



1755 N. Main St.  
Los Angeles, CA 90031  
1-323-576-1400  
1-800-933-8388  
[www.dttusa.com](http://www.dttusa.com)

## PCI-DSS Compliance at DTT Surveillance

*Written By:*  
*Vic Herrera*  
*Chief Information Officer for DTT*

PCI-DSS compliance has been a major focus at DTT for several years. The community has evolved. Over the years DTT has built relationships with several vendors with whom we share clients. Here we will discuss DTT's holistic approach to ensure Data System Security. We will explain the design of the system and software, the support policy, and ongoing efforts to ensure compliance and security.

DTT starts with a hardened Windows Operating System. All patches and security updates are installed and configured, unneeded programs are removed, and software tools are used to lock down the functionality of the server. Usage of the system is limited to Video Surveillance Recording. We also configure a Windows Firewall in order to lock down accessibility and a Windows Defender to eliminate the ability to install Spyware and Malware.

The system then receives the latest version of our Video Recording Software and we run a bench test. Once the system is properly configured and a complete Quality Control process is run, we put two identical systems on two very different networks to begin penetration testing by two different PCI compliance vendors.

We create an image or clone of this system and send it to our HP OEM team for review. They install the image, and burn in the system. The system is tested for stability and a first article is delivered to DTT. We then Quality Control that system, set it up on our penetration testing networks and, once it passes the system, send it to production.

We find our customers largely in two different network scenarios. The first is a more managed environment where the DVR sits behind a Commercial Grade Firewall with a one-to-one NAT port forwarding at a granular level and is tightly controlled. At the minimum, there is business level dedicated internet services, business grade cable modem or managed DSL, possibly a T1 or greater with static IPs. The client will likely connect via a VPN and also has a regular/daily IT resource in place, either a Managed Service provider or IT Staff dedicated to networking and security. The second network scenario is when the client is using a consumer grade router/firewall, port forwarding, dynamic DNS, and consumer grade internet access, usually a DSL line. This client usually uses an outside consultant for networking and IT services and has limited IT resources.

Once the systems have been put in place on either of these networks, penetration tests are scheduled with Security Metrics, and Trustwave. Once the systems pass the final penetration tests on both networks by both companies, they are put into production.

We also have standard quarterly penetration tests on current versions as prescribed in the latest PCI-DSS standard on both networks by both vendors. It should be noted that DTT has over 18,000 systems in production that are being scanned daily in every possible configuration. Occasionally, a system fails a scan, usually because of a configuration issue on the server or because the server is out of warranty, and therefore not covered by DTT software updates. Patches and configuration changes usually take less than an hour to complete.

DTT software engineering is built with PCI-DSS compliance in mind from the ground up. DTT uses a proprietary POS integration solution called Suregate™. The Suregate™ reads only receipt data, which is the same information printed on paper receipts and handed to customers. This software has been reviewed and certified by Microsoft; and, DTT is a Microsoft Certified Gold ISV partner. Earning the ISV competency required DTT to submit documentation and a tremendous amount of information regarding our software application and the POS integration application to Microsoft for review.

Suregate is 100% PCI compliant. Suregate never reads any card holder data and transmits all data in a proprietary format so that the contents cannot be read.

DTT's solution is in place at Tier 1 card processing sites. These sites process more than 20,000 credit card transactions per day. DTT DVRs are subject to the most rigorous scrutiny that PCI-DSS scanning vendors have to offer in these environments and they consistently pass all security testing.