NEWS RELEASE

Cisco Doubles Down on Security Innovation and Investment to Protect the Endpoint and Email

2018-04-16

Cisco Introduces New Email Security Services to More Effectively Prevent Phishing and Spoofing Attacks SAN FRANCISCO, April 16, 2018 (GLOBE NEWSWIRE) -- **RSA** — Employees remain an organization's greatest asset however they can be a risk when it comes to cybersecurity. Attackers are crafting highly targeted, fraudulent emails that look legitimate and use them to deliver malware to unsuspecting users. When successful, it costs the majority of companies $500K or more in lost revenue, customers, opportunities, and out-of-pocket costs.[1] To combat the rise of advanced threats targeting employees, Cisco is announcing new email security services to protect users from these fraudulent emails, as well as new capabilities to protect employees' devices from ransomware, cryptomining, and fileless malware.

Nearly all endpoint security solutions on the market claim to block 99 percent of malware. But what about the one percent of threats that evade detection using sophisticated techniques? Cisco® Advanced Malware Protection (AMP) for Endpoints, a cloud-managed endpoint security solution, prevents attacks and helps uncover the one percent of threats that can cripple a business. Cisco is adding a number of new capabilities to AMP for Endpoints, including:

- **Sophisticated detection and protection mechanisms to stop today's threats, including ransomware, and cryptomining:** Cisco is now bolstering its threat protection even when a user is offline. The new AMP for Endpoints exploit prevention helps protect against fileless attacks, including those that reside solely in memory. Cisco AMP's new malicious activity protection stops ransomware execution, killing the processes and preventing propagation.
    - Cisco threat researchers analyzed ransomware variants to identify the common techniques used for encryption. The result: a new engine that continuously protects against ransomware encryption and propagation to keep businesses safe from ransomware.
    - Fileless malware has recently gained popularity in part because of the difficulty in detecting it. Built directly into the foundation of Cisco AMP is a new protection mechanism that requires no tuning or adjustments to stop these threats. It protects against unpatched software vulnerabilities and keeps working around the clock, even when users are offline.

- **Threat investigation with Cisco Visibility,** a new cloud application built into the endpoint console which simplifies and accelerates security investigations so security analysts can rapidly investigate incidents with confidence, quickly and at scale. It ingests, normalizes, and enriches security events and provides a visual representation of the extent of a compromise spanning from endpoints to network to cloud.
    - Cisco Visibility combines threat intelligence from Cisco Talos™ and third parties with internal security event and alert data from across an organization's security infrastructure to simplify investigations, reduce complexity, and shorten incident triage and remediation time.
    - Visibility minimizes the need to switch between multiple consoles to perform common tasks. With a few simple clicks, a user can dive deeper into the data from Talos, Cisco Umbrella Investigate™, Threat Grid, AMP, and other sources to quickly understand how observables exist in an environment and how they relate to each other.

Cisco invests in new email security services
No matter how much the threat landscape changes, malicious email and spam remain vital tools for adversaries to distribute malware, and many of these threats reach the endpoint. Organizations must protect their own company domains from being misused as the delivery mechanism of malicious emails, as well as protect their internal users from phishing and spoofing attacks from emails with suspect senders.

Cisco is helping address these issues and more effectively prevent email identity deception used in phishing attacks. Cisco has concluded an OEM agreement with Agari to market and sell new services that enhance its Email Security product. The new email security services introduced include:

- **Cisco Domain Protection:** Automates the process of using email authentication to prevent phishing, protect brands from fraud, and maintain email governance by analyzing, updating, and taking action against senders misusing their domain to send malicious email. This service uses Domain-Based Message Authentication, Reporting, and Conformance (DMARC), an email authentication standard, and real-time reporting back to domain users about noncompliant emails being sent from their domains. This will be a requirement for many organizations in the future, and as of October 2017, the U.S. Department of Homeland Security ordered federal agencies with .gov email domains to fully implement strict DMARC policies by October 2018.
- **Cisco Advanced Phishing Protection:** Adds sophisticated machine learning capabilities to Cisco Email Security to block advanced identity deception attacks for inbound email by assessing its threat posture. It also uses both global and local telemetry data combined with analytics and modeling to validate the reputation and authenticity of senders. This helps organizations understand which emails carry targeted phishing and business email compromise (BEC) attacks so only legitimate emails reach an employee inbox.

Deployment through managed security services
To enable customers of all sizes to realize the benefits of these new capabilities, Cisco is expanding its relationship with ConnectWise so managed service providers (MSP) can offer Cisco Security as a part of their portfolio. The expanded relationship will offer the new ConnectWise Advanced Security Dashboard. This cloud management platform fully integrates with the ConnectWise Manage business management solution and complements ConnectWise Unite with Cisco, the existing portal for MSPs based on leading Cisco cloud-managed products. The new ConnectWise Advanced Security Dashboard provides MSPs with the ability to deliver managed security services with Cisco's security portfolio including Cisco AMP for Endpoints, Cisco Umbrella, Cisco Stealthwatch® Cloud, Cisco Adaptive Security Appliances, Cisco Next-Generation Firewall, and Cisco Meraki® MX appliances.

"Cisco understands that protecting employees and their endpoints requires more than just antivirus. Attackers leverage the Internet, email, and the network as vectors for breaching the endpoint," said Jeff

Reed, Senior Vice President of Product for *Cisco's* Security Business Group. "We deliver greater employee protection using cloud-delivered defense against threats hosted on the Internet. Cisco is also now one of the few organizations paving the way toward eliminating email identity deception. Through our expanded partnership, investments, and technology innovations, we are committed to delivering to our customers the best email and endpoint protection."

Supporting Resources:

- Infographic: Cisco Security Driving Innovation and Growth By The Numbers
- Blog: Protecting users, and uncovering the last 1% of threats
- Blog: New Cisco and ConnectWise Solution Helps MSP Capitalize on the Growing Managed Security Services Opportunity
- Cisco Email Security
- Cisco AMP for Endpoints

About Cisco
Cisco (NASDAQ:CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

_____
[1] Cisco Annual Cybersecurity Report 2018.

Press Relations
Raquel Prieto
408-527-3754
raqpriet@cisco.com

Analyst Relations
Jenna Duston
408-424 7210
jeabeyta@cisco.com

Investor Relations
Marty Palka
408-526 6635
mpalka@cisco.com

Source: Cisco