IBM Security Managed Endpoint Protection Services

Highlights

- Multi-layered endpoint protection tools
- Identify important trends in endpoint security
- Quickly assists in remediation of potentially harmful security exposures
- Improves incident management and response through notification of actions

Traditional endpoint defense from increasingly sophisticated attacks

Enterprises must now assume a compromised IT environment. More organizations are now falling into two categories—those that have been attacked and those that will be. A disturbing third category is also growing that includes enterprises that have been hacked and will be again.

Endpoints represent the new enterprise perimeter and advanced attacks can originate from an exponential number of remote devices. Several trends have converged to make endpoints more vulnerable than ever. The increased use of commercial cloud applications, pervasive employee-owned devices and the growing popularity of employees working remotely all result in more threats to the endpoint. There has also been a significant increase in corporate espionage, intellectual property theft, and attacks that focus on impacting a company's reputation which are affecting all industries across the globe.

Addressing the endpoint threat vectors requires an understanding of how cybercriminals can use an organization's own tools and resources to conduct attacks and make those attacks more difficult to detect. Most organizations keep back-end systems well protected. However, users and employee endpoints usually do not benefit from the same level of security practices — especially if those endpoints are on a personal device. Cybercriminals have achieved success using socially engineering techniques and tactics on users, deploying phishing schemes with malware to inevitably capture the users personal information and credentials. The criminals use the stolen credentials to take over the user's account, take advantage of authenticated sessions and drive fraudulent transactions through the user, right under the security team's radar.

Financial fraud is especially endpoint-centric because endpoints can offer the easiest and fastest path to the money.

Fortunately, the challenge can be effectively addressed with the right resources, expertise and industry recognized techniques and tactics. IBM Managed Security Services utilizes global expertise and industry recognized techniques to help solve today's toughest endpoint security challenges.

IBM Security Managed Endpoint Protection Services apply this same approach to help defend endpoints. It can help effectively alert your team of attacks, provide reporting and recommended actions required to protect your environment. The service helps provide deep visibility into security incidents and across the distributed enterprise. Trained IBM Security specialists can help provide ongoing health monitoring and recording of activity on endpoints, conduct routine status checks and escalate on high severity security threats.

Endpoint Security Services helps support your endpoint protection, working with you to develop an endpoint solution that meets your needs. If this does not support your business needs, we can satisfy most requests as a fully customized solution.

IBM Security Managed Endpoint Protection Services

Our endpoint security provides:

- Service planning and onboarding, including an assessment of your environment and architectural planning and support
- Management and maintenance of your selected endpoint protection product using an on-premise deployment model, allowing maximum flexibility and control over your data
- Monitoring of internal and external sources for new threats or infections on endpoints
- Expertise to analyze endpoint traffic combined with investigation and detailed recommendations for remediation

This IBM solution is built cutting-edge technology, intelligence and expertise—using intelligence from the IBM X-Force® threat intelligence and thousands of global analysts to help:

- Proactively protect your endpoints from malicious software
- Identify and remediate existing endpoint infections
- Profile the environment to determine “normal” behaviors and areas of weakness

- Configure and activate control points based on the prioritized risks

Why IBM?

IBM offers a full featured Managed Security Services portfolio that can enable end-to-end security monitoring and management, better visibility and efficiency while supporting multiple technologies, vendors and devices. Our competitive pricing and delivery model is standardized across the portfolio— offering increased flexibility based on service-level agreements to help with cost savings and help facilitate an overall improvement in your security posture over deal terms. We can help improve endpoint return on investment and offer highly customized services according to the needs of your enterprise.

Next steps

→ Learn more about IBM Security's Endpoint Security Services

For more information

To learn more about IBM Security Managed Endpoint Protection Services, please contact your IBM representative or IBM Business Partner or visit the following website: https://www.ibm.com/security/services/managed-security-services/endpoint-security

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.