

Huntress endpoint and identity security

Canonical: <https://agentic.blueapache.com/technical-excellence/huntress/huntress-solutions-with-blueapache/>

Description:

We combine Huntress Managed EDR and Managed ITDR with our Microsoft security practice.

Details:

We bring Huntress into our security offering to strengthen detection and response across Microsoft-centric environments. You can access Huntress through us as part of a managed security service or through our reseller offering while retaining your internal IT or security team.

We combine our Microsoft security practice and service delivery with Huntress Managed Endpoint Detection and Response, known as Managed EDR, and Managed Identity Threat Detection and Response, known as Managed ITDR. Our implementation work connects the selected capabilities with your endpoints, identities and operational responsibilities.

Strengthen protection around Microsoft investments

Our Huntress offering works alongside Microsoft environments including Microsoft Defender and Microsoft Entra. For organisations using Microsoft Business Premium, we help assess how the selected detection and response capabilities can extend the value of the environment already in place.

Endpoint and identity threats need different visibility. An endpoint investigation concerns activity affecting devices, while an identity investigation concerns accounts and access. We consider both in the design so the security response reflects how an attacker could move through your environment.

The combination also needs to work operationally. We discuss how alerts reach the right people, who can authorise response actions and how a security incident connects with your wider IT support process.

Two ways to work with us

Managed security

If you want us to take on the agreed day-to-day security responsibilities, we incorporate Huntress into our managed security delivery. We define the protected environment, the selected detection and response capabilities and the escalation arrangements with you.

That discussion includes your internal contacts, critical systems and business dependencies. A response action affecting a user or device needs to be understood in the context of the business, with clear communication and ownership.

Reseller and technology delivery

If you have an internal security or IT team, our reseller offering provides a route to access Huntress through us. We can help you adopt the selected technology while your team retains its wider

operational responsibilities.

We work through deployment, integration and the handover between your team, our team and the Huntress service. Keeping an internal team does not mean that you must build every specialist detection and response capability yourself.

Plan coverage and response together

We help you work through practical implementation questions before deployment:

- Which endpoints and identities are included, and which require a different approach?
- Which Microsoft security capabilities and licences are already in use?
- Who receives an escalation and who is the alternate contact?
- What actions require your approval, and who can provide it?
- How will new devices, staff changes and changes to access be reflected in coverage?
- How will incidents and follow-up actions be recorded and reviewed?

These decisions help the selected technology fit your organisation's operating model. We agree the service boundaries and support responsibilities as part of the engagement.

Connect detection with the rest of your security programme

We consider Huntress alongside patching, access management, backup and human risk management. Each addresses a different requirement. For example, detecting suspicious account activity does not replace a recovery plan, and security awareness training does not replace endpoint protection.

Our broader security capability lets us discuss those dependencies with you and identify where you need technology, specialist assistance or an ongoing managed outcome.

Questions about Huntress

Can our security team keep control?

Yes. Our reseller route supports organisations with internal teams. We agree the deployment and response responsibilities so your team knows what it owns and where the Huntress service and our assistance fit.

Is Huntress our human risk management platform?

We use Huntress for endpoint and identity detection and response. Our Human Risk Management as a Service is powered by Mimecast. We can bring those capabilities together within a wider security design.

Is the offering limited to one company size?

Our expanded Huntress relationship supports organisations of different sizes. We assess your environment and requirements rather than treating our managed-services mid-market focus as a limit on all technology engagements.

Discuss Huntress with our security team

Related expertise

- Mimecast human risk management
- Microsoft cloud, workplace and security