PaySafe Unified Threat Management Service*

**PDI's PaySafe United Threat Management Service is no longer available for purchase but will continued to be supported for existing Customers until further notice.*

PaySafe United Threat Management

Unified Threat Management (UTM) refers to a category of network appliances that utilize multiple security features in a single device. Typical UTM applications can include or combine a traditional firewall with VPN, content filtering, anti-virus, anti-malware, intrusion detection (IDS) and intrusion prevention (IPS) capabilities.

PDI's PaySafe UTM service provides a comprehensive, layered security approach to sensitive environments. The PaySafe UTM allows PDI to monitor, with multiple applications, the Customer environment.

PDI's ongoing monitoring and management of appliances deployed on the edge of sensitive environments is reinforced with proactive, bi-annual audits of firewall configurations. As security best practices mature, UTM services and configurations are dynamically updated as well.

Services include:

PDI's PaySafe UTM service consists of Managed UTM Services, UTM Software Licensing, UTM Hardware, and Cellular Connectivity.

- **Managed UTM Services**
  - Access Control Rules

    For sensitive card holder network environments, PDI will develop access control rules that meet business needs while limiting or blocking unauthorized or unneeded network traffic. PDI utilizes a "Deny by Default" security posture, limiting access to that which is explicitly authorized for the "CDE". "CDE" refers to processes and technology that store, process, or transmit cardholder data or sensitive authentication data. Upon request, PDI can apply restricted access controls to other network segments which are not part of the CDE.
  - Network Segmentation

    PDI configures all PaySafe UTM's with network segmentation to protect sensitive card holder networks from local and public networks using clearly defined sub networking and accepted best practices for isolating and securing critical networks. This would be the initial configuration for any later Network Segmentation Validation Tests, as required under certain circumstances by the PCI DSS.
  - Health and Functionality

    PDI utilizes automated alert systems in the event of changes in overall network health. These alerts include "online/ offline" primary connection alerts, automated failover and failback to secondary connections alert notifications.
  - IDS/IPS

    Intrusion detection service (IDS) will detect and log potentially malicious network traffic based on defined rulesets. The intrusion detection monitors all packets flowing between local networks and Internet interfaces.

    The Intrusion prevention service will automatically block potentially malicious traffic. Intrusion prevention's primary goal is to stop potential network attacks or unauthorized access before they are successful. All security events that trigger any IDS/IPS monitoring or action are immediately logged and available to view within the cloud-based portal. These reports can be filtered by date/time, host, or event occurrence type.
  - Advanced Malware Protection (AMP)

    PDI's UTM service includes malware protection technology. Malware detection screens the incoming and outgoing HTTP traffic for malware. Threats are detected and blocked based on either the URL or a signature triggered by the content. These services are updated daily, and events are logged and reviewable with the cloud-based portal.
  - Web Filtering

    The UTM web filtering service allows clients the option to block certain categories of websites based on your organizational policies, example Peer to Peer, Sports, videos. In addition, the allow list and block list enable additional customization to select web sites and/or website domains.
  - Site-to-Site VPN

Site-to-Site VPN allows for secure communications between 1 to many PaySafe UTM's. PDI administrators will configure and monitor the availability of all site-to-site VPNs. This includes any troubleshooting required to allow users to successfully connect and stay connected through the service.

- Group Policy Changes

  Group policies define a list of rules, restrictions, and other settings, that can be applied to network segments in order to change how they are treated by the network. Any requests made for access, either during the initial deployment or ongoing once configuration has been completed, are assessed against existing PDI policies and published best practices. PDI Helpdesk will provide guidance to clients regarding these practices and help provide additional solutions that will still meet published security policies.

- Content Tuning Policy

  As client requirements and needs change, PDI administrators will work to provide dynamic environments that meet any required compliance guidelines.

- **Cellular Connectivity**

  PDI offers two cellular connectivity services for clients for diverse connectivity or when a site is unable to order broadband.

  - PaySafe Cellular Failover

    PaySafe Cellular Failover provides a seamless secondary cellular internet connection should the primary internet connection become unavailable. This service is intended for business-critical applications ONLY and not for general internet use.

    - The PaySafe Cellular Failover service shall be used for back-up connectivity to the primary internet.
    - It is solely for the use of payment related applications.
    - Any other use of this service is strictly prohibited.
    - Includes 300MB of data usage per month.
    - Any use of this service except as intended may result in penalties including temporary suspension of cellular service and overage fees.

  - PaySafe Cellular Primary

    PaySafe Cellular Primary access allows clients to choose cellular as the primary connectivity option where traditional land based broadband service is unavailable. The PDI representative will work with clients to determine the appropriate data plan.

    - PaySafe Cellular Primary is billed monthly based on the site data plans provisioned in the boarding process
    - All data sent or received using the cellular connection, including any network overhead associated with content sent or received, will be considered usage.
    - Data transfer amounts will vary based on application; Customers may request assistance from PDI to determine the appropriate data plan.
    - If data usage exceeds the provisioned amount, PDI may or may not provide immediate notice, and in any event, shall bill Customer for any charges resulting in excessive usage.

Out-of-Scope Services

Services, deliverables and equipment not listed in the associated Service Order are out of scope and are not part of this particular Service. Any out-of-scope work may be completed by PDI after being defined in a separate, signed Statement of Work (SOW) upon your request. Out-of-scope items may include (but are not limited to):

- Professional Installation Services
- Support for any device or application not currently being managed by PDI, such as a modem provided by the Internet Service Provider (ISP).

Security

- **Network Environment**

Upon installation, by Customer, the network activity and devices connected to the PaySafe UTM will be assessed by PDI. It will be determined by PDI that the standard configuration and network controls have been applied and the secure CDE is segmented from the non-CDE environment. PDI may recommend changes to Customer-provided devices to support the recommended segmentation. If Customer does not make recommended changes to its devices to achieve the segmentation as recommended by PDI, the network will be deemed unsecure and Customer will be advised, either by telephone call, email or letter that there is risk of non-compliance with PCI DSS. Customer acknowledges that it has responsibility for PCI DSS compliance and that a PDI determination that the network is secure does not act as a warranty or guarantee of security standard compliance nor is Customer relieved of its independent obligation to maintain PCI DSS compliance.

Only a Customer employee authorized to request changes to Customer's Network Design may request modification to the network, including adding devices or opening ports for access. Any change that impacts a secure segmentation requires written notice to PDI and Customer is fully responsible for any such requests and results therefrom. If the requested change will result in an unsecure network segmentation of the CDE, Customer will be so informed, and PDI reserves the right to deny any such request. In any case, all liability for the security of Customer-approved network will rest with Customer. PDI is responsible only for either (i) accommodating Customer's request or (ii) providing an explanation for denying such request. PDI will maintain records of the request, any advisement of risk and any authorization to make the change, particularly if it is against the advice of a PDI network engineer.

Customer is liable for securing the physical environment and securing physical access to all network components. Physical alteration of the network could create risk and PDI is not responsible for restricting access to the on-premise physical environment.

- **Requesting Changes**

  After initial installation of the PaySafe UTM, all subsequent changes must be requested in writing using the PDI *PaySafe Firewall Change* Request form (provided by PDI support). This is required for tracking and audit purposes to ensure that all changes originated from an authorized representative of your organization. All changes will be reviewed to ensure the request does not violate PDI's secure configuration standards.