CLIENT:	East West Manufacturing
INDUSTRY:	Contract manufacturing
SIZE:	Mid-market, 500 employees
LOCATIONS:	5 locations world wide
CHALLENGES:	- Malware constantly affecting their network - Creating a layered approach to security - Getting rid of manual security processes - Securely sharing core applications with international locations

UTG Business. Driven. Technology.

United Technology Group (UTG) helped a global manufacturing company stop constant malware attacks through a layered approach to security

East West Manufacturing (East West) was one of many mid-market organizations that felt a firewall could provide an effective security infrastructure. But as malware issues continued to affect their operations and create security concerns when sharing applications across international locations, they quickly realized they needed much more. United Technology Group (UTG) was able to work with East West to build a layered approach to security capable of stopping malware before it infiltrated their network and protecting their organization from a growing list of advanced cyberthreats.

> "We trusted UTG to analyze the business problem, come up with a solid solution that fit our needs, and implement it with as little disruption as possible."
>
> EAST WEST MANUFACTURING

The situation, challenges, and needs

Because East West was relying on basic firewall features to protect their organization from cyberthreats, they were experiencing constant malware issues. These issues were affecting network operations, taking up their IT team's bandwidth, and making it difficult to provide a secure environment for their international locations to access core applications hosted in their United States headquarters.

Their specific network and security challenges included:

CONSTANT MALWARE ISSUES:

Malware attacks were affecting network functionality and their overall IT operations

MISSING SECURITY LAYERS:

Their security infrastructure offered limited malware detection and prevention capabilities

LOTS OF MANUAL PROCESSES:

Maintaining their security posture required a number of manual processes

SHARING APPS INTERNATIONALLY:

Shared applications with foreign locations created exposure to additional security threats

East West tried incorporating anti-virus software, OpenDNS, and disk encryption, but realized that their security infrastructure could not provide the layers of security necessary to stop the malware attacks from affecting their network. At that point, they reached out to UTG – a Cisco partner known for their breadth of experience with mid-market organizations – for some expert advice.

United Technology Group's solution

After discussing East West's needs and challenges with key stakeholders, UTG recommended that they replace the basic firewall at their US headquarters with a Cisco ASA Next-generation Firewall, as well as implement Cisco Advanced Malware Protection and Firepower Management Center. By adding next-gen firewall capabilities, best-in-class malware detection, and unified management to their security infrastructure, East West would be able to stop malware before it could infiltrate their network, and stave off security threats that came along with sharing applications internationally.

UTG'S SOLUTION LEVERAGED BEST-IN-CLASS CISCO TECHNOLOGY TO CREATE A TRULY LAYERED APPROACH TO SECURITY.

AMP provides advanced malware protection for end user devices and enables East West to rapidly detect, contain, and remediate malware threats

Cisco Advanced Malware Protection (AMP)

The ASA Firewall at their US headquarters provides best-in-class threat protection and enables East West to consolidate multiple layers of security into a single platform

Cisco ASA Next-generation Firewall

Firepower Management Center acts as the nerve center by providing deep visibility into their network, streamlined management, and security automation

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.

The results and ultimate benefits

Prior to the Cisco technology, malware was regularly affecting East West's network and taking valuable time away from their IT team. But after the implementation by UTG's professional services team, they saw immediate results and have not had a single successful malware attack since.

BUSINESS OUTCOMES

- Incredible reduction in successful malware attacks
- Organization-wide confidence in overall security
- The ability to share core applications across international locations with less security risk

IT OUTCOMES

- Zero malware tickets since the implementation
- Malware attacks are stopped before infiltrating the network
- Streamlined security management and oversight
- More interoperability within their security infrastructure

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

As your network grows in size and geographic complexity, so does your attack surface area. Having a layered approach to security and tools in place that allows you to centrally manage it will significantly reduce your security risk. 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**.