Selling Trend Micro Solutions for Ransomware: Start Here!

Ransomware has rapidly emerged as a significant threat to businesses and organizations of all sizes. Your customers and prospects need a plan to minimize the risk of this high profile threat. With Trend Micro, you can help them avoid the business disruption, loss of productivity, damage to brand reputation and legal implications that come along with recovering from a ransomware attack.

Along with the questions and answers below, you can get help:

- **Through Sales Library**. Resources include customer presentations (ransomware-specific and in all solution presentations), a solution brief, sales training content, and more. Partners can access this through the Trend Micro Partner Portal.
- **Through Chatter:** Get immediate selling help from solution experts *<Trend Micro sellers only>*
- **Online:** Refer your customers to http://www.trendmicro.com/enterprise-ransomware

Getting started: Understanding how they are thinking of or dealing with ransomware currently

Questions	Answer & discussion topics
How frequently have you encountered ransomware in your organization in the past 3 months?	• If not, are they worried about it? Email is the number one attack vector and fastest way to reduce risk. • If they are experiencing attacks, ask where they are seeing the attacks (email/web, endpoints, servers). Additional discussion topics on each area are listed below. Remember that Network visibility can also help with ransomware.
Do you use an automated backup and recovery system for your critical data? Do you have a program to educate employees on the hazards and prevention of phishing attacks?	· This question will simply help you understand how they are positioned to deal with a ransomware attack, today and in the future. If they don't have a good backup plan and aren't educating employees, they are at a higher risk, though these programs aren't enough protection from ransomware.

Email-specific conversations: Trend Micro has blocked 100M ransomware attacks since October, 2015, and 99% of those were via email or web attack vectors. ***Email is your number one opportunity*** to quickly help customers and prospects lower their risk of ransomware.

Question	Answer & discussion topics
Are you using advanced detection techniques (ex: sandboxing, unknown threat detection, spear phishing detection, social engineering attack prevention) to enhance your email deployment (on-premise or in the cloud)?	• **On-Premise:** Even if they are using an email or web gateway, they can reduce risk by deploying advanced security from Trend. For Trend customers using our gateways, focus on selling Deep Discovery Inspector. For non-Trend customers, focus on selling Deep Discovery Email Inspector • **Office365:** The built-in security of O365 is not enough to protect your organization from the number 1 attack vector for ransomware. Reduce risk and add a layer of protection to detect unknown ransomware threats with malware scanning, sandbox analysis, and web reputation security. Trend Micro Cloud App Security has blocked more than 2 million threats in Office 365.

Endpoint-specific conversations: End-users are an organization's biggest risk point and need to be protected. A layered approach to protecting those endpoints is the best way to reduce risk and protect an organization from data loss and business disruption.

Question	Answer & discussion topics
Are you using any technologies beyond traditional anti-virus to protect your endpoints from ransomware? (e.g., Behavior monitoring, application control, endpoint detection, and response)	• There is **no silver bullet** when it comes to protecting your endpoints against ransomware. Organizations should leverage multiple next-generation threat protection techniques to reduce the risk of ransomware. • **Smart Protection Suites** deliver the broadest range of advanced ransomware protection techniques, such as ransomware behavior monitoring, memory inspection, and lateral movement detection. These are combined with other ransomware protection capabilities like vulnerability shielding and application control—all in a single, integrated, high-performance solution, with centralized visibility and control.

Network-specific conversations: Email and web are common ways ransomware enters organizations, but other attack methods like island-hopping or allowing unmanaged devices on the network can also create risk. A network defense strategy is key to stopping ransomware from accessing and spreading within an organization's network.

Question	Answer & discussion topics
Do you have a single source of visibility and insight into malicious payloads and threat activity across all physical and virtual segments of your network?	• If no, they should **implement a breach detection** solution to gain visibility into malicious payloads and threat activity across all segments of your network. (Deep Discovery) • If yes, what? Ask: Are you monitoring all north-south and east-west traffic? If a device with an IP address is infected with ransomware, do you have visibility into attempts by criminals to discover other assets and file shares and/or to move laterally within your network? (Deep Discovery can help

Hybrid Cloud-specific conversations: While end-users (especially via email) may be an organization's biggest risk point, once infected they also may be connecting to corporate file shares, putting corporate data at risk. Server vulnerabilities can also be an attack vector for ransomware that can debilitate a business by shutting down critical applications.

Question	Answer & discussion topics
Are you running perimeter-only security (IPS) in your enterprise? Running any end-of-support systems in your data center (ex: Windows Server 2003)?	• If yes, they should complement with **Deep Security** to help protect servers (physical, virtual, cloud) from attacks (east-west traffic), compromised users accessing file shares, and vulnerabilities (remember Windows 2003) that could be used to inject ransomware and hold them hostage. • For an incumbent host vendor: are they protected against OS **and** application threats that could be used to inject ransomware? **Deep Security** has comprehensive security (1000s of rules) to help protect servers (physical, virtual, cloud), including specialized protection for Windows & Linux file servers that may be at risk of attack from a compromised end user that could be used to inject ransomware and hold them hostage.