

Radiant Security Services is...



Site Shield- A managed commercial grade hardware firewall service and much more.

- Radiant separates the Payment Network from other PCs and networks that are needed for business operations. This is done through configuring Virtual Local Area Networks (VLANs) for other business equipment that shares access to the Internet.
- All Internet access is blocked out except for necessary ports and connections (credit card or other third party solution provider products for example). Free range Internet browsing is removed as an option from this PC.
- Firewall inspections check for data packets that are likely to be associated with malware.
- Intrusion detection is employed to stop a cyber criminal from multiple scans of the network.
- Radiant provides a single point of authority in the event employees or other third party agents are looking to change port configurations or get access to business systems.
- Radiant provides and maintains the hardware firewall for new antivirus updates and manufacturer's security patches.
- If a firewall is damaged at no fault of the operator or can no longer receive manufacturer security patches or antivirus updates, Radiant will provide you with another firewall.
- Multiple configurations and options for secure public facing Wi-Fi.



Secure Access- A secure remote access tool.

- Radiant provides a two factor secured application for accessing the POS back office PC and network.
- This tool provides the operator with alerts that show potential security issues (i.e. antivirus definitions are out of date).
- Operators register their mobile phone number with Radiant, which provides access to a token password whenever access to the BOH PC at the site is requested.
- Operators can remotely access the BOH PC, securely transfer files or run POS level reports directly from the user interface.

Radiant Security Services is...



Threat Defender- An ongoing monitor and network defense service.

- Threat Defender attacks and defends against malware that finds a way past perimeter and in-store physical security defenses. It encompasses all of Radiant's efforts to continually improve layered security measures within the operator's Cardholder Environment (CDE).

- Active daily security scanning for network risks and threats, including:
 - Antivirus service not running or out of date
 - Crimeware, including RAM parsers and key loggers
 - Malware
 - Unbatched credit cards
 - Default Windows passwords and credentials found
 - Insecure remote access tools detected

- Process and service white listing is an added layer of security for locking down any software, processes or services from running in the Cardholder Environment (CDE) unless they are designated as a known "good" software. This restricts potentially dangerous or unwanted software from running on workstation terminals or back of house PCs.

- Threat Defender will continue to adapt to new malware threats as Radiant studies of all processes and services that reside within the CDE, including Department of Defense level file destruction for deleted files and information in "unallocated space", which is scheduled for deployment within the coming months.

Radiant Security Services Breach Assistance Program

- Radiant Security Services includes up to \$50,000 of breach protection per site.
- Don't jeopardize your business - protect it from the expenses that result from a suspected or actual data breach.
- The program covers the forensic audit when a breach is suspected, card replacement costs, assessments and fines levied by card sponsors and more.



877.794.RADS (7237)

www.radiantsystems.com

rss@radiantsystems.com