

MSSP Solutions



Products

EDR/MDR/SOC

- ❖ Endsight will configure and monitor Microsoft Defender for Endpoint. This license, available via Microsoft 365 Business Premium, standalone purchase, E5 plan, or Security and Mobility add-ons, must be purchased separately.
- ❖ Our security operations center (Blackpoint Cyber) monitors EDR on endpoints and acts as MDR for endpoints and Microsoft 365 cloud. They investigate issues, isolate computers, and lock accounts as needed. This full-service SOC, supported by our security team, provides extensive 365 monitoring, correlating events and expanding the trigger list of cloud activities.



Phishing Testing

- ❖ Bi-weekly test emails with reactive training for those who fall for the phish. Quarterly mandatory training is also included, regardless of testing results.



DNS Filtering

- ❖ DNS agent on laptops and DNS forwarding on onsite servers. Provides final protection against compromised computers and offers web filtering at no extra cost.



Dedicated Teams channel for documentation, collaboration, and escalation

- ❖ Our security team will setup a Microsoft Teams channel for the following:
 - ❖ Document sharing
 - ❖ Security product questions.
 - ❖ Automated channel for SOC alerts.
 - ❖ T2 support
 - ❖ Questions related to security configurations
 - ❖ This Teams channel is not for technical support, opinions on the latest security trends, or daily chat support – it's a way to get direct access to our security needs for urgent issues or related projects.



Services

Breach Assistance

- ❖ Our SOC and internal team will isolate breaches, investigate incidents, and provide detailed reports. While we don't wipe computers or reset accounts in 365, we'll offer recommendations and remediation steps to prevent future incidents.
- ❖ For MSSP clients, the initial investigation and classification from the SOC is covered.



Annual Security Audit

- ❖ Endsight performs an annual audit, covering the following:
 - ❖ Cloud configuration and logging
 - ❖ Phish testing performance
 - ❖ Endpoint configuration and incidents
 - ❖ Manual review of tickets
 - ❖ Domain configuration review
 - ❖ All happen annually with a deliverable report, designed to pass audit and be delivered to a board
- ❖ Individual server configuration and review.
- ❖ DNS protection review and reporting.
- ❖ Future strategy discussion and budgeting
- ❖ Human discussion with team to ensure nothing's slipping between the cracks.



Annual Insurance Form Assistance

- ❖ While we can't sign forms for clients, we'll complete as much as possible, save evidence, and prepare the form for insurance renewals. This process often reveals necessary fixes, which we are happy to assist with.



Quarterly Spearphishing

- ❖ Our team will lead a quarterly spearphishing campaign for high value targets. This includes some research (public information only), and we'll update you on who fails.



Policy Writing

- ❖ Endsight will help write and annually update major policies to adapt to changing threats. We offer templates that have passed insurance and regulatory review, with the top three being:
 - ❖ Incident Response
 - ❖ Acceptable Use
 - ❖ Backup/Disaster Recovery
- The policies will be saved to our system and to yours. This will require input and support from the executive team to be effective. Expect approximately 2 hours per year for review and updates.



Quarterly Penetration Testing:

- ❖ Endsight will attempt to connect to identified publicly available services (web servers, firewalls, etc.). If successful, we'll report our findings and recommend remediation. Importantly:
 - ❖ This is a best-effort attempt to reduce the attack surface, not a guarantee to find every vulnerability or patch everything.
 - ❖ This service is remote and technical only, excluding social engineering or physical efforts.



Documentation

- ❖ Everything included in this proposal includes full documentation and logging, available upon request

