

Infrastructure Security: Endpoints



PROTECT
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Is the Endpoint Security Service right for your company?

- Have employees lost laptops or cell phones containing sensitive corporate or personal data?
- Are you deploying a centrally-controlled system for encrypting mobile data?
- Are you concerned that dangerous malware could enter your network from unprotected endpoints, such as home computers granted remote access into your network?

Overview

One of the most significant threats to an organization's security are the endpoints—the user-controlled devices that connect to the network. These endpoints include workstations, laptop computers, personal digital assistants (PDAs), mobile phones and cameras, Blackberries, memory devices (USB keys and portable hard drives) and specialized equipment like Point of Sale terminals

Securing endpoints requires you to overcome some particular challenges:

- Network security devices (firewalls, VPNs, etc.) are ineffective at protecting mobile endpoints—therefore, each device must provide its own security
- An organization may not always own, or have control over, the endpoints that connect to the network
- The devices are frequently mobile, so security applied at the workplace must remain effective on the road and at the employees home

Digital Defence's endpoint security assessment provides a comprehensive program to auditably ensure the security of an organization's endpoints, and integrate them into your secure network.

Benefits of an Endpoint Security Program

- Central management and security of endpoints reduces the Total Cost of Ownership, TCO, for each device
- Reduce or eliminate financial and reputational costs of a data breach
- Comply with Federal and industry regulations; meet audit requirements
- Increase client and partner confidence by demonstrating ability to protect confidential information

Service Description

The Endpoint Security Assessment audit reviews the following :

- Network infrastructure, including network and device access controls
- Data flow analysis map to identify points where sensitive data can be accessed, copied, modified or stolen
- Policy development governing static and mobile endpoints, including central management, enforcement, and auditing
- Secure remote access from the secure network to mobile devices across wired and wireless networks
- Centrally managed vulnerability management, including update and patch delivery and auditing
- Implementation of effective security controls at the endpoint, including client firewall, anti-virus, IDS/IPS, encryption, and patch management
- Development and implementation of a Common Operating Environment, COE, to ensure consistent delivery of a secure environment
- Review of specific applications on mobile endpoints
- Secure messaging to endpoints, including e-mail, instant messaging, anti-spam and phishing protection, and archival
- Backup and recovery of endpoint devices
- Security awareness training for end-users

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.