CLIENT:	MAU Workforce Solutions
INDUSTRY:	Workforce staffing
SIZE:	Mid-market, 200 employees
LOCATIONS:	10 across the eastern US
CHALLENGES:	- Network reliability across their VPN - Firewall-related network and end-user downtime disrupting the business - Lack of consistent security configuration and management across all of their locations

UTG | Business. Driven. Technology.

United Technology Group (UTG) helped a workforce staffing company improve their network security and overall reliability with Cisco technology

Like many growing mid-market organizations, MAU Workforce Solutions (MAU) was focused on implementing technology that would help them meet their demanding business objectives. But as network security and reliability became bigger challenges, they knew they needed help. United Technology Group (UTG) was able to work with MAU to architect a Cisco-powered security solution that would not only help them address the challenges they were facing, but also create an automated security infrastructure that could grow with them while protecting their organization from advanced cyberthreats.

> ...THEY WERE SPENDING TOO MUCH TIME MANAGING THEIR VPN AND THE SECURITY OF THE NETWORK...

The situation, challenges, and needs

In an accelerated growth pattern, MAU's IT team found that they were spending too much time managing their VPN and the security of the network between their ten locations. The low-cost WatchGuard firewalls they had purchased were creating VPN stability issues, and because the tools in their security infrastructure were not built to work together, discovering and remediating security incidents were incredibly time consuming.

Their specific network and security challenges included:

VPN RELIABILITY:

There were VPN stability issues which required constant attention from their IT team

FIREWALL-RELATED DOWNTIME:

Firewall lockups were causing end-user downtime and disrupting the business

MISSING COMPONENTS:

Their security infrastructure didn't include intrusion prevention or malware protection

SECURITY MANAGEMENT:

Maintaining security without centralized configuration and management was time consuming

Over time, the WatchGuard firewalls were becoming an actual roadblock to conducting business – faltering growth and creating more headaches than results. MAU knew it was time to make a change. They evaluated several proposals and ultimately decided to work with UTG – a company known for their reliability and breadth of experience with mid-market organizations.

United Technology Group’s solution

After discussing their needs and challenges with key stakeholders, UTG recommended a network security solution powered by Cisco technology. In addition to eliminating their VPN reliability and security management challenges, UTG’s solution would provide a more stable platform, as well as the intrusion prevention and malware protection capabilities they lacked in their current security infrastructure.

> **UTG’S SOLUTION WAS BUILT USING BEST-IN-CLASS CISCO TECHNOLOGY AND WAS IMPLEMENTED BY THEIR WORLD CLASS PROFESSIONAL SERVICES TEAM.**

AMP provides advanced malware protection and enables MAU to rapidly detect, contain, and remediate threats that evade front-line defenses

Cisco Advanced Malware Protection (AMP)

The ASA Firewalls provide best-in-class threat protection and enable MAU to consolidate multiple layers of security into a single platform

Cisco Adaptive Security Appliance (ASA) Firewalls

CDO enables MAU to orchestrate and manage security policies across their entire network from one cloud-based application

Cisco Defense Orchestrator (CDO)

Firepower Management Center acts as the nerve center and provides unified management over their firewalls, apps, IPS, URL filtering, and AMP

Cisco Firepower Management Center

Cisco security products leverage security intelligence and analytics from Cisco Talos. They are a dedicated group from Cisco that analyzes millions of malware samples per day across 1.6 million global sensors. Visit **www.talosintelligence.com** to learn more about them.

A phased approach to implementation was used to avoid any impact to productivity. After allowing the initial Cisco technology to collect data for a couple of weeks to build a baseline, UTG reviewed the reports with MAU’s IT team to identify any processes or traffic that required attention before fully rolling out the other components of their solution.

The results and ultimate benefits

Prior to the migration, MAU had experienced firewall lockups every few months. But since UTG’s Cisco solution has been implemented, they have not had any firewall-related downtime or VPN stability issues. Although the solution required a bigger investment than other options they had considered, UTG and Cisco enabled MAU to continue their growth without the constant downtime and reliability issues associated with their previous security infrastructure.

BUSINESS OUTCOMES

- Security infrastructure that can grow with the business
- Better protection against modern cyberthreats
- Improved network reliability and stability
- IT resources can focus more on supporting the business

IT OUTCOMES

- Little to no security-related downtime
- Improved security visibility across all their locations
- The ability to manage security from one location
- The ability to categorize network traffic

See how UTG can improve the security and reliability of your network

Cyberattacks are becoming more sophisticated and harder for IT professionals to manage. If you’d like to learn how we can help you build a reliable solution to secure your network and improve visibility, schedule a meeting today by visiting **www.utgsolutions.com/contact**.