Conversation Guide – Partner Breach Readiness and Response

Follow these tips when discussing Cisco's Breach Readiness and Response offerings with customers

CONVERSATION STARTERS – WHY IS BREACH READINESS AND INCIDENT RESPONSE SO IMPORTANT?

- **Rising number of security incidents.** With more than 5 million records stolen worldwide every day, according to the data breach statistics of BreachLevelIndex.com, and 3 times more incidents than 4 years ago, breach protection and incident response have become topics of prime importance. The ability to prevent incidents from happening in the first place, and to effectively respond to incidents if they should happen, is critical to every organisation. Customers need to establish a process that will ultimately help them to:
    - Maintain business continuity
    - Protect their reputation and employee morale
    - Avoid fines, legal fees, and remediation costs

- **Endpoints are the primary point of entry for attacks.** According to IDC, an estimated 70% of breaches start on endpoint devices (IDC: Effective Incident Detection and Investigation Saves Money, 2016). Why on the endpoint? The main reasons are:
    - **Gaps in protection**: when users are off the corporate network, antivirus is often the only endpoint protection available. This is not enough when it comes to today's advanced threats.
    - **Gaps in visibility**: organisations often have limited visibility into user and endpoint activity. They are unable to determine the cause of the breach (where the malware came from, what it is doing, which systems have been compromised).
    - **User error:** a large number of attacks bypass the endpoint defences due to user error (e.g. despite trainings, users are going to open phishing emails with a malicious file or link)

- **The approaching GDPR deadline adds urgency.** On 25th May, 2018, the European Union (EU) General Data Protection Regulation (GDPR) will come into force. It will apply to all organisations that do business in the EU, regardless of where the business entity is located (i.e. in a Non-EU country). GDPR requires "appropriate security" and "due diligence" to protect personal information from data breaches. GDPR also urges companies to have a strong data protection programme to address in stringent timeframe attacks, incidents, and leakage of personal information. Organisations will have 72 hours to report breaches.

- **Take your Breach Readiness and Response capabilities to the next level.** Organisations take, on average, 191 days to detect a breach and 66 days to contain it. (Source: Ponemon Institute, Cost of Data Breach Study, 2017). Cisco's Advanced Threat solutions can help to strengthen your security posture. Cisco blocks 20 billion threats daily - with a median time to breach detection of 3.5 hours.

EXPLAIN THE SOLUTION: HOW TO STRENGTHEN THE SECURITY POSTURE

The three building blocks of the solution

AMP for Endpoints
Next-Gen Endpoint Security

A cloud-managed endpoint security solution that prevents cyberattacks and rapidly detects, contains, and remediates malicious files on the endpoints

Key Features

- antivirus inspection engine
- machine learning
- static and dynamic file analysis (sandboxing)
- vulnerability monitoring
- continuous analysis of file behaviour
- retrospective detection

www.cisco.com/go/ampendpoint

Do a dCloud Demo

Offer a free trial

+

Umbrella
Secure Internet Gateway

Cloud-delivered network security service protecting users on and off the corporate network, anywhere they go, even when not using the VPN

Key Features

- offers both DNS and IP Layer enforcement to block malware, phishing, and command & control callbacks over any port or protocol
- increased visibility into internet activity across all locations and users

www.cisco.com/go/umbrella

Do a dCloud Demo

Offer a free trial

+

Incident Response Services
Cisco Security Experts

Immediate access to skilled incident responders with years of experience. The experts can respond within 4 hours by phone and be deployed to the customer's location within 24 hours

Key Features

- protect the business with a stronger security posture
- adhere to compliance and regulatory demands
- quickly react and respond to incidents
- 24-hour access to assigned and dedicated security professionals

www.cisco.com/go/securityservices

DISCOVERY QUESTIONS TO QUALIFY A BREACH READINESS OPPORTUNITY

- Does the customer know that 70% of breaches start on the endpoint? (Source: Effective Incident Detection and Investigation Saves Money, IDC, 2016)
- Does the customer have advanced breach detection capabilities?
- Does the customer have processes and procedures to identify those breaches that may impact privacy, and to report those within 72 hours after becoming aware of them? (GDPR Compliance)
- Does the customer have in-house skills to detect, contain, and remediate a breach?
- How is the customer preparing to address potential threats? Is the customer planning to manage by themselves, or outsource?
- For the most recent infection, how long did it take the customer to figure out how the attack originated, what endpoints were impacted, and what the malware did?
- How does the customer protect endpoint devices when they are off the corporate network?
- Does the customer have a way to automatically detect malicious file behaviour once that file is already on the endpoints?
- What is the customer currently doing for recursive DNS security and visibility organisation-wide?

OBJECTION HANDLING

Customer Objections	How to respond
We are already well protected. We have a firewall, IPS, and antivirus solution.	Advanced malware can evade even the best front-line defences. Point-in-time detection products, like antivirus, firewalls, and intrusion prevention systems inspect traffic at the point of entry into your network to prevent breaches, but they will never detect 100 percent of all the threats. Prevention is a very important part of Breach Readiness, but it is not enough. You need to go beyond prevention and be ready with technology that can quickly detect, contain, and remediate malware that evaded the front-line defences and got inside. A strong Breach Readiness and Response solution is based on three main capabilities: **Prevent – Detect – Respond** Cisco AMP for Endpoints and Cisco Umbrella are two security solutions that work together to prevent, detect and respond to attacks targeting endpoints. Endpoints are the primary point of entry for malware attacks. According to IDC, an estimated 70% of breaches start on endpoint devices **Prevent:** ○ **AMP for Endpoints:** blocks known malware at initial inspection (point-in-time) and uses advanced sandboxing capabilities to analyse unknown files

	○ **Umbrella:** Blocks malicious internet requests (domain, URL & IP) requests, regardless of delivery mechanism (email, web, etc.) **Detect:** ○ **AMP for Endpoints:** Continuously analyses all file activity on endpoints to quickly detect malicious behaviour and retrospectively alerts security teams ○ **Umbrella:** Prevents Command and Control (C2) callbacks to attacker's servers to stop data exfiltration and execution of ransomware encryption **Respond:** ○ **AMP for Endpoints:** Shows the full history and context of a compromise (point of entry, path of the malware through the network, what systems were affected, what the malware did and is doing now). Eliminates the root cause, making sure the malware is thoroughly eradicated from the network to prevent reinfection ○ **Umbrella Investigate:** Provides up-to-the-minute threat data and historical context about domains, IPs, and file hashes for faster investigation
If something gets in, I simply reimage my systems.	No need to always reimage systems. AMP for Endpoints gives the ability to surgically remediate and pull files out of memory across multiple endpoints at one time with the click of a button. Because AMP for Endpoints knows where the malware came from, where it has been, and what it is doing, it can pinpoint its location across your extended network and eliminate it with limited or no collateral damage.
Our roaming workforce is well protected. They use the VPN when they are off the corporate network.	The reality is that not every connection goes through the VPN. Employees are using cloud apps and will sometimes also be leveraging their work laptops for personal use. Users can access the internet from any location and your existing perimeter security loses visibility and can't provide protection. According to IDG, 82% of workers admit to not always using the VPN. Roaming laptops keep getting infected when off the corporate network. Umbrella offers a simple, unobtrusive way to protect users wherever they're working. Umbrella enables security no matter where the endpoint is located, even if they aren't using the VPN.
We already invested heavily in security technology from other vendors. We need to protect our existing investments.	Umbrella's API enables integration with other systems including security appliances, threat intelligence platforms or feeds, and custom in-house tools — enabling you to amplify investments you've already made. Nor is AMP for Endpoints a siloed point product. It has an API that lets you sync AMP for Endpoints with you other security tools or SIEMs.
We already have security products from other vendors deployed in our IT environment. We don't have the	Naturally, managing multiple security products from different vendors means increased efforts to build, integrate, manage, and run the environment. Also, when you deploy multiple security products from different vendors, they don't always communicate or share

bandwidth to deploy and manage additional security solutions.	information. This means that finding threats and remediating them will take longer. With a set of integrated security solutions from Cisco, all communicating and working together, it results in an easier-to-manage security architecture. **Umbrella** is the simplest security product you'll ever deploy. Protect all devices on your network, all office locations, and roaming users in minutes. Just sign up, point your DNS, and you're done. By performing everything in the cloud, there is no hardware to install, and no software to manually update. **AMP** is also a cloud-based "software-as-a-service" endpoint security solution, and deployment is simple. Basically, it's done in four simple steps: you set up your account, you choose the number of endpoints, you choose a subscription term (1, 3, or 5 years), you deploy the AMP lightweight connector on your endpoints and synch with your account.
We are understaffed. We don't have the in-house skills. Too complicated.	Incident Response Services can help you strengthen your security programme. Cisco Security experts will work with your IT team to design a mature Breach Readiness and Incident Response approach. Check out the different service offers and SLAs to find the right option for your needs.

NOTE

- By discussing a customer's Breach Readiness needs, you'll likely discover other security and networking needs that turn into up-sell and cross-sell opportunities.
- Determine if the customer is overspending (e.g. due to a complex patchwork of security point solutions). This is a great opportunity to highlight hardware and licensing packages, as well as your managed service offerings that create a holistic solution for the customer.
- Understand whether the customer has problems with their current security solution and is looking for an easier to manage, tighter integrated (architecture-based) security approach.
- Breach Readiness and Incident Response are also important aspects of Digital Transformation projects. Digital business models require a strong cybersecurity foundation.
- You can find additional demand generation material on Partner Marketing Central:
    - Ransomware Defense and IoT Threat Defense: http://cisco.pmclinks.com/6LAJa
    - Network Security (Security Solution Bundles): http://cisco.pmclinks.com/6LACk
    - General Data Protection Regulation (GDPR): http://cisco.pmclinks.com/6LAJe