BREAKOUT VIEWPOINT:
Unlocking New Revenue with Security

There were a few underlying themes that pulled through all of our security breakout sessions, none more prevalent than the fact that global events continue to complicate the threat landscape. Cyber-attacks continue to make headlines yearly, and 2023 has been no exception.

Organizations require reliable protection, whether internal or external threats cause it. Yet so many need to pay more attention to the need for security solutions, or they inaccurately believe their outdated solutions will protect them. This adds up to a significant amount of vulnerability and a $136B 2027 TAM for physical and cybersecurity solutions, creating a fertile field for you to grow your security business.

The enthusiasm for this opportunity was evident in the standing-room-only crowds that showed up for this year's security breakout sessions at Channel Connect.

While all the sessions triggered a healthy conversation, three highlights stood out most to us.

RANSOMWARE

Ransomware remains the primary concern expressed by most businesses today. Consider that 95 percent of companies hit by ransomware or account takeovers had more than five security tools in place when the attack occurred. This tells us that IT security leaders need to know if their tools are actually working.

The question is not if a business will be the target of an attack but when. As the attackers become more sophisticated, businesses need to evaluate their security posture and assess the maturity of their security programs. Often, attacks will include not just encryption of data but also the exfiltration of the data. This results in a ransom demand for the decryption key and the threat of releasing critical company data to the public.

Attendees were encouraged to organize their market opportunity in five related yet distinct buckets:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Resist the urge to use fearmongering as your discussion starter. Instead, focus on how security solutions solve their biggest problems. Sixty percent of cybersecurity sales end without a decision being made. Focus on the information and the intended outcomes to keep your pursuits on track.

THE HUMAN ELEMENT

The human factor remains the weakest link in the cybersecurity defense effort.

Many of the security conversations at Channel Connect linked back to the MGM hack. This will likely be the costliest cyber-attack ever when all the accounting of lost revenue and legal action is done. Yet social engineering targeting the MGM helpdesk provided the bad actors with the path to shut down all IT functions across all MGM properties for nearly ten days.

The key insight is that not all security gaps are equal or look the same. Your customers need a comprehensive audit that includes operational, finance, compliance, and technical gaps.

When it comes to people, security is everyone's responsibility. From staff training to cybersecurity awareness, you are coaching your customers about this critical audience.

THE ARTIFICIAL INTELLIGENCE ERA IS HERE

AI conversations were everywhere at Channel Connect, and the security breakouts were no exception.

Security has been leveraging AI and machine learning for many years. These technologies power many managed detection and response ("MDR") and other cyber tools that support security operations in many businesses. These tools will continue to advance cybersecurity applications' capabilities, specifically in data correlation and shortened incident response times.

However, the bad actors also leverage AI to create more sophisticated attacks. AI functionality is being incorporated into malware. AI generates more authentic phishing schemes by harvesting information from the public Internet and the dark web, then using natural language models to create more authentic phishing messages in high volume. Next-generation email protection and end-point protection products can provide a layer of defense, and security awareness training can shore up the "human" defense element.

CONTINUED LEARNING

ScanSource Networking and Security Solutions