MICROSOFT 365 PREMIUM + EMAIL & IDENTITY SECURITY PLATFORM

ALL I.T

CONTACT US ⊹

RISKY USER MONITORING

At All IT, we monitor Microsoft account logins 24/7. If a login is flagged as risky based on our security parameters, we assess and take action, including blocking access when necessary.

Risky logins can be triggered by several factors, such as:

LOCATION
A user consistently logs in from one location, but an impossible travel event is detected (e.g., a login from another country within minutes).

VPN
A login attempt is made from an unknown VPN.

PROGRAM
A login occurs using an unfamiliar program that the user has not previously used.

When a risky login is detected, we immediately block user access, then reach out to verify the activity. If the login is determined to be malicious, we reset the account and change passwords.

GEO-BLOCKING

By default, we block logins from outside a user's nominated country. If you need to travel, we can make temporary exceptions to maintain access while keeping security intact. This significantly reduces exposure to threat actors.

HUNTRESS MANAGED IDENTITY THREAT DETECTION & RESPONSE (ITDR)

Huntress provides 24/7 monitoring for Microsoft 365 user accounts, detecting and responding to:

- **Session hijacking (which can bypass multi-factor authentication)**
- **Credential theft**
- **Malicious inbox and forwarding rule manipulations**
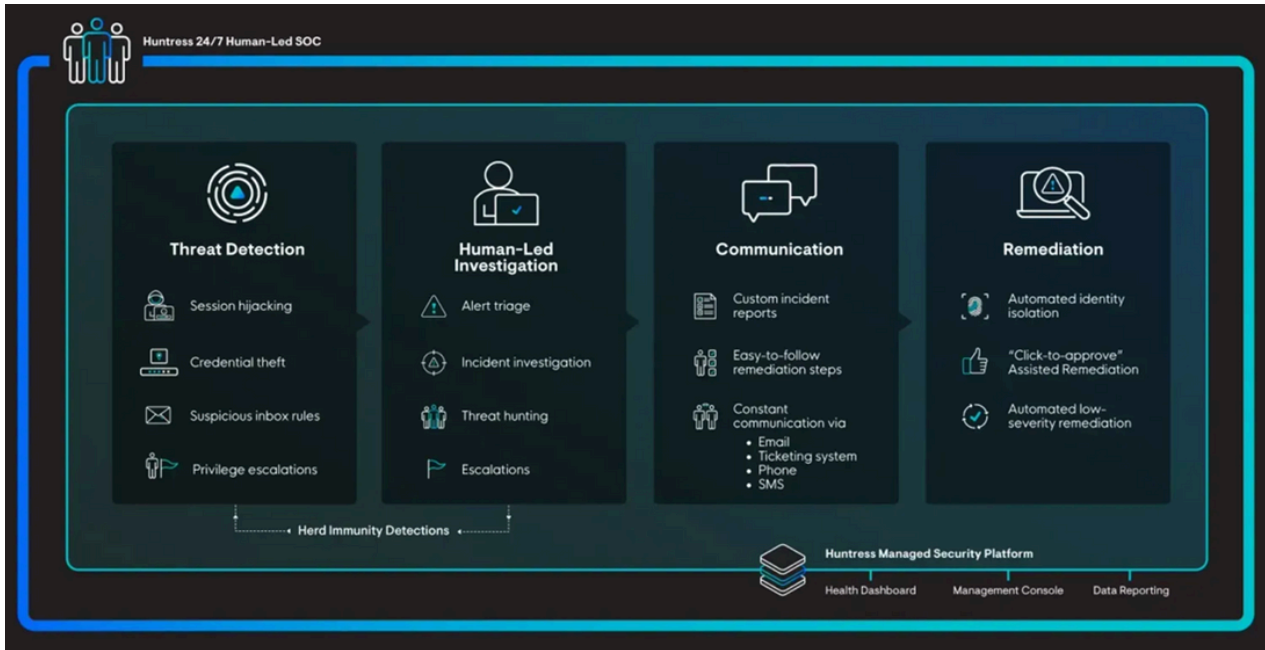- **Account takeover and business email compromise (BEC) attempts**

If a high-risk threat is detected, our team will immediately block the user account until remediation is complete.

MICROSOFT 365 PREMIUM + EMAIL & IDENTITY SECURITY PLATFORM

ALL I.T

CONTACT US

Huntress 24/7 Human-Led SOC

Threat Detection
- Session hijacking
- Credential theft
- Suspicious inbox rules
- Privilege escalations

Human-Led Investigation
- Alert triage
- Incident investigation
- Threat hunting
- Escalations

Communication
- Custom incident reports
- Easy-to-follow remediation steps
- Constant communication via
  - Email
  - Ticketing system
  - Phone
  - SMS

Remediation
- Automated identity isolation
- "Click-to-approve" Assisted Remediation
- Automated low-severity remediation

← Herd Immunity Detections →

Huntress Managed Security Platform
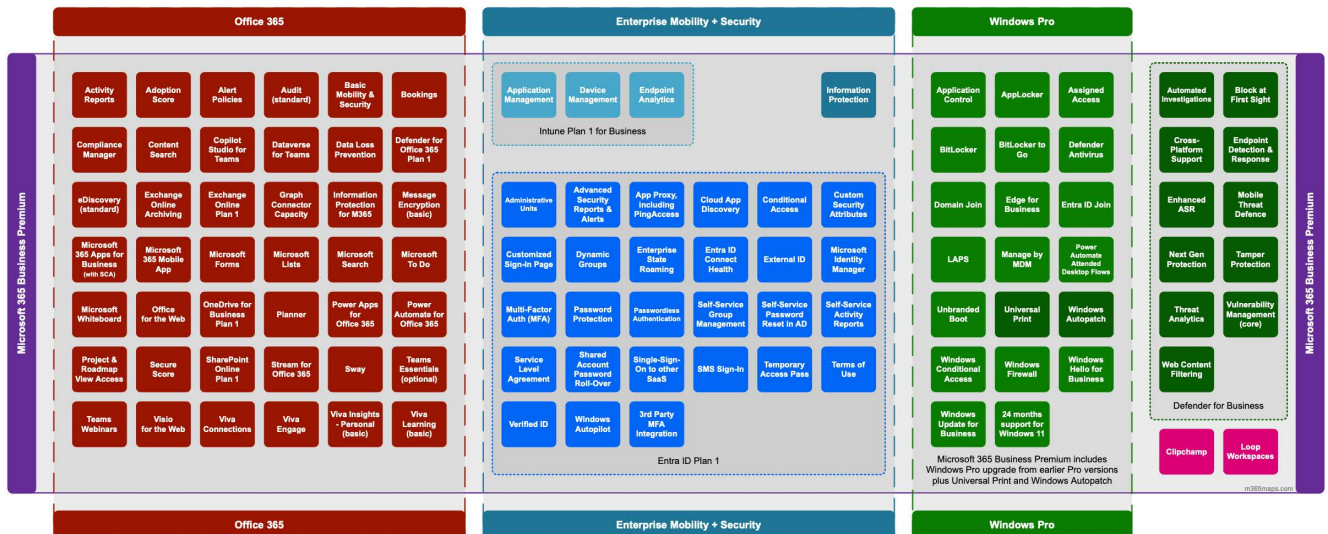Health Dashboard   Management Console   Data Reporting

MICROSOFT 365 PREMIUM LICENSE

This license provides access to email, Microsoft Office programs, and the logging and security features that we use to implement your security baseline.

However, it's important to note that Microsoft 365 (like all Microsoft products) does not have all security features enabled by default. Activating these features requires careful configuration to align with each organisations specific needs and security requirements.

The full feature set is detailed below:

FEATURED PARTNERS   HUNTRESS   Microsoft 365   Microsoft Defender