SECURE AND RESILIENT COMMUNICATION SERVICES

FOR CRITICAL REMOTE CONNECTIVITY

Table of Contents

1. Understanding the Current Security Environment to Manage Vulnerabilities

Customers operating in remote and harsh environments within highly competitive market segments recognize that protecting data is growing in importance each day. This is especially true within the resources sectors as cloud-based networks, applications, and data become increasingly attractive targets. Keeping security standards up-to-date helps to keep customer networks operational, and their brand reputation strong.

At ITC Global, our staff has a deep understanding and appreciation for the criticality of customer operations in the markets we serve, and we take our network security design and development process very seriously. Our approach includes a comprehensive understanding of each customer's network, increasing vigilance with constant monitoring of known threats and changes in network behavior, and quickly responding to any real or perceived vulnerability. A custom network from ITC Global is a different undertaking than that of our competitors. We design and deploy purpose-built networks to render highly resilient and protected, reliable connectivity for mobile and remote customers from the start of installation through each network's entire lifecycle.

The ITC Global team takes into account security concerns that apply to every customer, as well as specific security requirements more specific to certain vertical segments. This includes everything from ship owners worried about hackers getting into their antenna systems and onboard IT equipment, to concerns about onboard computers and devices that can be vulnerable to exploits that install malicious software, and fears that remote users will access illegal or illicit content. We design and deploy network solutions to keep management and Internet traffic completely separated to limit exposure from the World Wide Web. Our team vigilantly monitors our intrusion detection system and can pinpoint problematic and intrusive actions back to the specific computer where it originated, notifying customers of a potential security concern even before they are aware of it.

In one instance, ITC Global's proactive monitoring capabilities alerted the Network team to a crew member at a remote offshore site who was connecting a personal laptop to the corporate network in the drilling rig's below deck equipment (BDE) room. While not malicious, ITC Global was able to notify the customer that we identified a network threat at the remote site. The client removed the machine without incident, avoiding any security issues that come with "after hours" devices on the corporate network.

2. The Panasonic Standard — Enforcing Strict Security Policies

As an independent operating unit of Panasonic Avionics Corporation, both organizations share network infrastructure resources. Because of this, ITC Global is subject to the same strict security policies, guidelines and reviews as its parent company. These policies include those dictated by the FAA, as well as by Payment Card Industry Data Security Standards (PCI-DSS). In addition, Panasonic also maintains GRC (Governance Risk Compliancy) ongoing certifications and compliancy.

Since joining Panasonic, ITC Global has conducted a complete technical audit of our cyber security practices and environment across each of our global offices, teleports and data centers. The rigorous exercise resulted in further tightening and upgrading of our network that has enabled us to stay ahead of the cyber security curve so we can continue to deliver highly reliable services to our customers, many of whom are now keenly focused on the issues surrounding cyber security.

3. Defense-in-Depth Approach

ITC Global has a long-standing commitment to developing end-to-end network solutions that uniquely suit users in tough, remote environments. These customized networks deliver high-speed global connectivity for always-on, enterprise-class communications. To ensure that users can operate securely 24/7, ITC Global has expanded its security expertise and activity to optimize network resiliency and protection. In today's globally connected world, ITC Global has developed a Defense-in-Depth methodology to network monitoring and security. This includes a comprehensive understanding of customers' networks, where multiple layers of security are implemented to mitigate the impact of a compromise or breach of any one layer.

For example, device-appropriate filtering may be applied on the edge Ethernet switch, then on the edge router, then within both the upstream and downstream directions in the satellite transport layer, and then again in the routers and firewall at the teleport. Implementing Defense-in-Depth requires an intricate understanding of the end-to-end network design and end-to-end traffic flows, however, this deep understanding is required in any case, in order to implement a meaningful and optimized granular QoS model. Further, the implementation of the security model via Defense-in-Depth means that security is implemented across hardware from multiple vendors, and on multiple models of equipment, thus also offering Systemic Diversity; that is, helping to mitigate the impact of a "zero day" vulnerability in any one specific device.

Compromise in one device in the Defense-in-Depth model inherently results in unexpected traffic being seen by the layer(s) on either side of the compromised device, thus drawing attention to the breach. Additionally, this approach dramatically increases the time required for a malicious attacker to compromise the network, thereby giving additional time for Intrusion Detection Systems to signal a security event and for ITC Global network engineers to respond and address the threat. Defense-in-Depth works methodically at all times. The ITC Global team also leverages Panasonic resources to watch for traffic alerts, tracking and blocking all malicious traffic to again address each threat.

4. Cyber Security Best Practices Implemented 24/7

ITC Global employs industry-standard best practices in Information Security management, which has been certified to ISO 27001 standards. The company provides multiple layers of resiliency—from national espionage to corporate misconduct to accidental employee breaches—with firewalls in place at the network edge to mitigate illegitimate or threatening traffic at all possible points of entry. ITC Global takes cyber threats seriously and engages in daily security activities such as threat monitoring, security auditing, and routine password rotation to ensure the network's safety.

ITC Global networks and security policies are implemented so the company's corporate data is isolated from client data at all times, including transport. Client data is also completely separated from one another. ITC Global's robust security backbone prevents cross-contamination between client data so they cannot interfere with each other's networks. As crew communications grows in every vertical market served, ITC Global has also deployed turnkey solutions to ensure crew activity and data reside on their own network and are entirely separate from management's operational data. This optimizes bandwidth speeds while limiting possible security concerns that come from bring-your-own-device and after-hours network use on the corporate system.

5. Intrusion Detection and Artificial Intelligence

ITC Global's highly skilled, experienced security team reinforces our strong, Defense-in-Depth security backbone. Leveraging Panasonic's robust Security Operations Center, the team focuses on all types of monitoring, including network audits, threat intelligence and security incident reviews, and malware analysis. This oversight is based on our own highly customized policies that are constantly fine-tuned so we can respond immediately and stay ahead of attacker trends. The Panasonic security team also automatically and proactively scans the underground hacking community to understand and defend against new and developing security threats. Coupled with Threat Intelligence advanced warning capabilities, our security posture is on par with many top fortune companies.

The Security Operations Center team members have a very critical role for ITC Global and its customers and undergo regularly scheduled training to maintain specialties in all areas of security, including: AppSec (Application Security), NetSec (Network Security), GRC (Governance, Risk, and Compliance).

ITC Global also anticipates the future of network security and incorporates artificial intelligence into its intrusion detection and prevention. Leveraging Panasonic's powerful security infrastructure support, ITC Global can apply the autonomous learning capabilities of all security-related devices to monitor network traffic automatically and block it when necessary.

Panasonic's overall security posture adds many advanced elements to ITC Global's capabilities. Breach assessment activities enable proactive analysis that gives the company and its customers' visibility into unidentified security threats before any negative impact may occur. Both ongoing penetration tests and certifications and compliance provide ITC Global valuable data about the security landscape.

6. Examples of security technology and practices used:

- IDS\IPS (Intrusion Detection\Protection System)
- Firewall
- Malware Analysis
- Network Device Hardening
- Ongoing Breach Assessment Analysis
- Ongoing Pen Testing
- Dynamic rotation of passwords on network elements

ITC Global and Panasonic also leverage industry-leading tools to coordinate users, devices, applications and activities across all network locations. The Exinda network management tool combined with next-generation security platforms can be integrated with customers' security systems with built-in firewall capabilities. The Exinda platform also allows ITC Global to manage customer traffic for shaping.

Exinda Platform Network Management Tool Offers:

- Integrated policy management for applications, users and groups
- Proactive alerts and recommendations to exceed customer SLAs
- Application monitoring, control and acceleration
- Purpose-built reports for common customer problems
- Recommendations based on network and application
- Elimination of unwanted traffic on customer networks
- Transparency into ISP committed service levels
- Insights into how network resources are being used
- Application performance scoring to detect user experience problems sooner
- Automated alerts sent to your NOC team when performance issues arise
- Interactive analytics for easy diagnosis and troubleshooting

7. Internet Access and Hub Firewalling

ITC Global and Panasonic operate all Internet POPs inside major, Tier 1 co-location facilities. In addition, ITC Global operates at least two (2) diverse Internet transit ports with separate providers. All Internet transit ports are equipped with firewall and security Intrusion Detection System (IDS) / Intrusion Protection System (IPS) equipment. ITC Global utilizes firewalls at all the teleports for Internet access. Only authorized ITC Global employees can manage the firewalls. All changes and modifications are tracked and logged to the specific authorized individual. ITC Global also establishes firewalls at every data center and teleport, and more importantly, places them at the network edge to mitigate illegitimate or threatening traffic.

ITC Global and Panasonic's terrestrial network consists of an MPLS, interconnecting multiple teleports and POPs around the world. The combined networks of Panasonic and ITC Global provide access via approximately 20 different teleports around the world.

The network is mainly based on Ethernet Layer point-to-point leased lines over which MPLS technology is deployed. All MPLS nodes have equipment deployed on a hot standby redundancy basis. The main MPLS Core provides connectivity between major POPs located in four business centers across the U.S.; London, UK; Perth, Australia; and Frankfurt, Germany. Each teleport is connected to the MPLS core via private leased lines with virtual private networks backups. Additional POPs are located in the U.S. and Europe.

8. Network Scanning

Clients' networks are separated at the Data layer (Layer 2) and clients cannot scan each other's networks. In addition to network scanning, ITC Global can provide content filtering utilizing a Websense appliance. Some network providers use only one type of network scanner to identify and validate potential exposures. This procedure cannot encompass other potential attack vectors that may impact your operational environment.

ITC Global addressed this issue directly by proactively ingesting various, different types of reports from tools that assess network infrastructure FW rules. These include Titania-Nipper, Nessus, Nexpose, Fortify, Burpsuite, Acunetix, and possibly others as the Defense-In-Depth Approach focuses on new threats and addressing them with the best tools available. By being able to look at different potential attack paths and determine weaknesses, we can better focus on needed remediation to address potential issues but most of all confirm our strong and resilient security posture.

9. Implementing Innovation for Future Security

Providing secure networks is very dynamic, and successful companies are committed to implementing the latest methods and technologies to ensure security into the future. ITC Global continuously researches and evaluates new ways to bring innovative security solutions to our customers. From development and testing, to full implementation, ITC Global takes all the needed steps to provide the best and most secure networks to our customers and employees.