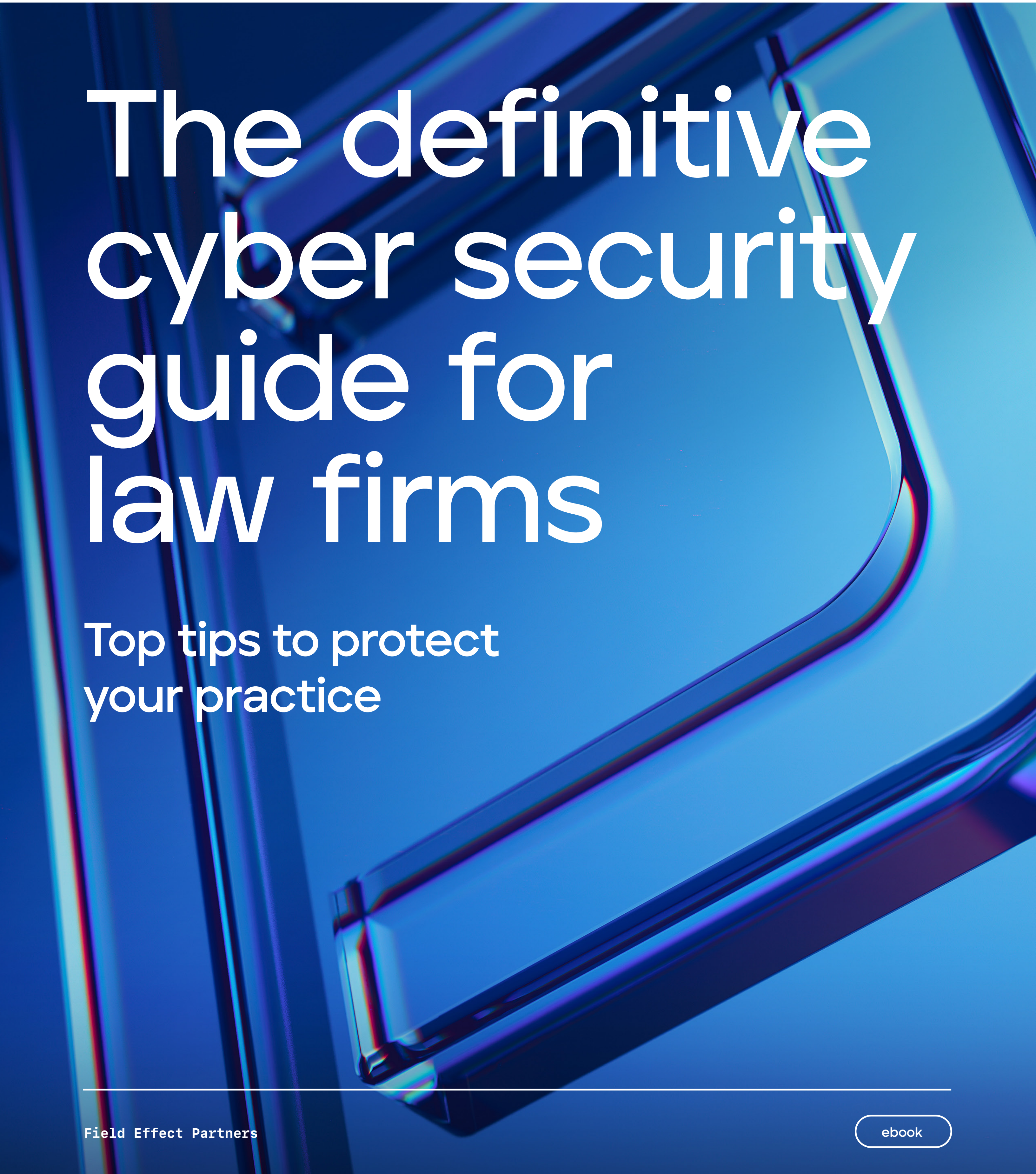
FIELD EFFECT / Partners



The definitive cyber security guide for law firms

Top tips to protect your practice

Field Effect Partners

ebook

What We Believe

Trust is everything in the legal industry. A single cyber attack can expose privileged data, destroy client relationships, and permanently damage a firm's reputation. You know that strong cyber security is a necessity, but it's tough to know where to start.

This ebook has all the information needed to protect your practice. Learn about the cyber threats targeting the legal industry and actionable tips to create a more resilient defence.

Remember, we've got your back.

If you have any questions, or if you need help with your cyber security goals, please reach out.

Table of Contents

A survey conducted by the American Bar Association found that 25% of firms have experienced a data breach at some point. Overall, the number of attorneys reporting a breach has increased over the years.[1]

Your legal practice is a treasure trove of valuable, sensitive data, putting a giant target on your back. By their very nature, law firms create, share, and store massive amounts of privileged information, such as:

- Intellectual property (IP) — trade secrets, copyrights, trademarks, and patents
- Financial statements — company or personal income, assets, and debts
- Business contracts — client and partner agreements, mergers and acquisitions, and bills of sale
- Personally identifiable information (PII) — full names, social security numbers, birth dates, addresses, and phone numbers
- Electronic health records (EHR) — diagnoses, medications, imaging reports, and lab data
- Private correspondences — confidential emails, text messages, and letters

Attackers seek out this data because of its value. Confidential information can be worth a pretty penny on the dark web* or offer deeper access for more damaging attacks.

The good news: no matter your practice's size, location, or specialty, solid cyber security is within reach. The first step? Understanding the cyber threats targeting your firm.

*What is the dark web? The dark web is not accessible via traditional search engines such as Google or Bing. Unlike the visible web (the one you probably use daily), the dark web is intentionally hidden, requiring a special browser to access. Cyber criminals often use these secret websites to illegally buy and sell malware, stolen credentials, and more.

The top cyber security threats to the legal industry

The key to a strong defence? Understanding the offence.

It's critical that you understand and recognize the major cyber threats to your firm — only then can you take the right steps to defend against them.

Credential theft

Last year, 61% of data breaches involved the use of stolen credentials.[2] Credential theft often starts with a malicious email designed to trick partners, lawyers, or staff into sharing login information. If successful, the cyber criminal may end the attack and simply sell the credentials. Alternatively, they may use the account to to conceal their identity to access sensitive files and data, edit or delete contracts, reset passwords, or inflict other damage. Since the attacker uses a legitimate account to do this, it can be hard to detect trouble until it's too late. If employees, clients, or third parties reuse credentials for different portals, the attacker could access additional accounts and cause more damage.

Financial redirection

Financial redirection occurs when an attacker intercepts payment between you and a client or vendor. After gaining access to an email account — often through credential theft — attackers may initially study the activity to learn your billing process, relationships, and payment schedules. Just before you'd usually issue invoices, they'll message clients or vendors from your email address, asking them to send payment to a new banking account. Because the request appears to be from you, a trusted professional, it wouldn't look suspicious. The attacker then empties and closes the bank account, erases evidence of their presence, and walks away with the money.

Ransomware

Ransomware is a form of malware that encrypts important files and information until the victim pays the ransom request. Attackers may begin a ransomware attack via phishing emails or by exploiting a security vulnerability, such as an outdated operating system. In the past, victims would receive a note explaining they'd get their data back upon paying a ransom. But today's attackers are taking a new approach. Rather than encrypt files, they'll make copies and threaten to publish them.

Nation-state attacks

The legal industry's access to national and corporate secrets makes it a unique target for nation-state attacks launched by foreign governments or state-sponsored attacks carried out by cyber criminal groups. Your practice may be particularly vulnerable if you have information that helps the attackers' mandate or may otherwise be valuable for corporate espionage. Unlike amateur hackers, these groups can be extremely skilled and persistent.

Why your firm should prioritize cyber security

Cyber attacks can be financially debilitating

Losing access to case files results in fewer billable hours, immediately affecting your legal firm's bottom line. But operational downtime isn't the only financial consequence.

Between investigating the threat, repairing or replacing infected systems, and improving your defences for the future, expenses add up — and even quicker if you need external help. In total, the cost of a data breach rose 10% over five years to an average of $3.86 million.[3]

Attacks are becoming increasingly sophisticated and frequent

Cyber criminals are attacking with more aggression, sophistication, and tenacity than ever before, and there are three main reasons why:

01 Automation. Attackers do far less manual work these days. They now often turn to automated tools to execute attacks or outsource the task to someone else entirely.

02 Scale. Large businesses aren't the only entities at risk. Hacking requires far less effort, skill, and time than ever before, allowing cyber criminals to launch larger attacks affecting more victims.

03 Motive. Cyber crime can be a lucrative business. Hackers can make quick money by selling data or extorting victims for ransom.

One breach can devastate your firm's name and reputation

Even one cyber security incident can damage critical client relationships, devaluing years of hard work — especially if the attack compromises sensitive data.

After an attack, your clients may look elsewhere for legal representation. Worse, they may file a malpractice lawsuit if you didn't make a reasonable effort to secure their privileged information.

The negative publicity stemming from an attack could make it challenging to bring on new clients or turn a profit if you plan to eventually sell the practice.

Clients are starting to ask about cyber security

The EY Global Consumer Privacy Survey found that the biggest concern for consumers sharing their data is secure collection and storage.[4]

Clients may soon inquire about your cyber security posture — have you experienced a data breach before? Is your firm covered by an insurance policy? Do you have an incident response plan? Are you compliant with data privacy regulations?

How you answer these questions could mean the difference between landing a major client and losing out on the opportunity.

You may have legal or ethical cyber security requirements

Cyber security regulations are heating up across many industries and countries. Depending on where your office and clients are located, you may be governed by one or more data privacy laws, such as:

- The General Data Protection Regulation (GDPR)[5]
- The Personal Information Protection and Electronic Documents Act (PIPEDA)[6]
- The California Consumer Privacy Act (CCPA)[7]
- The New York Stop Hacks and Improve Electronic Data Security Act (SHIELD)[8]

Your firm may also be ethically bound to take cyber security seriously. Some bar associations require that attorneys make reasonable efforts to protect sensitive client data from unauthorized access. Failure to comply could be a conduct violation, providing grounds for victims to file malpractice lawsuits.

Actionable ways to improve your defence

Build cyber situational awareness

Your first step toward stronger cyber security starts with building cyber situational awareness (CSA).

This includes knowing:

- Your IT infrastructure (computers, phones, software, smart technology, cloud-based apps, USBs)
- The threats and risks to your network (misconfigured or outdated "legacy" hardware, phishing attacks, ransomware)
- How to respond to those threats (an incident response plan, a disaster recovery plan)

Strengthen passwords

Consider all the services and systems your firm relies on, such as email, DropBox, DocuSign, Clio, and custom-built systems. Passwords are the first (and sometimes only) line of defence that prevents attackers from accessing accounts and compromising sensitive information.

Far too many users still rely on weak passwords, such as:

- password
- 123456
- qwerty
- 111111

While easy to remember, they're also easy to guess. Passwords should be long and complex with a combination of upper and lowercase letters, numbers, and symbols. If that sounds inconvenient, we also recommend using passphrases — strings of words that make sense to the user and no one else.

Another tip:

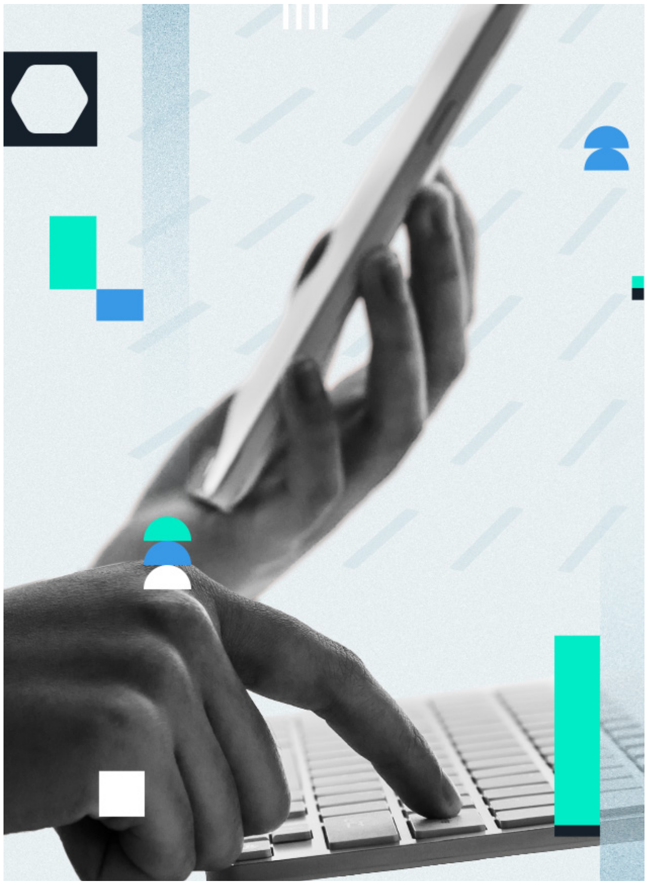
Never reuse passwords. If you do, a single set of breached credentials could put other accounts using that same login information at risk. And don't worry about having to memorize them all — password manager tools make it easy to generate, manage, and store hundreds or thousands of credentials.

Use multi-factor authentication

Multi-factor authentication (MFA) adds another defensive layer by requiring two or more authentication factors to confirm user identity. These may include:

- Unique passwords, passphrases, or personal identification numbers
- Hard tokens (USB keys) or soft tokens (text messages or an authenticator app)
- A unique biometric characteristic (a fingerprint or face ID)

With MFA enabled, even if an attacker has your password, they don't have the keys to the kingdom. They'll still need other credentials to access the account.



Back up your critical data

Russia-linked ransomware gang REvil successfully hacked Grubman Shires Meiselas & Sacks and stole 756 gigabytes of confidential data, ransoming it for $42 million before putting it up for auction on the black market.[9]

Routinely backing up data ensures you can rapidly recover files and resume operations after a cyber attack. Take the time to back up your data by copying it to an external hard drive or another secure location separate from your network, or by using a cloud-based or automated backup service.

Patch and update your software regularly

Attackers are always looking for ways to circumvent your defences — sometimes by exploiting outdated or unpatched software and operating systems.

Updates are sets of changes applied to a piece of software or an operating system, often to improve performance or fix a bug. Patches, however, are specific updates that address security vulnerabilities found by the developer.

ALL PATCHES ARE SOFTWARE UPDATES, BUT NOT ALL SOFTWARE UPDATES ARE PATCHES.

Applying patches as soon as they become available is a critical way to reduce security gaps but it's still a challenge for many. The UK's Cyber Security Breaches Survey 2021 found that only 43% of businesses have patching procedures in place.[10]

Use a virtual private network

Accessing your firm's data over a shared internet connection can introduce added risk. Public hotspots, while convenient, typically have minimal security measures which means they're easy targets.

If you must use public Wi-Fi, a virtual private network (VPN) can secure your connection by masking your internet protocol (IP) address. This protects you from cyber crime tactics that target weak infrastructure, such as man-in-the-middle attacks or DNS poisoning.

MAN-IN-THE-MIDDLE ATTACK: THE ATTACKER, POSITIONED BETWEEN TWO USERS OR ENTITIES, INTERCEPTS OR ALTERS COMMUNICATIONS DATA.

DNS POISONING: THE ATTACKER EXPLOITS DOMAIN NAME SYSTEM (DNS) VULNERABILITIES TO REROUTE TRAFFIC FROM A LEGITIMATE SERVER TO A MALICIOUS ONE.

When to use a VPN:

- When you're using public Wi-Fi
- When you're travelling
- When you need to access your firm's network remotely
- When you want continual privacy on the internet

When choosing a VPN, look for one based in a privacy-friendly country — that is, a country with solid data protection laws to secure your personal data[11]. Also look for a VPN with nearby servers to ensure fast, reliable internet access.

Remember that VPNs offer improved security but, unlike certain firewalls, can't stop users from clicking on malicious websites or links...which brings us to the next tip.

Invest in security awareness training

Many of the biggest cyber threats to law firms rely on social engineering techniques to fool users into opening malicious links or sharing their credentials. If successful, attackers can then:

- Steal IP and demand ransom to get it back
- Redirect client payments to an account they control
- Sell your confidential information on the dark web

The tactics used in these attacks take advantage of busy, distracted teams. Reduce their success with ongoing security awareness training. Educate employees on the red flags of a social engineering attack (such as typos, urgent language, odd file names, and requests for sensitive information), and what to do if they're targeted.

Training should also cover:

- Data privacy regulations and how they impact operations
- Maintaining the physical security of IT assets
- Best practices for sharing data digitally
- How to respond to a cyber security incident

Delivering ongoing education can foster a culture of security. Defending against attackers is a shared responsibility — getting everyone involved improves your firm's overall security posture.

Take a proactive approach to cyber security

A growing number of legal firms are using cyber security insurance to mitigate risk. Insurance is a necessary addition to any defence program, but typically as a last resort alongside other security measures.

Unfortunately, insurance offers little protection from an actual cyber attack. Despite premiums soaring in recent years,[12] a policy won't stop attackers from targeting your practice, nor does it guarantee reimbursement after an incident.

The better approach is a holistic one. Look for cyber security solutions that offer visibility across your entire IT infrastructure — the network, cloud-based services and apps, devices, and users — to detect and eliminate threats early. Work with vendors who can provide security guidance that improves your defence.

Cyber attacks are an unfortunate reality, but end-to-end visibility and the right response can minimize risk to your firm.

IN MARCH 2021, THE NEW YORK DEPARTMENT OF FINANCIAL SERVICES RECOMMENDED THAT CYBER INSURERS STOP PAYING RANSOM AS DOING SO COULD ENCOURAGE SIMILAR ATTACKS IN THE FUTURE.[13] TWO MONTHS LATER, ONE OF EUROPE'S TOP CYBER SECURITY INSURANCE PROVIDERS STOPPED REIMBURSING CLIENTS FOR RANSOM PAYMENTS.[14]

Conclusion

Your clients rely on you to keep their confidential data safe. But implementing the proper cyber security measures can be challenging, especially if you don't have the right information, tools, or guidance.

We hope this ebook provided you with a clearer understanding of the cyber attacks targeting your firm and actionable, straightforward steps you can take to build a stronger defence.

And remember, you're not alone.

It's our mission to help protect your legal firm, client data, and privileged information from cyber threats. If you have questions, or need help with cyber security, get in touch with our team.

We've got your back.

Sources

1. https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/
2. https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
3. https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html
4. https://www.ey.com/en_ca/cybersecurity/has-lockdown-made-consumers-more-open-to-privacy-
5. https://gdpr.eu/
6. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
7. https://oag.ca.gov/privacy/ccpa
8. https://www.nysenate.gov/legislation/bills/2019/s5575
9. https://www.businessinsider.com/trump-data-ransomware-grubman-law-firm-madonna-2020-5
10. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/
11. https://vpnalert.com/best-virtual-private-network/country/
12. https://www.fitchratings.com/research/insurance/sharply-rising-cyber-insurance-claims-signal-further-risk-challenges-15-04-2021
13. https://www.jdsupra.com/legalnews/nydfs-cyber-insurers-should-not-pay-3295217/
14. https://www.insurancejournal.com/news/international/2021/05/09/613255.htm

Covalence threat monitoring, detection, and response platform

Covalence, Field Effect's threat monitoring, detection, and response platform, provides small and mid-size businesses continuous visibility into their IT networks to identify potential threats, vulnerabilities, and malicious activities. By providing easy-to-understand, actionable insights, Covalence helps customers prioritize and resolve cyber security issues and improve their security. The end result is a powerful cyber threat detection system, delivering big business insights without the matching price tag.

Covalence

The Covalence product line includes Covalence Remote Work, Covalence Cloud, and Covalence Complete.

Field Effect Covalence

It's time to get the single source of protection you need to identify and stop cyber attacks across your entire IT infrastructure and secure your business.

Through powerful monitoring and advanced analytics, Covalence makes it easy to understand, prioritize, and act on cyber threats and risks in real-time. Providing analyst-verified threat data as simple, prioritized, actionable reporting, Covalence helps you understand your threats as Actions, Recommendations, and Observations (AROs). This proprietary approach removes noise to show you the alerts that matter with the context needed to resolve them.

Contact our team today.

Email:

letschat@fieldeffect.com

Phone:

Canada + United States
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418

FIELD EFFECT

fieldeffect.com