CASE STUDY

Connecting Miami to Latin America with Cisco Meraki SD-WAN & VPN

Secure, high-performance connectivity across 3 international locations

CLIENT OVERVIEW

ICP Miami is a leading heavy equipment parts and machinery distributor with over 12 years serving the construction and mining industries. With headquarters in Miami, FL and operations spanning Panama and a second Latin American location, ICP coordinates high-value inventory, technical support, and customer service across borders daily.

3	99.9%	1
Locations Connected	VPN Uptime	Unified Dashboard

THE CHALLENGE

With operations across three countries, ICP Miami relied on fragmented, consumer-grade VPN connections between offices. IT visibility was nonexistent: staff experienced frequent connection drops during video calls, shared drives were inaccessible to remote teams, and security policies could not be enforced consistently across sites.

Cross-border file transfers — critical for parts lookup, purchase orders, and warranty documentation — were slow and unreliable, costing staff hours each week in workarounds.

OUR SOLUTION

Infinity Network Support designed and deployed a unified Cisco Meraki SD-WAN fabric connecting all three ICP locations under a single cloud-managed dashboard.

- Deployed Cisco Meraki MX security appliances at Miami HQ, Panama logistics hub, and the third Latin American branch
- Configured Auto VPN tunnels between all three sites with automatic failover and load balancing
- Implemented centralized firewall policies, content filtering, and IDS/IPS from a single Meraki dashboard
- Established QoS rules prioritizing VoIP and ERP traffic over best-effort data
- INS NOC provides real-time monitoring for tunnel health, bandwidth, and security events

RESULTS

- All three sites unified under a cloud-managed network — deployed in a single window with zero business disruption
- VPN tunnel uptime reached 99.9%, eliminating dropped connections that disrupted daily operations
- Cross-site file transfers became fast and reliable, enabling real-time collaboration on inventory and orders

- Full IT visibility across all three countries from one dashboard — no more site-by-site troubleshooting
- Consistent security policy enforcement across all locations reduced the attack surface significantly

TECHNOLOGIES USED

Cisco Meraki MX **SD-WAN** **Auto VPN** **IDS/IPS** **QoS** **INS NOC**

CASE STUDY

Cloud Infrastructure Migration Across Miami & Latin America

From on-premise silos to a unified Microsoft 365 environment across 3 countries

CLIENT OVERVIEW

ICP Miami operates across three international locations with teams that collaborate daily on parts inventory, customer orders, warranty claims, and supplier communications. As the company expanded its Latin American footprint, the need for reliable, always-available shared resources became critical.

100%	3	Hours
Users on MFA	Countries Unified	RTO (vs. Days Before)

THE CHALLENGE

ICP Miami's critical business data — inventory databases, customer records, supplier contracts, and ERP files — lived on aging on-premise servers at Miami HQ and unmanaged local drives at remote offices. Staff in Panama and other locations routinely worked off outdated file versions, leading to order errors and duplicated work.

No centralized identity management existed: departing employees retained access to company resources after offboarding. Disaster recovery was nonexistent — a server failure would have meant days or weeks of lost productivity and potentially unrecoverable data.

OUR SOLUTION

Infinity Network Support designed and executed a phased cloud migration to Microsoft 365 and Azure, tailored to ICP Miami's cross-border operational model.

- Migrated all email, documents, and shared drives to Microsoft 365 (Exchange Online, SharePoint, OneDrive)
- Deployed Microsoft Entra ID (Azure AD) for centralized identity management across all three locations
- Implemented Multi-Factor Authentication (MFA) and Conditional Access policies for all users
- Configured SharePoint team sites per department with role-based access controls
- Retired legacy on-premise file servers and migrated all shares to SharePoint with full permissions mapping
- Deployed automated cloud backup with immutable storage for ransomware protection

RESULTS

- All staff across three countries now access the same live files — version conflicts eliminated entirely
- Centralized identity management: employee offboarding now takes minutes, not days
- MFA deployed across 100% of accounts — credential-based breach risk dramatically reduced

- On-premise server infrastructure retired at Miami HQ, cutting hardware maintenance costs
- Recovery time objective reduced from days to hours with cloud-based disaster recovery

TECHNOLOGIES USED

Microsoft 365 **Microsoft Entra ID** **SharePoint** **Exchange Online** **MFA** **Conditional Access**

CASE STUDY

VoIP Deployment: One Phone System Across Miami & Latin America

Replacing fragmented phone lines with a unified cloud PBX across 3 countries

CLIENT OVERVIEW

ICP Miami's sales, technical support, and logistics teams rely on constant phone communication — with clients across South Florida, suppliers in North America, and internal teams in Panama and Latin America. Reliable, professional voice communication is a core part of how they serve customers and coordinate operations.

3	$0	1
Locations on One System	Inter-Office Call Cost	Business Phone Number

THE CHALLENGE

ICP Miami operated with a mix of traditional landlines at Miami HQ and consumer mobile plans at Latin American offices. There was no unified phone system: calls between offices were billed as international calls at full carrier rates, internal extensions didn't exist, and clients calling the Miami number could not be transferred to staff in Panama.

Call quality was inconsistent — particularly for Latin American offices where internet infrastructure is variable. Dropped calls during client negotiations were a recurring source of frustration and lost business.

OUR SOLUTION

Infinity Network Support designed and deployed a cloud-based VoIP solution integrating all three ICP locations under one phone system.

- Deployed cloud PBX platform with Miami as the primary business number, routing to all three locations
- Configured auto-attendant, call queues, and extension dialing across all three offices
- Provisioned desk phones and softphone apps (desktop + mobile) for all staff
- Implemented QoS on the Meraki SD-WAN network to always prioritize VoIP traffic
- Configured call recording, voicemail-to-email, and business-hours routing with after-hours overflow

RESULTS

- All three offices operate under one phone number — calls transfer seamlessly between Miami and Latin America
- Internal extension dialing between countries eliminated international call charges entirely
- Call quality issues resolved — Meraki QoS ensures VoIP traffic is always prioritized over best-effort data

- Staff can take calls from desk phones, laptops, or mobile — full flexibility for field and remote workers
- Professional auto-attendant significantly improved the first impression for all inbound callers

TECHNOLOGIES USED

Cloud PBX **VoIP** **Cisco Meraki QoS** **Auto-Attendant** **Softphone** **Call Recording**

CASE STUDY

Managed Backup & Recovery: Protecting Critical Data Across 3 Countries

Automated, immutable, tested backups — so data loss is never a business risk

CLIENT OVERVIEW

ICP Miami manages thousands of parts SKUs, supplier contracts, customer records, and financial data across three international locations. For a distributor operating at their scale, data loss from hardware failure, ransomware, or accidental deletion could halt operations and damage client relationships irreparably.

<24hr	3-2-1	100%
Recovery Point Objective	Backup Strategy	Locations Protected

THE CHALLENGE

Prior to engaging Infinity Network Support, ICP Miami had no formal backup strategy. Critical files lived on a mix of local servers, individual workstations, and USB drives managed by staff at each location. No backups were tested. No recovery plan existed.

The risk was significant: a single ransomware attack or hardware failure could have wiped out years of inventory data, customer history, and supplier contracts — with no path to recovery.

OUR SOLUTION

Infinity Network Support implemented a 3-2-1 backup strategy across all three ICP locations, with automated monitoring and regular recovery testing.

- Deployed INS-managed backup agents on all servers and critical workstations across all three locations
- Configured automated daily backups: local NAS copy, encrypted off-site replication, and immutable cloud backup
- Set retention policy: 30 daily, 12 weekly, 12 monthly recovery points
- Implemented ransomware-resistant immutable storage — backups cannot be encrypted or deleted by malware
- Connected backup health monitoring to INS NOC for real-time alerts on failures or anomalies
- Conducted initial full recovery test to validate RTO/RPO targets and prove backups actually work

RESULTS

- All critical data across all three countries is now protected with automated, monitored daily backups
- Recovery Point Objective (RPO) under 24 hours — worst case, ICP Miami loses one day of data, not everything

- Ransomware-resistant immutable backups ensure no attacker can encrypt or destroy the backup chain
- First recovery test completed successfully — ICP Miami has proof their data is recoverable
- INS NOC monitors backup health daily and alerts before failures become data loss events

TECHNOLOGIES USED

Managed Backup **Immutable Cloud Storage** **3-2-1 Strategy** **INS NOC** **Ransomware Protection** **Recovery Testing**

CASE STUDY

XDR Deployment: Enterprise Threat Detection Across Miami & Latin America

Unified endpoint detection, behavioral analysis, and automated response — 24/7

CLIENT OVERVIEW

As a company handling high-value inventory, supplier contracts, and financial transactions across three international locations, ICP Miami represents an attractive target for cybercriminals. With staff connecting to shared cloud resources from Miami, Panama, and a third country, the attack surface spans borders and time zones.

24/7	Minutes	3
SOC Monitoring	Automated Isolation	Countries Protected

THE CHALLENGE

ICP Miami's endpoint security consisted of basic antivirus — a technology largely ineffective against modern threats like fileless malware, living-off-the-land (LOTL) attacks, and ransomware. With staff across three locations, a threat on any one device could propagate laterally across the entire environment before anyone noticed.

There was no central security visibility, no alert correlation, and no incident response plan. Any breach would have been entirely reactive — meaning significant damage would already be done before detection.

OUR SOLUTION

Infinity Network Support deployed an Extended Detection and Response (XDR) solution across all three ICP locations, integrated with Microsoft 365 and monitored by the INS Security Operations Center.

- Deployed XDR agents on all endpoints (workstations, laptops) across all three countries
- Integrated XDR with Microsoft 365 for identity-based threat detection: suspicious logins, OAuth abuse, and email compromise
- Configured behavioral detection for LOTL techniques, lateral movement, and privilege escalation
- Enabled automated response playbooks: isolate compromised endpoint, kill malicious process, alert INS SOC
- Connected XDR telemetry to INS SOC for 24/7 human-led monitoring and incident response
- Delivered initial threat assessment identifying pre-existing risks and misconfigurations for immediate remediation

RESULTS

- Full endpoint visibility across all three countries — INS SOC monitors every device from one console

- Behavioral detection catches threats that signature-based antivirus misses entirely
- Automated response isolates compromised endpoints in minutes, containing the blast radius before damage spreads
- Microsoft 365 integration means account compromise attempts trigger immediate alerts and automated actions
- Initial threat assessment uncovered several critical misconfigurations — remediated before they became incidents
- ICP Miami now meets the security posture expectations of enterprise suppliers and international partners

TECHNOLOGIES USED

XDR **INS SOC** **Endpoint Detection** **Microsoft 365 Integration** **Behavioral Analysis** **Automated Response**
