AppDirect

Security Sales Guide

CYBERATTACKS ARE GROWING RAPIDLY

When it comes to cyber threats, every company is a reachable target. With the increase in network complexity, AI, and cloud-based services, attackers have more opportunities than ever to attack.

BY 2026, SMB CYBERSECURITY SPEND IS PROJECTED TO INCREASE TO

$109B

$5M USD

The average cost of a data breach in 2024 – *10% increase from 2023.*

HELP CUSTOMERS ADOPT A HOLISTIC SECURITY STRATEGY

With access to a leading catalog of security solutions and a team of product experts, you can help your customers stay ahead of the evolving threat landscape.

CUSTOMER CHALLENGES

Common challenges faced by your customers and prospects and solutions to position against them.

CHALLENGE	SOLUTION
Inadequate security expertise	Companies need help staying up to date with the latest technology and guidance on how to manage new security solutions.
Insufficient toolstack	Companies need the right security stack to protect their business, employees, and customers, and to qualify for cybersecurity insurance.
Lack a holistic strategy	Companies need comprehensive security plans and frameworks to protect against, detect, respond to, and recover from security breaches.

Grow your business with security solutions

SECURITY SOLUTIONS OVERVIEW

Managed Security Services

Provides comprehensive support to address security concerns, offering guidance and expertise as needed.

SUB-CATEGORIES

Security Operations Center
Managed Detection & Response
Backup / Disaster Recovery
Network Operations Center
Penetration Testing
Virtual Chief Information Security Officer
Security Assessments

User Security

Maintains the security and protection of user accounts to safeguard user data and prevent unauthorized access.

SUB-CATEGORIES

Email Security
Phishing Detection
Identity & Access Management:
CIAM/MFA/SSO
End-User Training
Video & Audio Conferencing
Mobility

Network Security

Ensures that data is protected while in transit and prevents unauthorized access to the network.

SUB-CATEGORIES

SASE & SD-WAN
IPS/IDS
DDoS Attack Mitigation
OT Security
Zero Trust
On-Prem & Remote Firewall

Cloud Security

Implements measures such as encryption and access controls to safeguard data stored in the cloud.

SUB-CATEGORIES

Cloud Apps
Public/Private/Hybrid Cloud
Cloud Security Posture Management
Cloud Access Security Brokers

Endpoint Security

Protects devices accessing the platform against potential threats and unauthorized access.

SUB-CATEGORIES

Endpoint/Extended Detection & Response
Data Loss Prevention
Vulnerability Scanning

Physical Security

Prevents unauthorized access to physical assets.

SUB-CATEGORIES

Smart Cameras
Smart Locks
Secure Data Centers

Intelligent Incident Detection & Response

Utilizes intelligent systems to promptly detect and respond to security incidents, minimizing potential damage.

SUB-CATEGORIES

SIEM | UEBA | SOAR | AI

The top security threats your customers face

SECURITY THREATS OVERVIEW

78%

OF IT LEADERS SAY SECURITY IS THEIR TOP PRIORITY

Malware

Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.

Ransomware

A type of malware that encrypts a victim's data and demands payment for its release.

Insider threats

Security risks originating from within an organization, often involving employees who misuse their access.

Social engineering

Psychological manipulation used to trick individuals into divulging confidential information or performing actions that compromise security. This includes:

DDos attacks

Distributed Denial of Service attacks, where multiple systems overwhelm a target server or network, causing it to crash or become unavailable.

Pretexting

An attacker creates a fabricated scenario or pretext to deceive someone into revealing confidential information.

Mobile device vulnerabilities

Security weaknesses in mobile devices that can be exploited by attackers to gain unauthorized access or control.

Phishing

Deceptive messages to trick individuals into revealing sensitive information or downloading malicious software.

9 OUT OF 10

CYBERSECURITY BREACHES START WITH A PHISHING ATTACK

Help your customers qualify for cyber insurance

5 FUNDAMENTALS FOR CYBER INSURANCE READINESS

As cyber threats continue to spread, global regulators are enforcing stricter data protection and security measures. Although there isn't a universal standard for business protection, following five key security requirements can help you and your clients meet important cyber insurance demands. AppDirect provides access to these essential tools and expert support, giving your clients the basic protection they need.

01

Email security

Protects sensitive information from phishing attacks, data breaches, and other threats that can compromise corporate data and employee privacy.

02

Multi-factor authentication (MFA)

Reduces the risk of unauthorized access to sensitive accounts and data, even if a password is compromised.

03

Endpoint detection and response (EDR) and managed detection and response (MDR)

MDR solutions provide threat detection, incident response, and continuous monitoring across an organization's entire network, while EDR focuses on detecting and responding to threats specifically at the endpoint level.

04

Security awareness training

The majority of breaches stem from human error. Routine training can educate team members about the latest threats and reinforce the importance of remaining vigilant against potential malicious activities.

05

Segregated backups

Ensures that critical data is stored in separate locations and systems, reducing the risk of data loss from ransomware attacks, hardware failures, or other disasters, and facilitating quicker recovery.

Gain customer trust with AI

LOWERS COSTS & ACCELERATE DETECTION WITH AI

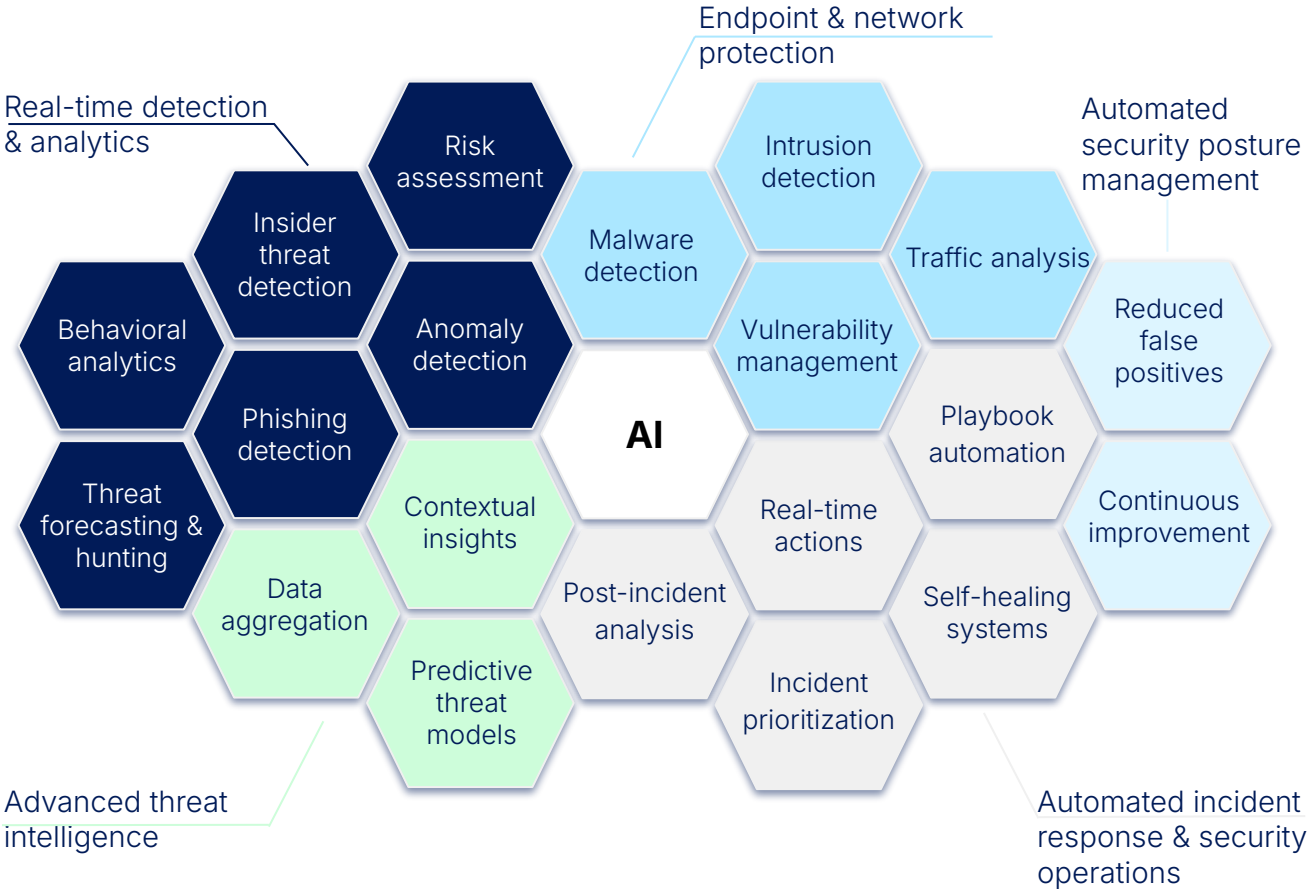
As cyber threats grow in complexity and frequency, integrating AI into your customers' security solutions is essential for staying ahead. Equip your customers with AI-assisted cybersecurity solutions so they can quickly detect and respond to threats, significantly reducing both the time and costs associated with breaches.

COMPANIES THAT APPLIED AI TO SECURITY PREVENTION SAVED AN AVERAGE OF

$2.2M

HOW ARE SECURITY PROVIDERS USING AI?

Traditional security measures are no longer sufficient in today's environment. Your customers want to know how AI can enhance their security measures and protect them from the growing threat of cyber attacks.



LEADING PROVIDERS LEVERAGING AI

CROWDSTRIKE SentinelOne zscaler paloalto NETWORKS okta TREND MICRO

> Companies using security AI & automation identified data breaches **100 days faster** than those that did not.

Ask the right questions

Use these conversation starters to uncover basic customer security needs, assess current security systems, and understand long-term objectives. Frame your questions using the tiered approach below to cater to different levels of expertise.

01 UNDERSTANDING SECURITY NEEDS

START THE CONVERSATION

- What are your concerns around data security, privacy, and/or compliance?
- How prepared are you today for a cyber attack?
- What were the results of your last cybersecurity assessment?
- What challenges or concerns do you face when conducting a comprehensive security audit?
- Do you have cyber insurance? Are you confident you meet policy requirements and that you would be covered if there was an incident?

UNCOVER THEIR NEEDS

- With data breaches consistently on the rise, do you feel comfortable that confidential data residing on your infrastructure is secure?
- Have you had any breaches or attacks recently?
- How do you report and handle security breaches or incidents?
- How would you describe your disaster recovery & business continuity strategy?

02 ASSESSING CURRENT SYSTEMS

START THE CONVERSATION

- When there's a security issue, is there a plan in place and who do you call?
- What do you use for security today?
- What should I know about your company's environment when it comes to security that we have not already discussed?

UNCOVER THEIR NEEDS

- How do you manage and prioritize patching within your infrastructure?
- What regulatory requirements or compliance standards is your organization subject to?
- How do you secure all your endpoints and remote workers?

03 UNDERSTANDING LONG-TERM OBJECTIVES

START THE CONVERSATION

- What is your long-term strategy and goals for cybersecurity?
- How do you measure the effectiveness of your current security programs?
- What initiatives are in place for enhancing the security awareness of your employees?

UNCOVER THEIR NEEDS

- What security frameworks do you follow and how do you track progress?
- How do you handle onboarding and offboarding employees and their data after they leave?

BONUS QUESTIONS

- Do you have fully documented policy and procedures for IT and Cybersecurity?
- Do you have a well tested after hours cybersecurity incident response?
- What dedicated staff do you have today for monitoring and responding to attacks?
- How are your employees currently assessing the corporate network along with critical business applications and data?

After you've assessed if your customer's Security needs, your Channel Manager can connect you with a Sales Engineer to help find a solution.

INDUSTRIES WITH THE HIGHEST NEED FOR SECURITY SOLUTIONS

- ✓ **Financial Services** are frequently targeted due to the value of financial data and have the highest average data breach cost at USD 5.6M.
- ✓ **Technology & Software** companies are heavily investing in security due to the rise in cloud adoption and the need to protect intellectual property.
- ✓ **Healthcare** is a prime target due to the sensitivity of health records.
- ✓ **Retail** is a major target for payment fraud and data breaches, with 24% of breaches involved in payment card data theft.
- ✓ **Energy & Utilities** are vulnerable to cyberattacks that could disrupt energy supplies and critical infrastructure.

Overcome objections

Here are some common objections and example responses that you can use to address your customer's concerns and hesitations.

"My industry is safe."
Cyberattacks will only continue getting more sophisticated with the rise of AI. Ransomware attacks are targeting more sectors than ever, and even industries that were once considered safe can become targets as cybercriminals adapt and find new opportunities.

"Cybercriminals don't attack small businesses."
Cybercriminals are more likely to go after small businesses since they are often less prepared. In fact, 94% of SMBs have experienced at least one cyberattack in the last year. 43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

"I don't have the budget."
We'll find the right security solution for your business and your budget. The average cost of a data breach is $5M; being the victim of a cyberattack is more costly than being prepared.

"I don't have the expertise to implement security solutions."
Let us provide the expertise you need. Our experts are trained on the most up-to-date and effective security technologies and will provide security solutions tailored to your specific needs.

"I have cybersecurity insurance."
Cyber attacks have more than just a financial impact on your business; a breach can also have legal and reputation impacts. Most cybersecurity insurance doesn't cover ransom payments. It's better to be prepared and defend against attacks than to rely on insurance.

"New security measures will disrupt my existing systems."
Our security solutions are designed with seamless integration in mind. We conduct compatibility assessments and provide detailed implementation plans to ensure a smooth transition with no disruption. Our team also offers ongoing support to address any issues quickly, allowing your operations to continue running smoothly.

Top solutions to offer

ALL THE LEADING SECURITY PROVIDERS

LUMEN, CYBERSAFE SOLUTIONS, okta, zscaler, mimecast, CROWDSTRIKE, SentinelOne, COMCAST BUSINESS MASERGY, proofpoint, FORTINET, eSENTIRE, paloalto NETWORKS, CORO, SOPHOS, CHECK POINT, HARBORSHIELD CYBERSECURITY CULTURE ENABLES SECURITY, CLOUDFLARE, Bitdefender, LevelBlue, RAPID7

IN THE EVENT OF A SECURITY INCIDENT

Companies need your help before, during, and after security incidents occur.

Discover incidents in real-time	Qualifying for insurance	Malware & virus removal
A SOC or NOC solution can provide real-time monitoring and isolate issues before they become outages or breaches.	85% of companies need to update their security posture to qualify for cyber insurance.	AppDirect's SmartSupport team resolves 96% of issues like malware removal on the first call.

Contact your Channel Manager for more information about our Security solutions—our team of experts will guide you on the best path forward

ABOUT APPDIRECT

AppDirect is a San Francisco-based B2B subscription commerce platform company that brings together technology providers, advisors, and businesses to simplify how they buy, sell and manage technology. More than 1,000 providers, 10,000 advisors and 5 million subscribers rely on the AppDirect ecosystem of subscription marketplaces to power their innovation, growth, and success. For more information about AppDirect, please visit www.appdirect.com.