AppDirect

The cybersecurity opportunity for technology advisors

Why now is the right time to add a security practice to your portfolio—And tools to get you started

Businesses today face an increasingly complex spectrum of security threats on a scale that was unimaginable just a few years ago. These threats are sophisticated, constantly evolving, and they target weaknesses within your company. Although most cyber crime originates externally, employees have unwittingly become a large part of the problem, as external perpetrators exploit employee trust using sneaky, increasingly credible methods to gain access to company data and systems.

From phishing, zero-day exploits, and ransomware attacks, to data breaches, supply chain vulnerabilities, and insider threats, grasping the intricacies of this complex landscape and knowing how to make the right risk prevention choices is daunting for most businesses.

As a technology advisor, your customers have always turned to you for sound advice in sourcing the best solutions for their technology stack. Today, ensuring they're protected from cyber crime should be an essential part of your offer.

IN THIS EBOOK

Read this ebook to gain practical insights into the security challenges your customers encounter so you can engage in more productive discussions with them. Learn how you can start integrating cybersecurity expertise and solutions into your advisory services.

Table of contents

01

Cyber crime—The cost, the opportunity

Cybersecurity is rapidly evolving, as a growing problem for businesses, and an opportunity for technology advisors.

THE HIGH COST OF CYBER CRIME

The number of cyber crime attacks is accelerating at a staggering pace, with increasing impacts.

Cybersecurity impacts

$10.5 TRILLION

Projected cyber crime costs for 2025. Up from $3 trillion in 2015.[1]

$5 MILLION

The average cost of a data breach[2]

74% OF COMPANIES

reported that in 2022, sensitive data was potentially compromised or breached[3]

23.5 BILLION

cybersecurity attacks were detected in 2022.[1]

43% OF CYBER ATTACKS

are directed at SMBs, but only 14% of small businesses are equipped to deal with these incidents[4]

95% OF CYBER BREACHES

are financially motivated[9]

The impacts of cyber crime can extend well beyond financial costs and losses.

Financial

losses resulting from the theft of corporate and financial data can also lead to breach of contract issues, affecting future revenues.

Reputational

impacts through compromised customer trust can lead to customer churn, lost revenue, and impacts on partner and supplier relations.

Legal

impacts resulting from non-compliance with data protection laws that safeguard personal data can lead to huge financial penalties.

THE OPPORTUNITY FOR TECH ADVISORS

With so much at stake, security is a growing priority for businesses, which has led to a strong market for cybersecurity solutions and expertise.

Cybersecurity spending is on the rise

79% OF IT BUSINESS LEADERS

rank security as their top overall priority[5]

$76 BILLION

spent by SMBs on cybersecurity in 2022. This is projected to increase to $109 billion by 2026, driven by greater awareness of cyber risks, mobile device use, and cloud adoption.[6]

$109 BILLION

the total projected cybersecurity spend for SMBs in 2026—represents a 30% increase over 2022[6]

74% OF IT BUSINESS LEADERS

plan to purchase cybersecurity solutions in the next 12 months—more than any other spending category[5]

Businesses face significant cybersecurity challenges

- **9 out 10** cybersecurity breaches start with a phishing attack[1]
- **50%** of IT leaders are anxious about their security posture[5]
- Only **53%** of companies that had to use their cybersecurity incident response plan said it was very effective[5]
- **95%** of organizations surveyed in the Fortinet 2023 Cloud Security Report study were concerned about their security posture in public cloud environments[7]
- **59%** of those cited misconfiguration as the biggest cloud security risk.[7]
- **32%** of IT leaders feel challenged because of the complexity of implementing and managing technologies[5]

Key advisor takeaway

Business customers need help grappling with the security attacks that continue to expand in range, severity, and frequency. Advisors can capitalize on this growing market to provide valuable support and services to customers while expanding the breadth of solutions they offer.

02

Four essential truths about cyber crime

With more than 30 years' experience investigating and combating cybercrime within the FBI Cyber Crime Fraud Unit, Scott Augenbaum knows cybersecurity—what motivates perpetrators, how they gain sensitive data and systems, and the havoc they wreak when they gain access. But most importantly, he knows that most cyber crime is preventable.

In his book, The Secret to Cybersecurity, Augenbaum outlined four truths that individuals and organizations need to know about cybercrime:

ONE

No one ever thinks a cybersecurity event will happen to them. Every victim is caught off guard.

TWO

Once a cyber criminal has your money or data, it's almost impossible to retrieve.

THREE

Since most cyber criminals are located outside the United States, the chances of law enforcement bringing them to justice is low.

FOUR

Most cyber crime incidents could have been prevented if the victims used simple best practices.

Key advisor takeaway

Most cyber attacks are preventable if the right processes are put in place.

> *Humans are a principal cause of cybersecurity failures — The number of cyber and social engineering attacks against people is spiking as threat actors increasingly see humans as the most vulnerable point of exploitation.*[8]

SOURCE:

Gartner Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, January 25, 2023

Cyber crime is largely a people problem

THE HUMAN ELEMENT

Today human error accounts for the largest percentage of cyber attacks. In the IT Business Leaders 2024 Outlook Report, based on an AppDirect-sponsored survey of IT business leaders conducted by Propellor Insights, 49% of the respondents cited employee and human errors among their top security concerns. In fact, all of their other concerns—malware, stolen data, phishing, ransomware, and misconfiguration of cloud services—include an element of human and employee error
and/or malice.

Similarly, the 2023 Comcast Business Cybersecurity Threat Report revealed that 9 in 10 breaches start with individuals clicking on what they believe is a harmless link.[1]

And Verizon found in its Verizon Data Breach Investigations Report 2023 that 74% of breaches and attacks on organizations involved a human through error, misuse of access privileges, use of stolen credentials, or social engineering attacks that exploit employee-related vulnerabilities.[9]

SECURITY BREACH STATISTICS

44.7%

Involve stolen credentials[9]

83%

Involve external actors

outside the organization and its partners)[9]

95%

Are financially motivated

Top actor by far is organized crime, followed by espionage[9]

50%

Of social attacks are pretexting incidents

That's almost double the 2022 number[9]

19%

Involve internal actors

Trusted and privileged people within the organization who acted by error or by intention[9]

24%

Involve ransomware

Consistent across all organization sizes[9]

04

The top cybersecurity threats your customers face

Malware

Hackers create a software code or program to gain unauthorized access to sensitive data, hijack computer systems and operate them remotely.

Ransomware

This form of malware encrypts a victim's data or infrastructure, then prevents access until they pay a ransom to have it unencrypted. According to IBM, ransomware accounted for 17% of all cyberattacks in 2022.[2]

Social engineering

This encompasses a range of malicious activities that trick people into revealing sensitive information. There are several types of social engineering but the two most common are phishing and pretexting.

- **Phishing**
  Posing as a reputable organization, cybercriminals send a deceptive email or SMS to their intended victims to trick them into disclosing sensitive information. The perpetrator exploits psychological vulnerabilities to create a sense of urgency. According to Comcast's 2022 Official Cyber crimes Report, 9 out of 10 attempts to breach ne tworks start with a phishing attack.[1]

- **Pretexting**
  Pretexting, from the word pretext, is generally initiated by a perpetrator pretending to be someone that the user already knows and trusts. For example, a senior leader in the company, a bank, or government department that the victim has an established relationship with.

Insider threats

Authorized users—employees, contractors, business partners— intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals. These threats can be more difficult to detect than external threats because they appear to be authorized, and are invisible to antivirus software, firewalls and other security solutions aimed at blocking external attacks. According to a recent IBM study, 44% of insider threats are caused by malicious actors, and the average cost per incident for malicious insider incidents in 2022 was USD $648,062.[2]

DDoS attacks

The attacker overwhelms a server with Internet traffic, causing it to crash and prevent users from accessing their online services, websites, and data. Threats come from apps that install spyware and malware, and apps that steal data over unencrypted WiFi networks.

Mobile device vulnerabilities

Mobile devices are increasingly at the center of security threats, as more people rely on them, and as more business applications become available on mobile devices.

Key advisor takeaway

There's a huge opportunity for you to become your customers' trusted security advisor. For 78% of IT leaders, security is their top priority, and over the next 12-24 months, 74% of IT leaders expect to invest in cybersecurity solutions.[5]

As an advisor, you can play an important role in identifying your customers' security gaps, while building up your security practice to generate new sources of revenue.

THE REMOTE WORK FACTOR

Other common risk factors involve employees who work remotely. As users move from a secure corporate office network to their home, they can expose security shortcomings and flaws if stringent security measures aren't in place and followed.

Notable factors impacting business security include:

Household Internet

Employees in offices are protected by the company network's firewall, but employees working from home often rely on weak or non-existent ISP network protection. As a result, employee devices can become infected, moving laterally and potentially infecting corporate devices on the network.

Recommendation—This risk can be mitigated by requiring VPN access back to the corporate network for internet traffic.

Personal devices

Employees working remotely who use personal devices such as PCs, tablets, and phones can quickly become an attack target and security risk without the proper software.

Without the security software issued on corporate devices such as endpoint protection, VPN, DNS filtering, and more, all sensitive company data passing through that device is at risk.

In a Fortinet, 2023 study, 43% of respondents said the public cloud risk is somewhat to significantly higher than on-premises.[7]

Recommendation—Mobile Device Management (MDM) allows IT to remotely control, update or wipe devices. MDM solutions can be used on company issued devices (helping with management and billing) or for BYOD policies.

Inadequate awareness and training

When it comes to remote work, IT needs to be involved quickly to quarantine a compromised device.

Recommendation—Stringent training and awareness are critical in such cases. Employees need to know what to do if they suspect a device has been infected or when a device is lost or stolen. Additionally, companies should adopt zero trust policies, enabling added verification layers for anyone trying to access resources on the company network.

Email security

Employees can easily fall prey to phishing scams or impersonating emails.

Recommendation—Integrate email security solutions with SaaS mail services such as Office 365 or G-Suite to prevent email attacks.

IoT devices

Today's homes are filled with smart devices—light bulbs, fridges, TVs—all connected to the internet. IoT devices are a long way from catching up with necessary security and introducing a corporate device onto a network shared with IoT devices can be an open door for malicious activity.

Recommendation—Network segmentation through two connections—for example, VLANs and VRFs—can ensure that company-related traffic stays separate from personal home traffic.

Key advisor takeaway

People, more than technology, are your customer's biggest vulnerability. Companies need to ensure their cybersecurity strategy includes rigorous employee training and processes that will allow them to become part of the solution, rather than unwittingly being part of the problem.

In your conversations with customers, a key step will be to identify internal and external people-related vulnerabilities. AppDirect provides a framework and tools for doing this.

05

Beyond the checklist—The limitations of compliance

Scott Augenbaum, a 30-year veteran of the FBI Cyber Crime Fraud Unit, and author and speaker on cybersecurity, says that after organizations have complied with cybersecurity regulations and obtained their insurance, they can become complacent. He cautions that relying on compliance isn't an effective prevention strategy because compliance requirements don't keep pace with the ever-evolving sophisticated threats.

This realization leaves many business leaders with a sense of doubt and insecurity.

THE CONFIDENCE-ANXIETY DICHOTOMY

Security anxiety isn't uncommon, even among IT leaders who believe they've diligently addressed compliance and security measures. The 2023 Gartner cybersecurity report indicates that cybersecurity leaders find themselves in a constant defensive stance, knowing that despite their security measures, they may fall victim to cyber threats. This unrelenting pressure often leads to psychological stress and burnout among security professionals.[8]

The IT Business Leaders 2024 Outlook Report, an independent study conducted by Propellor Insights and sponsored by AppDirect, sheds light on why this anxiety persists. The study's findings provide revealing insights into how IT leaders feel about their security posture. Surprisingly, despite believing they've ticked the right boxes in terms of compliance, cybersecurity insurance, and security measures, half of the IT leaders admit that they lose
sleep over their company's security, and 45% of them experienced a security breach in the previous year.[5]

The following statistics reveal what's behind this unease.

BOXES CHECKED[5]

92% OF IT LEADERS

feel they've made sound security investments.

88% OF IT LEADERS

claim to meet all compliance requirements.

77% OF IT LEADERS

have cyber insurance in place.

TOP AREAS OF CONCERN[5]

- Cybersecurity risk (58%)
- Information security risk (53.1%)
- Operational risk (46.5%)
- ESG risks (environmental, social, governance) (41.2%)
- Compliance risk (38.8%)
- Financial risk (38%)
- Strategic risk (34.7%)
- Reputational risk (30.2%)

Key advisor takeaway

Although cybersecurity compliance and insurance and the existing security measures they have in place can give IT leaders a level of confidence about their security posture, many still worry that it's not enough.

As an advisor, you have access to training and tools to help you identify your customers' key vulnerabilities and recommend an action plan to build their level of confidence.

> *Compliance is not the same thing as being secure."*

SCOTT AUGENBAUM,
AUTHOR, THE SECRET TO CYBERSECURITY[10]

4 SMB cybersecurity perceptions and myths you need to dispel

When you start talking about security to your SMB customers, you may run into reasons why they don't treat cybersecurity as a serious threat.

Part of the problem stems from the fact that many SMBs aren't well equipped with the knowledge, processes, skills, and people they need to fully secure their organization, and they may not fully understand the level of risk they currently face.[6]

01—MY INDUSTRY IS SAFE

In reality, no industry is safe from cybersecurity threats. In 2021 82% of ransomware attacks targeted companies with fewer than 1,000 employees, and 37% had fewer than 100 employees.

In truth, most government and private-sector organizations are vulnerable. For example, ransomware attacks are targeting more sectors than ever, including local governments, nonprofits and healthcare providers, government websites, and critical infrastructure.[2]

02—CYBERCRIMINALS DON'T ATTACK SMALL BUSINESSES

Nothing could be further from the truth. In fact, 43% of cyber attacks are directed at SMBs. And although SMBs are a top target for cyber attacks, many use only consumer-grade cybersecurity tools to protect their company. 20% don't even have any endpoint security. 43 Small Business Cybersecurity Statistics, Published: May 29, 2023 by Kevin Ocasio[4]

03—I DON'T HAVE THE BUDGET

As the old saying goes, an ounce of prevention is worth a pound of cure. With high costs and impacts of cyber attacks, every company needs to allocate an appropriate percentage of their budget to security, or they face the potential of much higher costs at a later date.

04—I HAVE CYBERSECURITY INSURANCE

Cybersecurity insurance doesn't prevent malicious perpetrators from attacking a business. Furthermore, cyber attacks have more than just a financial impact on a business. A breach can also have serious legal and reputational impacts. Additionally, most cybersecurity insurance doesn't cover ransomware. It's better to be prepared and defend against attacks than to rely on insurance.

Key advisor takeaway

When it comes to cyber threats, every company is a reachable target and has operations, brand, reputation, and revenue pipelines that are potentially at risk from a breach. The cybersecurity landscape is shifting and with the increase in network complexity, remote work, and cloud-based services, attackers have more opportunities than ever to attack. Every new device or application a business adds to the mix injects vulnerabilities into their environment.

As an advisor, you can play a pivotal role in creating a sense of urgency about the risks and impacts of security, and how they can mitigate those risks.

07

7 security best practices every organization should follow

As you work with your customers to take a proactive approach to mitigating future threats, here is a list of 7 security basics every organization should have in place.

01—THIRD-PARTY ANNUAL AUDIT OF YOUR ENVIRONMENT

An objective third party can discover gaps, identify vulnerabilities, and recommend required updates.

02—SECURITY AWARENESS TRAINING AND TESTING

Education is the first line of defense and ongoing training should be mandatory. Put in place a best-in-class security awareness and training program, and ensure employees understand what they've learned through testing.

03—FIREWALL SECURITY

Missing firewall patch updates causes 60% of breaches, so it's important to ensure that patches are up to date at all times. Managed firewall solutions make that easy to manage with ongoing monitoring, updates, 24/7 maintenance, and reporting. Next gen firewalls feature an intrusion detection system that blocks malware from entering the network, along with content filtering, application awareness, and more.

04—EMAIL SECURITY AND ENCRYPTION

Take preventive measures to ensure perpetrators can't intercept and access emails.

05—ENSURE EQUIPMENT IS STILL UNDER MANUFACTURER SUPPORT

Any technology that has reached its end of life and can no longer be updated and becomes a significant vulnerability.

06—PROTECTED ACCESS, USING MULTI-FACTOR AUTHENTICATION AND VPNS

Username and password are no longer enough. Multi-factor authentication requires at least three or more layers of authentication to enable access to sensitive company data. Additionally, for any remote access, Virtual Private Networks (VPNs) enable safe remote access to the corporate network.

07—END-POINT DETECTION AND RESPONSE

Every device used to access company and customer networks and systems, including personal mobile devices, tablets, and computers, provide a point of entry for attacks. Endpoint security, managed from a network server or gateway and installed on each device, blocks threats, prevents malicious apps from being downloaded and can remotely wipe devices should it be lost or compromised. It's vital to make endpoint detection and response a critical part of your customers' security approach.

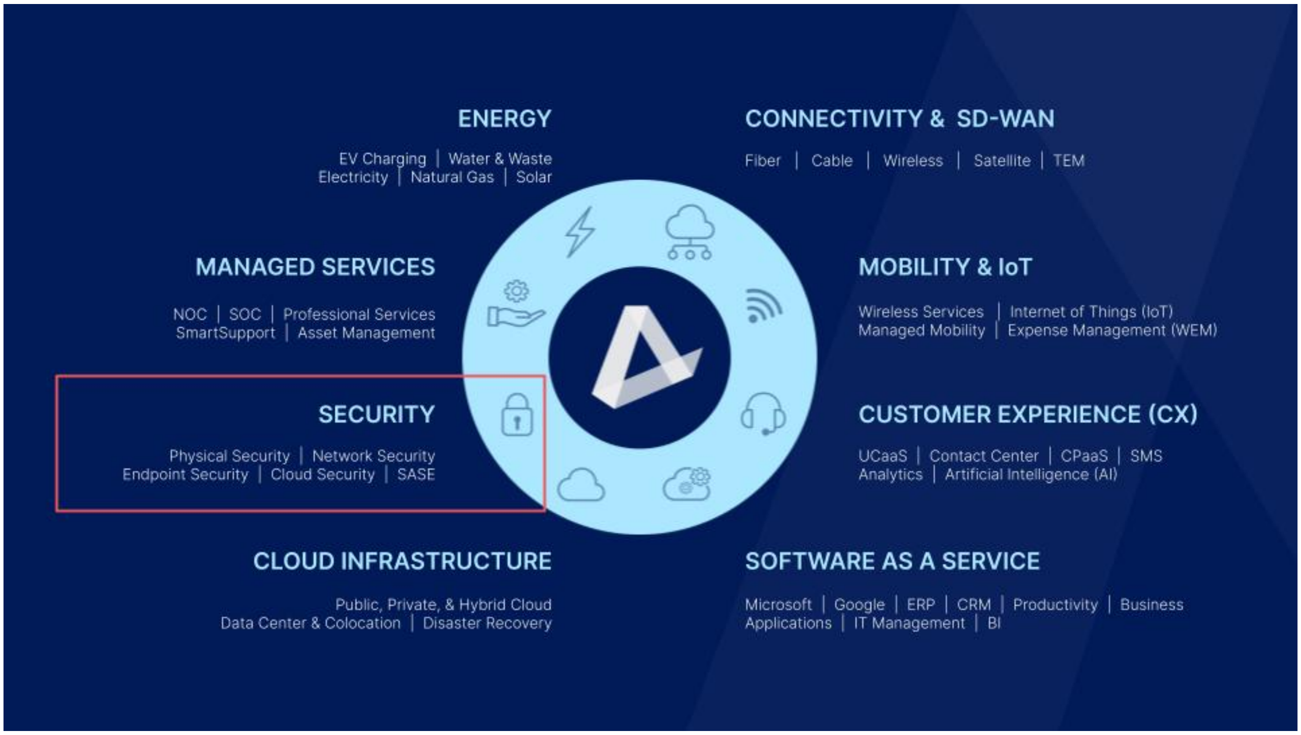
Key advisor takeaway

The security solutions your customers need cover a broad spectrum, but adding this much-needed area of expertise to your portfolio is easier than you might think. AppDirect has solutions to address each of the 7 areas described above. If you're an advisor who already works with AppDirect, talk to your AppDirect Channel Manager to learn more. If you aren't, you can sign up to get started today.

08

How to start building your security practice

Increase your value to your customers with a one-stop-shop experience for all their technology solutions, including security. By selling complementary security solutions, you’ll earn commissions, increase your wallet share, and gain new recurring revenue streams.



ENERGY

EV Charging | Water & Waste
Electricity | Natural Gas | Solar

CONNECTIVITY & SD-WAN

Fiber | Cable | Wireless | Satellite | TEM

MANAGED SERVICES

NOC | SOC | Professional Services
SmartSupport | Asset Management

MOBILITY & IoT

Wireless Services | Internet of Things (IoT)
Managed Mobility | Expense Management (WEM)

SECURITY

Physical Security | Network Security
Endpoint Security | Cloud Security | SASE

CUSTOMER EXPERIENCE (CX)

UCaaS | Contact Center | CPaaS | SMS
Analytics | Artificial Intelligence (AI)

CLOUD INFRASTRUCTURE

Public, Private, & Hybrid Cloud
Data Center & Colocation | Disaster Recovery

SOFTWARE AS A SERVICE

Microsoft | Google | ERP | CRM | Productivity | Business
Applications | IT Management | BI

GROW YOUR BUSINESS WITH ALL THE SECURITY SOLUTIONS YOUR CUSTOMERS NEED

Simplify the experience of finding and buying security solutions for your customers with security experts to guide you. All of the solutions you need to help your customers are available in the AppDirect catalog.

Preventive tools and services

- Customer identity and access management (CIAM)
- Workforce management
- Physical security
- Cloud security
- Endpoint protection
- Network security
- Phishing detection
- SASE
- SD-WAN
- Firewall
- Web application firewall
- Security Information and Events Monitoring (SIEM)
- Managed firewall
- Infrastructure configuration and setup
- Penetration testing
- Threat evaluation

Incident recovery

- Virus and malware removal
- DDoS mitigation
- Ransomware response
- Backup / disaster recovery

EXTEND YOUR TEAM WITH SUPPORT FROM APPDIRECT SECURITY SPECIALISTS

Help your customers adopt a holistic security strategy. At any time, you can get support from AppDirect experts who can help you evaluate your customers' security needs and the related available solutions. We can help you achieve your (and your customers') security objectives without any upskilling or new hiring.

Get help with:

- End-user security training and compliance
- Managed security and network management (NOC)
- Penetration testing and vulnerability scans
- System configuration
- Security audits

Solution engineers bring extensive technical expertise to the customer discovery and qualification process.

Solution architects help you confidently present solutions that are fully scoped, designed for your customer, and vetted by top cybersecurity experts.

Training and resources to help you sell security solutions

ENROLL IN THE APPDIRECT SECURITY CERTIFICATE PROGRAM

Learn cybersecurity essentials and bring newfound knowledge to your customer discussions by completing the AppDirect Security Certificate program, available in the Advisor Training Center.

Rooted in the esteemed National Institute of Standards in Technology (NIST) framework and designed specifically for advisors, the program will equip you with an unbiased understanding of security solutions, based on technology rather than touting specific vendors.

You'll gain a solid understanding of the crucial stages of cybersecurity and the knowledge you need to help your customers stay ahead of threats.

You'll master the art of articulating security solutions and generating quotes for security solutions by confidently navigating the NIST process.

The curriculum covers the five elements of the NIST framework:

1. **Identify—**Tools to develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
2. **Protect—**Solutions to provide appropriate safeguards to to ensure delivery of critical services
3. **Detect—**Technologies to identify the occurrence of a cybersecurity event
4. **Respond—**Implementation of activities to detect and respond to cybersecurity events
5. **Recover—**Restoral of capabilities and service that were impaired due to a cybersecurity event

You'll also work through sales scenarios targeted to cybersecurity prospecting, which will be manually reviewed by the channel advisor training team.

How to access to the AppDirect security certificate program

If you're an AppDirect advisor, Log in to your Marketplace account to sign up. If you're not an advisor, sign up now to get started.

ADDITIONAL TRAINING AND RESOURCES

Level up your security skills and learn to position and sell security with comprehensive AppDirect training tools and events.

- **Live workshops—**Instructor-led sessions with practical sales activities and scenarios. Learn alongside like-minded advisors and technology providers.
- **Training Center—**Learn at your own pace with short videos, expert interviews, reference materials, and impactful training
- **Resource kit—**Access co-brandable datasheets, guides, pitch decks, email templates, and more to help you sell

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND

10 Key takeaways—Seizing the cybersecurity opportunity

Today's cybersecurity landscape is filled with evolving threats and challenges. Businesses of all sizes are engaged in an ongoing battle against these pervasive risks, with higher than ever stakes and impacts.

For technology advisors, this presents a ripe opportunity to help customers prevent attacks and mitigate their impacts when they do happen. You can help your customers move well beyond meeting compliance standards to adopting robust cybersecurity practices.

Adding cybersecurity to your portfolio makes business sense. With a growing market for these services, you can deepen your relationships with your clients, grow your business, and bolster your position as their essential partner.

AppDirect makes it easy to get started on this journey. Through workshops, training, resources, access to experts, and a cybersecurity certification program, you can gain the knowledge you need to guide your clients through this complex world.

You can also grow your business and earn more commissions by sourcing security solutions for your customers from the vast AppDirect catalog on a robust marketplace platform, supported by best-in-class back office tools and expertise.

If you're an AppDirect advisor, download your Security toolkit with handy resources like a sales guide, shareable data sheet, security comparison guide, and a pitch deck. Or connect with your Channel Manager to dive into security opportunities.

Not an AppDirect Advisor? Sign up today!

Related resources:

How to Build a Robust Cyber Security Strategy—AppDirect blog article, December 20, 2022
Jay Kaplan, CEO and Co-Founder of Synack, on How Businesses Can Stay Protected—Video, December 2022

Sources:

[1] 2023 Comcast Business Cybersecurity Threat Report
[2] What is Cybersecurity? IBM, 2023
[3] Top Security Threats in 2023, Forrester, April 2023
[4] 43 Small Business Cybersecurity Statistics, Small Business Trends
[5] IT Business Leaders 2024 Outlook Report, by Propellor Insights survey, sponsored by AppDirect, October 2023
[6] SMBs' spending on cyber security will increase at a 10% CAGR to reach USD109 billion worldwide in 2026, Analysys Mason, June 1, 2023, by Youngeun Shin
[7] 2023 Cloud Security Report, Fortinet
[8] Gartner Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, January 25, 2023, by Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, Charlie Winckless
[9] Verizon Data Breach Investigations Report 2023
[10] The Secret to Cybersecurity, by Scott Augenbaum, 2019

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.

Created November 2023