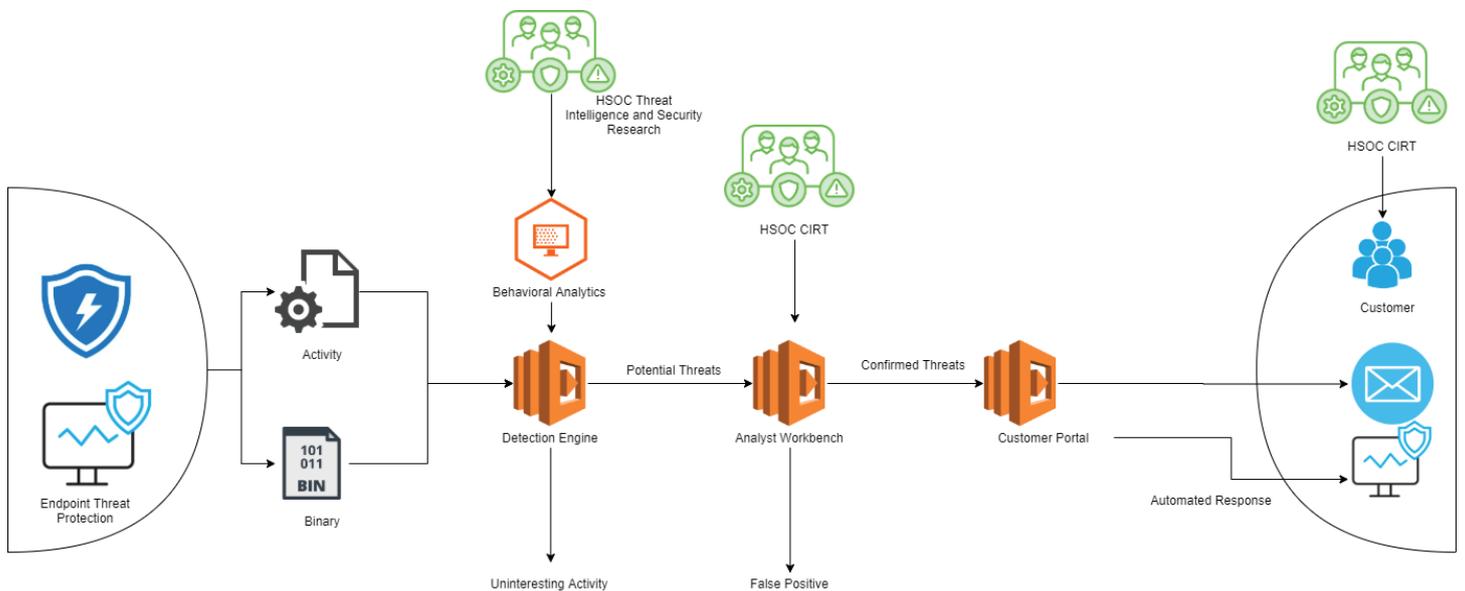
- HPT provides the Azure Sentinel (remote site or standalone implementation) deployed inside the customer's system which is responsible for collecting and processing log and necessary data from servers, devices, and applications ... related to information security
- Event log of customer is monitored and can be forwarded to the HPT Security Operations Center (SOC) via secured communication channel.
- Security experts conduct 24x7 monitoring with automated tools and professional experience and notify customer right away when any issues occur
- Periodic report (weekly, monthly) or incident report on information security of customers' environment along with recommendations and instructions to protect and enhance information security

## Microsoft Defender ATP



Management and APIs

Microsoft Threat Protection



### BENEFITS:

Managed Endpoint Detection & Response as an extension of your team, you'll improve security overnight and reduce risk over time. There are clear benefits associated with cyber security outsourcing as proposed to handle the challenges:

- Bring simplicity and convenience in deployment, flexibility in expanding the scope of monitoring by integration of extended security services.
- Reduce investment costs for information security experts
- Ensure 24x7 system monitoring, help to detect early and mitigate security risks
- Enhance system security based on recommendations

### WHAT WE WORK

- HPT provides the EDR software deployed on customer's endpoints (workstations or servers) inside the customer's system which is responsible for detecting, alerting and processing data in those endpoints related to information security
- The service helps customer to protect well-known malware and exploitations in the endpoints.
- Security experts conduct 24x7 monitoring with automated tools and professional experience which reduces false positively and detects unknown threats.
- Periodic report (weekly, monthly) or incident report on information security of customers' environment along with recommendations and instructions to protect and enhance information security

## Microsoft 365 Security Managed Service

Microsoft 365 offers customers like you new ways to proactively protect and monitor the security of your intellectual property and customer data, Microsoft 365 Security Managed Service enables you to effectively respond to security incidents and realize the full benefits and return on your Microsoft 365 security investments as an end-to-end service, our experts provide design, implementation and ongoing monitoring and management through design, deploy, protect, detect and respond covering all three main security pillars of Identity and Access Management, Threat Protection and Device Protection.

Included in our service is our Security Operations Center (SOC). The SOC continually monitors, investigates and responds to security alerts from your environment enabling your security team to respond faster and more efficiently to threats and security incidents.



### **BENEFITS:**

If you're looking for guidance on how to build a robust and reliable security solution for your organization, let us help you to protect your Microsoft 365 environment continuously. There are clear benefits associated with cyber security outsourcing as proposed to handle the challenges:

- Bring simplicity and convenience in deployment, flexibility in expanding the scope of monitoring by integration of extended security services.
- Reduce investment costs for information security experts
- Ensure 24x7 system monitoring, help to detect early and mitigate security risks
- Enhance system security based on recommendations

### **WHAT WE WORK**

- Proactive monitoring and alerts for Microsoft 365 environment.
- Based on security policies and security best practices, the service configures Microsoft 365 tenants to the optimal level of security.
- The service is easy to implement, continuously monitors security settings and automatically corrects misconfigurations.
- Prevent identity theft with effective password and authentication policies.
- Prevent data leakage, Managed Security 365 informs you when a user is sending spam.
- Periodic report (weekly, monthly) or incident report on information security of customers' environment along with recommendations and instructions to protect and enhance information security.

## Continual Improvement

### Hardening and Optimizing Security Baselines

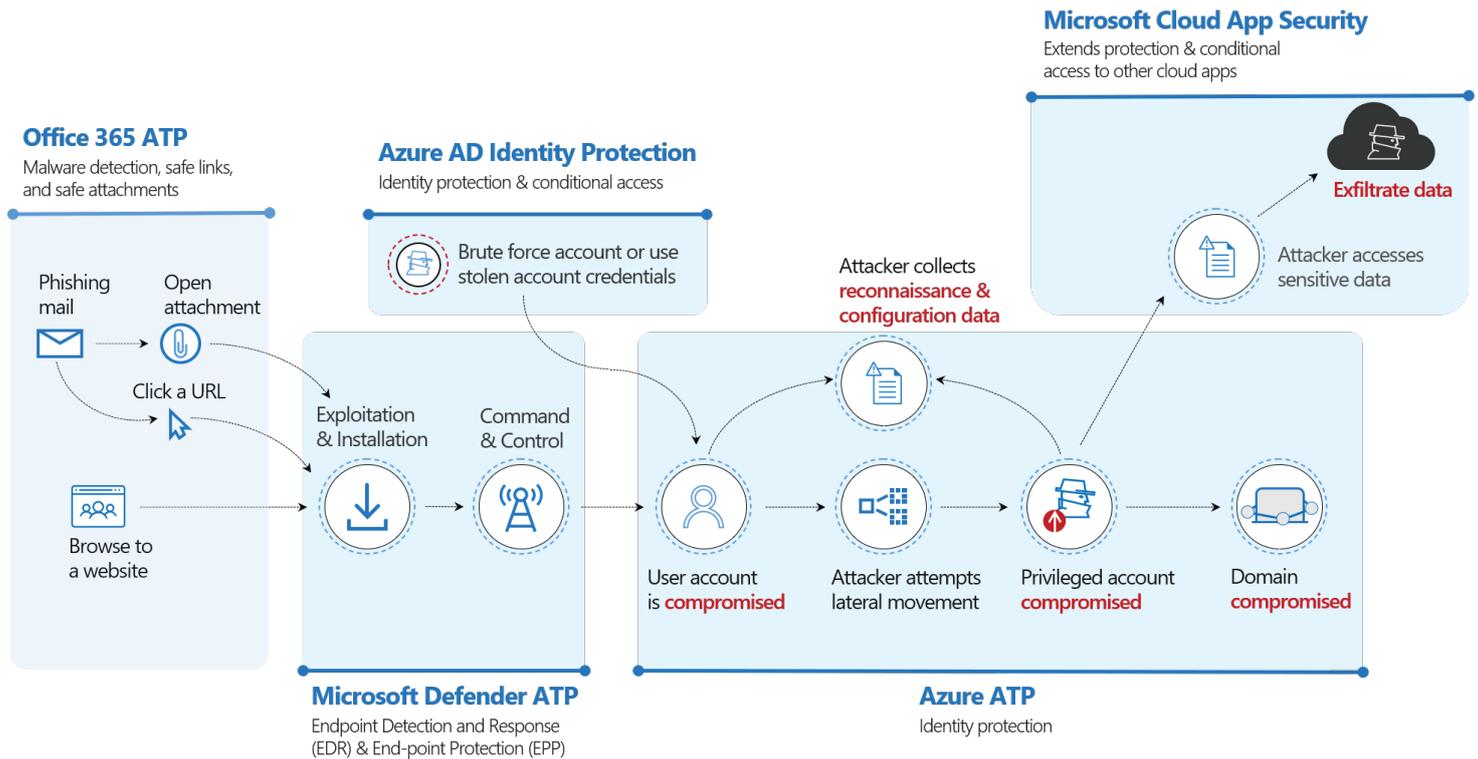
Every organization faces security threats. However, the types of security threats that are of most concern to one organization can be completely different from another organization. For example, an e-commerce company may focus on protecting its Internet-facing web apps, while a hospital may focus on protecting confidential patient information. The one thing that all organizations have in common is a need to keep their apps and devices secure. These devices must be compliant with the security standards (or security baselines) defined by the organization.

Security baselines are pre-configured groups of configuration settings that explain their security impact, help organizations apply a known group of settings and default values. Security baselines can help you to have an end-to-end secure workflow when working with Microsoft 365. Some of the benefits include:

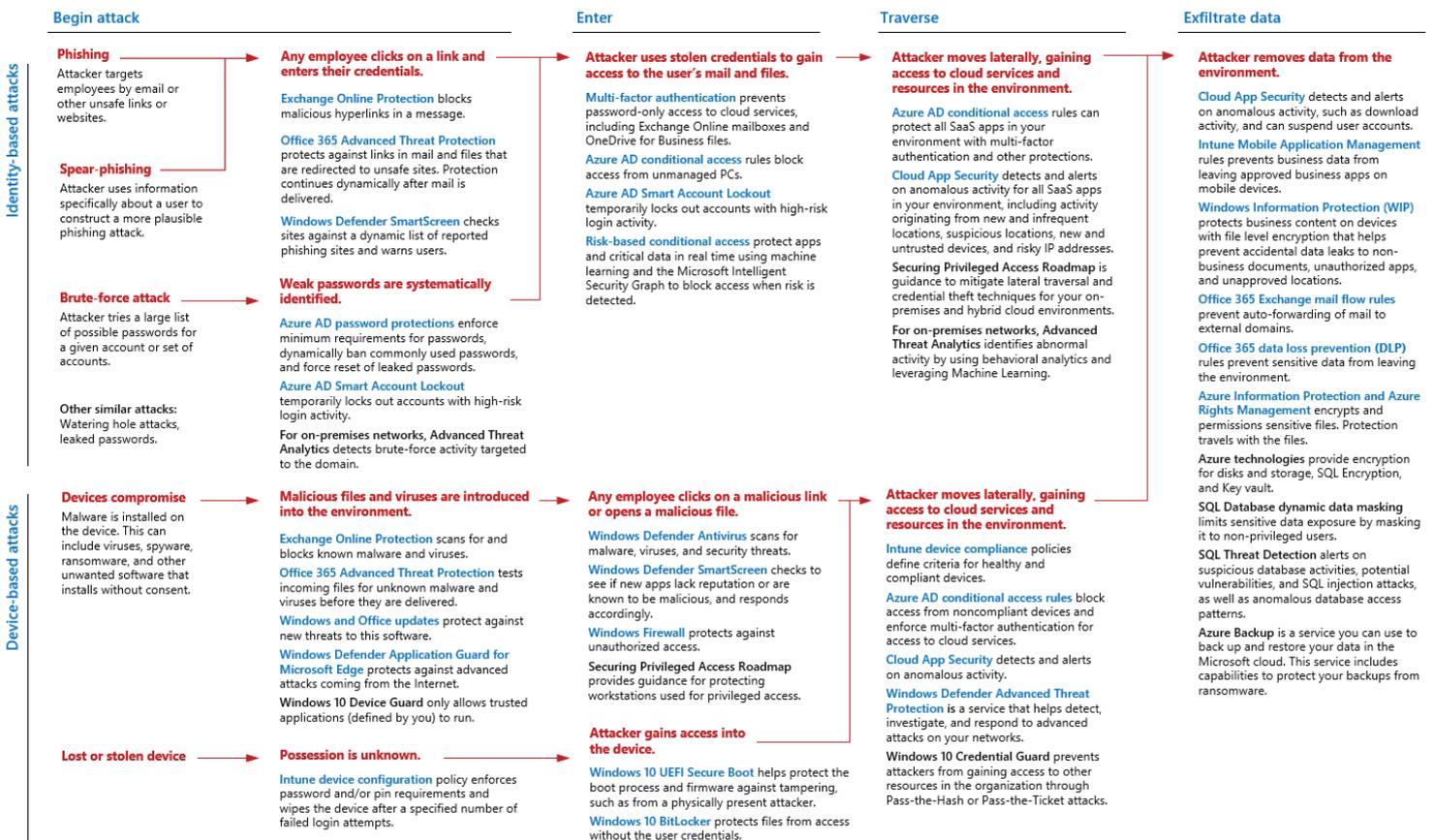
- A security baseline includes the best practices and recommendations on settings that impact security.
- The baselines are designed for well-managed, security-conscious organizations in which standard end users do not have administrative rights.



# How Microsoft solutions protect your organization?



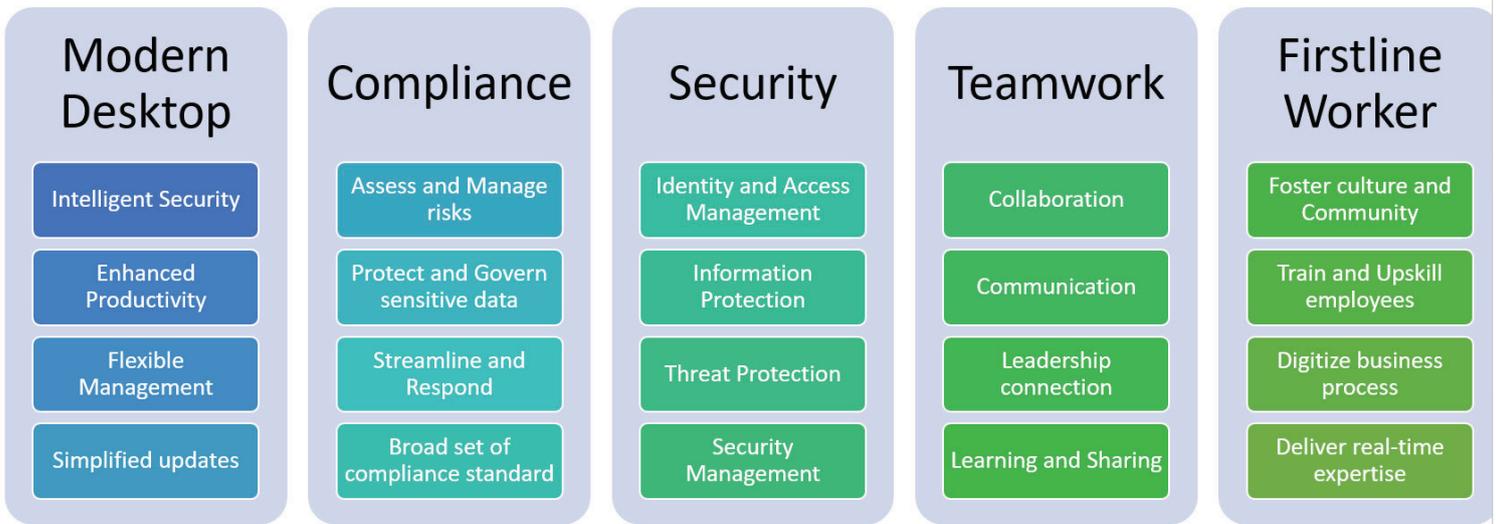
## Protect across kill chain



## Common attacks and Microsoft capabilities

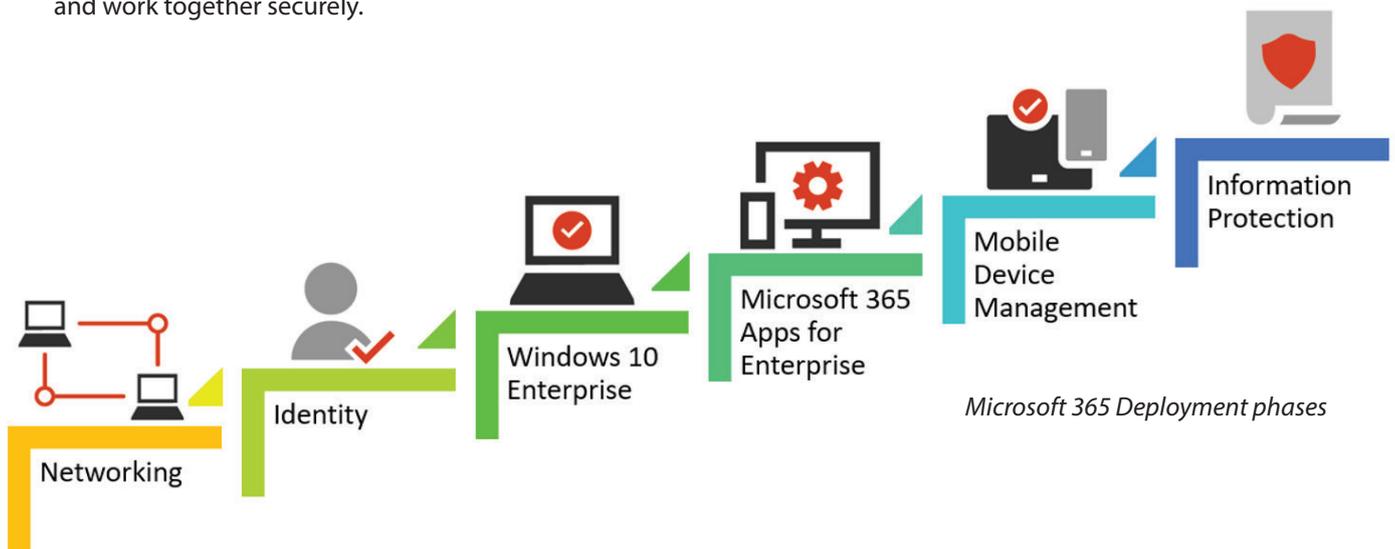
## Microsoft Modern Workplace deployment phases

Microsoft Modern Workplace consists of 5 pillars:

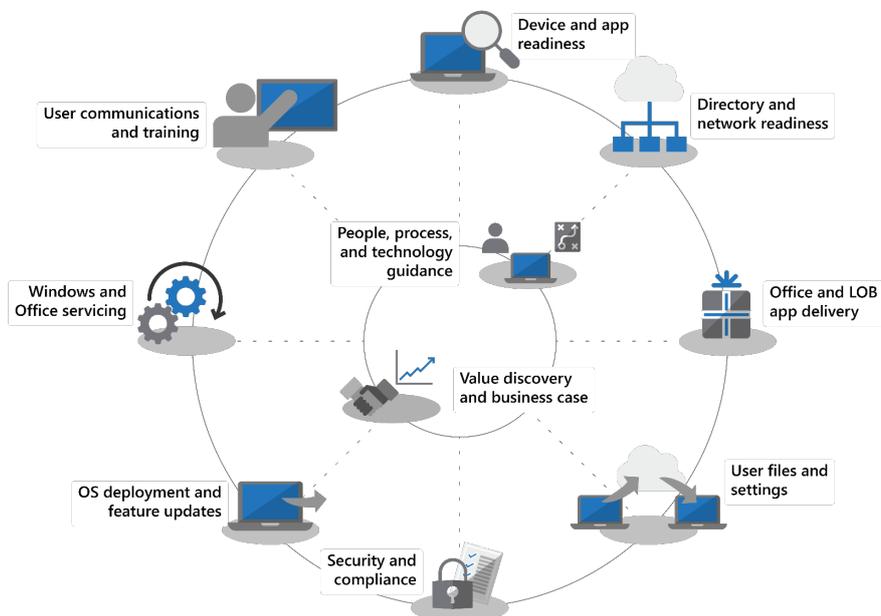


## Microsoft 365 Deployment Phases

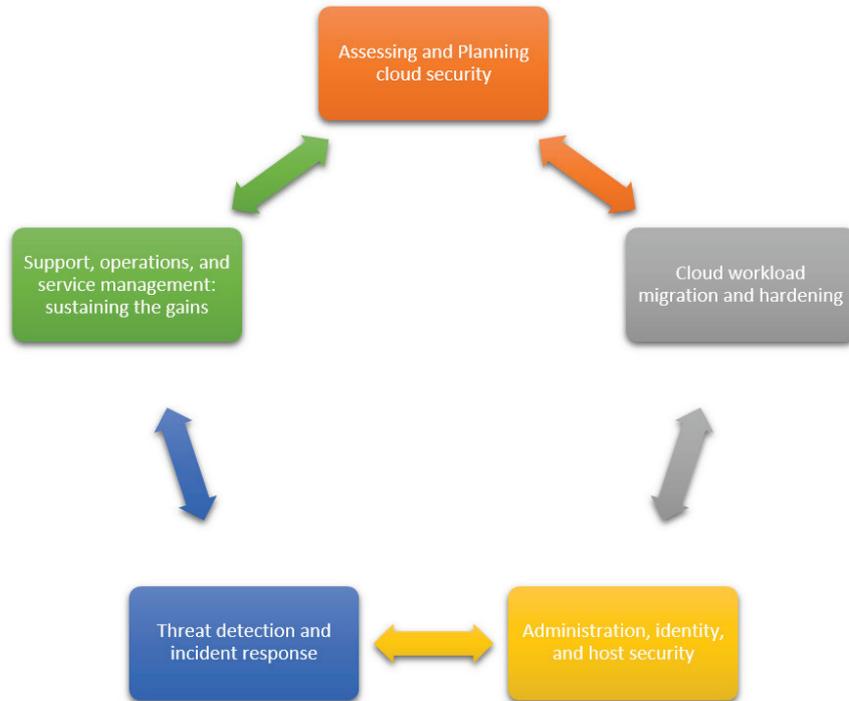
Microsoft 365 for enterprise is a complete and intelligent solution that empowers everyone to be creative and work together securely.



## Desktop Deployment Process Wheel



# How can HPT services help organizations?



## Where to start?

HPT recommends starting with a view of your entire organization and addressing your top risks first:

- Assess your cloud security position to get a broad view of the road ahead.
- Enable advanced threat detection.
- Address top risks — protect business-critical social accounts and cloud administrative privileges accounts with hardened workstations and security tailored to those roles.

## Why HPT?

HPT has 25 years of experience in providing IT Services in Vietnam, consistently delivering business value through our professions, commitments and devotion.

Understanding security challenges of enterprises, HPT invested in IT Security for over 10 years.

Our expert security team offer both Managed Security Services and Security Services tailored for specific business needs.

### Certificates & Awards:

- High level international security qualification: CISSP, LPT, CEH, ECSA, EMAPT,....
- International Security Contest participation: Top 10 Hack in The box Singapore, Top 2 Mates CTF,...
- SOC Certificates: CSA, ECIH
- Cloud Solution Provider 1-Tier
- Microsoft Gold Partner
- National System Integrator (NSI)
- Microsoft Outstanding performance
- Microsoft Country Partner of The Year 2015, 2017

### **HPT is referred by customers and trusted organizations:**

## Contact us:

For further information on HPT Cyber-Security Services or discussion, please contact:

### **CYBER SECURITY CENTER – HPT VIETNAM CORPORATION**

Lot E2a-3, D1 St., Saigon High Tech Park, Long Thanh My Ward, Dist.9, HCMC, Vietnam

📞 (+84) 2854 123 400

✉️ [hsoc@hpt.vn](mailto:hsoc@hpt.vn)

🌐 [www.hpt.vn](http://www.hpt.vn)