

# PCI-DSS SECURITY

Protecting sensitive financial data is the goal of PCI compliance and a requirement from your credit card processor. That means you must have protections over card payments, payment data transmission, and how transaction records are stored. Make Atlantic.Net part of your PCI compliance journey. Our purpose-built PCI-DSS Cloud environments help your team pass the 12 main PCI requirement groups with over 250 PCI-DSS sub-requirements and over 400 PCI-DSS testing procedures!



## MANAGED FIREWALL SERVICE

Our fully managed firewall stack service is connected to Atlantic.Net; all other network traffic is isolated.

- ✓ A professionally managed firewall service
- ✓ Exceeds physical and logical security requirements
- ✓ All patching, configurations, updating, etc. are handled by Atlantic.Net certified engineers
- ✓ Redundant firewall options are available



## A FULLY MANAGED VPN

The VPN offering is available as a user-based VPN and a point-to-point VPN tunnel.

- ✓ Encrypted AES-256 VPN tunnel
- ✓ Support for OpenVPN and IPsec by default that exceeds PCI-DSS standards
- ✓ Includes the management, maintenance, and troubleshooting of the VPN connectivity



## MANAGED NETWORK INTRUSION PREVENTION SERVICE

The Managed IPS Service works hand-in-hand with the ACP Managed Firewall Service to analyze and take action against suspected malicious traffic.

- ✓ Packet logging and reporting
- ✓ Real-time traffic analysis and control panel for review
- ✓ Flexible configurations to match your deployment needs
- ✓ Fully updated, patched, maintained, and serviced by Atlantic.Net



## ENCRYPTION AT REST BY DEFAULT

Our systems use AES-256 encryption as a standard, and our teams are highly trained in security best practices when handling sensitive data.

- ✓ Automatic disk-level encryption is enabled by default on ACP Compute and ACP SBS
- ✓ Optional application-level encryption with support for BitLocker and PGP
- ✓ Encrypt your network traffic using TLS certificates
- ✓ VPN Encryption by default with Managed Firewall
- ✓ Database encryption available
- ✓ ACP Backup systems utilize encryption at rest and in transit by default

# PCI-DSS SECURITY



## MANAGED EDGE PROTECTION

Edge Services shield your environment and lower your attack surface.

- ✓ Edge Services shield your en
- ✓ Content Delivery Networks (CDN) to reduce the attack surface of your website while providing faster response times that improve customer experience and SEO
- ✓ Web Application Firewall (WAF), an additional service that uses policy-defined protection for web applications by monitoring and filtering traffic via the network edge



## TREND MICRO DEEP SECURITY

Trend Micro™ DEEP SECURITY Network Security Package intelligently and proactively monitors network activity and is an optional managed service add-on for our clients.

- ✓ Threats are monitored and prevented in real-time
- ✓ Shield your system from new and known global exploits
- ✓ Increase the visibility of applications accessing the network
- ✓ Intelligent protection against known and zero-day attacks
- ✓ IPS firewall packet inspection
- ✓ Protection from local vulnerabilities at the network layer
- ✓ Traffic shaping and simultaneous connection limitations are easily configurable



## TREND MICRO DETAILED LOG INSPECTION

With our Trend Micro™ DEEP SECURITY System Security Package, you'll get detailed log inspection features.

- ✓ Automated monitoring of critical operating system and application files, such as directories, registry keys, and values
- ✓ Integrity Monitoring that detects and reports malicious and unexpected changes to files, the hypervisor, and systems registry in real-time
- ✓ Log Inspection optimizes the identification of key security events buried in log files
- ✓ SIEM integration



# PCI-DSS SECURITY



## TREND MICRO ANTI MALWARE PROTECTION

Atlantic.Net's engineers selected Trend Micro™ DEEP SECURITY Anti-Malware Package because it provides the full required coverage to help protect against external threats.

- ✓ Protect virtual machines against viruses, spyware, and other malware
- ✓ Web Reputation that strengthens protection against web threats to servers and virtual desktops
- ✓ Trend Micro™ Smart Protection Network™ web reputation capabilities to safeguard users and applications by blocking access to malicious URLs



## MULTI-FACTOR AUTHENTICATION (MFA)

MFA is not just a best practice, but a requirement for PCI-DSS systems. Atlantic.Net provides the easiest-to-use MFA solution available. SMS or smartphone applications make it easy to use MFA and without slowing your team down.

- ✓ Can be set up at scale from 1 to 100,000 users
- ✓ MFA authentication software can be distributed directly to users
- ✓ Each user will need a username and password, a pin, and a code generated from a mobile app
- ✓ SMS option available



## DATA PROTECTION AND AVAILABILITY

The Atlantic.Net Cloud Platform provides standard and customizable Onsite and Offsite Backups and Replication options. Some of the standard configurations are:

- ✓ 5 Minute Backups with 96 retention points
- ✓ 15 Minute Backups with 96 retention points
- ✓ 1 Hour Backups with 24 retention points
- ✓ Daily Backups with 30 retention points



## VULNERABILITY SCANS

Our Managed Services include biweekly vulnerability scans for host servers or configured websites which are tested against over 500,000 vulnerabilities! Upon request, we can also assist with evaluating scan results and implement requested firewall rules to mitigate potential issues.



## Get Help with PCI Compliance

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, call **888-618-DATA (3282)**, or email us at [sales@atlantic.net](mailto:sales@atlantic.net).