Cisco Distribution Partner

INGRAM MICRO

Fly higher.

PROFITABILITY SOLUTION STUDY: ENTERPRISE

How to provide a commercial enterprise with centralized management capabilities for all security functions

Here's a hypothetical example of how to design and sell a cost-effective security solution to a commercial enterprise with multiple locations worldwide. See how a Cisco Security solution can be customized to address the challenges posed by today's threat landscape—and how resources from Cisco and Ingram Micro can help facilitate the sale and maximize your profits.

Environment

- 2,500 employees using desktops, laptops and mobile devices
- Multiple offices worldwide
- BYOD environment
- Experienced IT staff with some security expertise
- Mobile and telecommuting workforce

Pain points

- With so many employees connecting remotely using multiple devices, the company needed the ability to monitor the online activity of everyone with access to the network—through the implementation of application visibility and controls, content filtering and blocking inappropriate web content.
- The company was looking for a security solution that could accommodate future growth and expansion.
- The company was looking for comprehensive next-generation firewall capabilities and the ability to manage them from one centralized location.
- Email security, data loss prevention and encryption capabilities were essential requirements—combined with high availability and resiliency.
- The ability to support remote VPN users—and protect them on and off the VPN—was also critical.
- The IT team wanted to be able to tie security solutions into an Active Directory so they could utilize user ID information to create group policy and speed up remediation.
- The IT team was also looking for tools to provide ongoing security intelligence and reporting capabilities.

Risk factors

- Employees' use of their own devices and their non-business-related online activity could leave the company susceptible to malware and ransomware threats.
- The company handles large quantities of highly sensitive information, so the financial risks of data breaches are particularly acute.

The custom Cisco Security solution

Cisco 2X Firepower 2140 next-generation firewall with full TMC license

- 2X Firepower 2140 NGFW provides full hardware redundancy.
- TMC license provides threat-based Intrusion Prevention System (IPS), Application Visibility and Control (AVC), Advanced Malware Protection (AMP) for Networks and URL filtering to protect users from malware and other threats as well as boost employee productivity.

Cisco AnyConnect Apex VPN licenses support client or web-based SSL VPN (Secure Sockets Layer virtual private network) capabilities.

- Includes connector software to support AMP for Endpoints and Cisco Umbrella from a single client interface
- AC Apex license required for ISE endpoint compliance and remediation integration

Cisco Advanced Malware Protection (AMP) for Endpoints—AMP offers best-in-breed endpoint malware protection, including the ability to support batch deployment to multiple endpoints simultaneously. A cloud-based solution, it provides a high level of resiliency.

- Offers high visibility into the endpoint network, giving IT administrators the ability to determine which machines were impacted during a breach and the damage that was done—speeding up network remediation and the patching of vulnerabilities
- Provides information on more targeted threats and a prioritized list of vulnerable software
- Integrates with Active Directory to provide identity information, making it easier to identify vulnerable endpoints and users

Cisco Cloud Email Security Premium—This cloud-based solution provides inbound (antimalware/antispam protection) and outbound (DLP and encryption) security services as well as a high level of resiliency.

Cisco Umbrella platform—This cloud security platform offers companies complete visibility into all internet activity across all devices and users. It automatically uncovers current and emerging threats and blocks them before they can reach the network or endpoints.

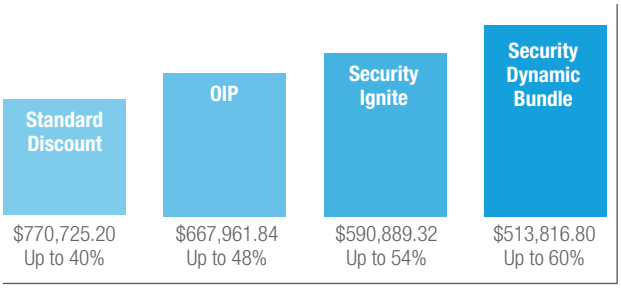
- Offers easy setup and configuration of base policies—in under 10 minutes
- Blocks DNS-based malware requests
- Monitors all ports and protocols to help detect and prevent ransomware “phone home” activity
- Works for users on and off the network
- Integrates with Active Directory to identify users who are vulnerable or out of compliance
- Includes Umbrella Investigate, which allows users to dig deeper into suspected malicious activity and create alerts around high threat scores and indicators of compromise to speed up response to malicious activity

Cisco Identity Services Engine (ISE)—This network administration product enables the creation and enforcement of security and access policies for endpoint devices connected to a company’s routers and switches.

- 4X servers to support redundant admin and logging servers
- Authentication servers covering two sites, each with up to 7,500 concurrent device connections
- Includes a base license for basic AAA/radius authentication and guest wireless portal creation
- Also includes a license to provide BYOD access for users to self-connect their personal devices to the network based on user privileges and device type—and an Apex license for endpoint compliance and remediation capabilities in conjunction with AC Apex
- Deployment licenses to support two devices per user in a 2,500-employee company (for a total of 5,000 concurrent device connections.

Promotions from Cisco and Ingram Micro

Cisco offers a variety of special pricing plans and promotions to help maximize profitability. To see the discounts available with Cisco Security’s latest profitability bundles, refer to this graph.



Additional sales resources

- Dedicated Ingram Micro channel account specialist (CAS) for help with programs, promotions, incentives
- Onsite and virtual training through Cisco Experience Center
- Certification opportunities through Ingram Micro Training Academy

Contact Collin Rauen to learn more.