Endpoint Security

TBI Battlecard

What to Look for in the Field/What you should know

- Anyone deploying new devices to end users (laptops/desktops)
- Customers renewing Antivirus/endpoint contracts
- Customers expanding, adding employees/devices

Overview

Endpoint security refers to a methodology of protecting the corporate network when accessed via any device—from laptop to desktop, printers and mobile phones. Each device with a remote connection to a network creates a potential entry point for security threats.

Endpoint security is a system that is typically comprised of security software, located on a centrally managed and accessible server or gateway within the network. In addition to client software being installed on each of the endpoints (or devices).

Although endpoint security software differs by vendor, most software offerings provide antivirus, antispyware, firewall, and they also a host intrusion prevention system (HIPS).

Discovery Questions

Do any of your employees bring personal devices to work?

What security risks are you most concerned about?

How do you secure your endpoints today?

Make sure to address servers as well as traditional laptop/desktop endpoints.

What do you do to secure your network, from the edge to the endpoint?

Do you have visibility to endpoints and security policies around them?

Add-ons to Endpoint Security

- Managed Firewall
- Email security
- VPN/Identity Access management
- Mobile Device Management (MDM)
- Wireless Expense Management
- Consider asking about colocation and cloud connects

Top Providers

CenturyLink | Coeo | First Communications | GTT | Hypercore

Masergy | Nitel | NTT* | Synoptek | Telesystems

TPx Communications | Zayo

**Only available with other security services*