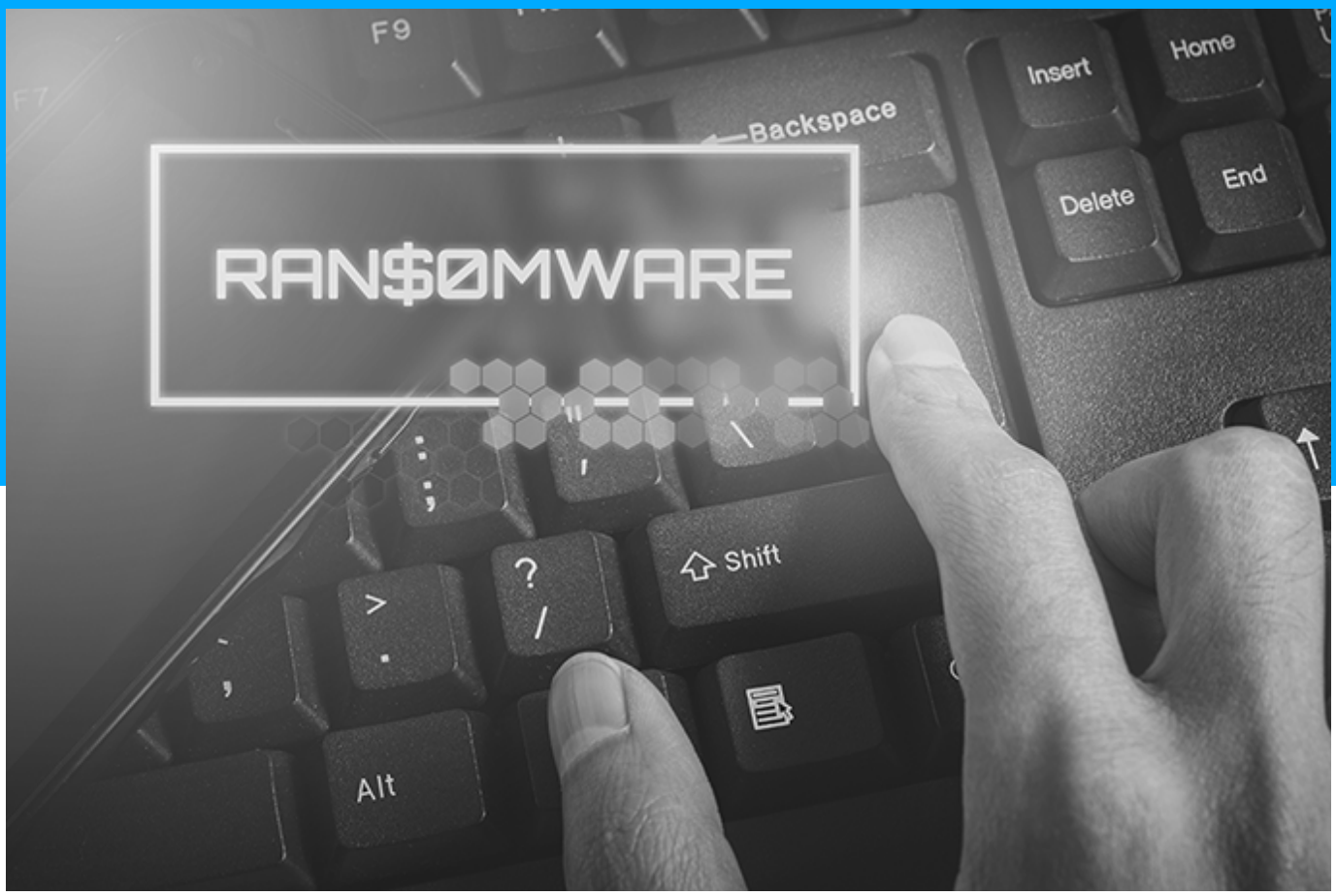
RANSOMWARE

THE FASTEST GROWING CYBER THREAT TO YOUR BUSINESS

WINDES
AUDIT | TAX | ADVISORY

ALLIANT
CYBERSECURITY
An alliantgroup Company



The World Economic Forum ranks "cybersecurity failure" as the fourth most dangerous short-term risk the world will face alongside health pandemics and extreme weather events.[1]

Within that danger, Ransomware ranks as the second biggest cyber threat after social engineering.[2] Exploiting others by holding sensitive and valuable information is an age-old crime, but the digital age has changed the game.

Stealing and encrypting sensitive data, locking down a system, or extorting a business has never been easier. Ransomware has emerged as the preferred method for cybercriminals looking for easy money. Bad actors do not even need to have technical skills to hack into a system, they can now pay for RaaS (Ransomware as a Service) to perform the attack on their behalf. Anyone can be a threat now.

1. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
2. https://www.securitymagazine.com/articles/94506-5-biggestc bersecurity-threats

What is Ransomware?

By definition,
Ransomware is a type of malware that encrypts the whole or part of your data and holds it for ransom.

In a typical attack, criminals will take advantage of any exploitable information. These include proprietary business information such as IPR, client/customer personal data, PII, PHI, R&D files, tax, and other legal information to keep that data from the owner or threaten to release it in a damaging manner until a ransom is paid. They may also lock the owner out of a system completely to shut down operations.

Paying the ransom may not even be the end of it. There are many instances where the attackers do not keep their promises, and there are no guarantees. The attacker may not release all the data or return the data in a damaged form due to poor decryption. Even if the data is received, there is evidence that attackers tend to leave "bread-crumbs" or loopholes to create backdoor entries for future attacks.

Ransomware Threat Trends

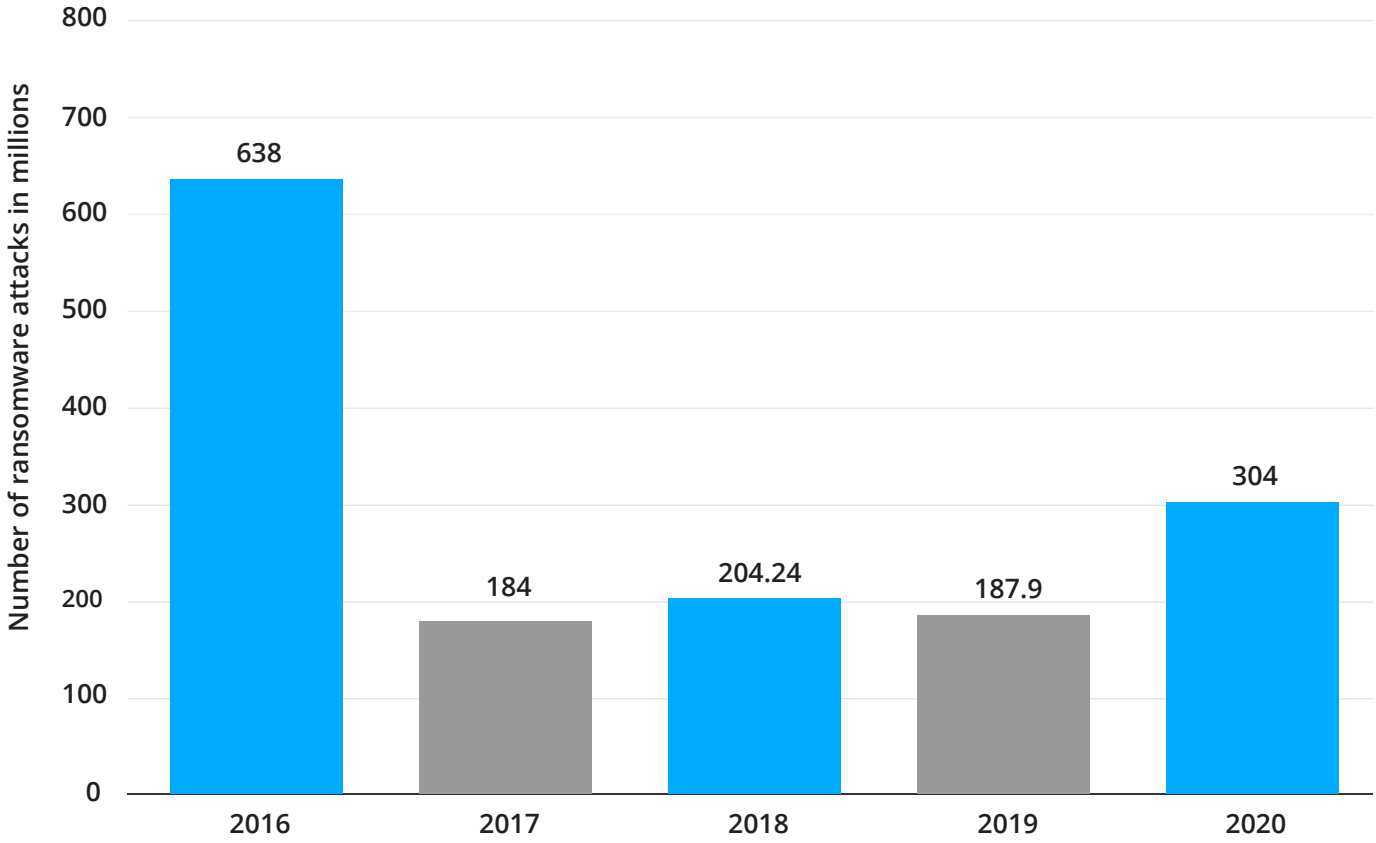
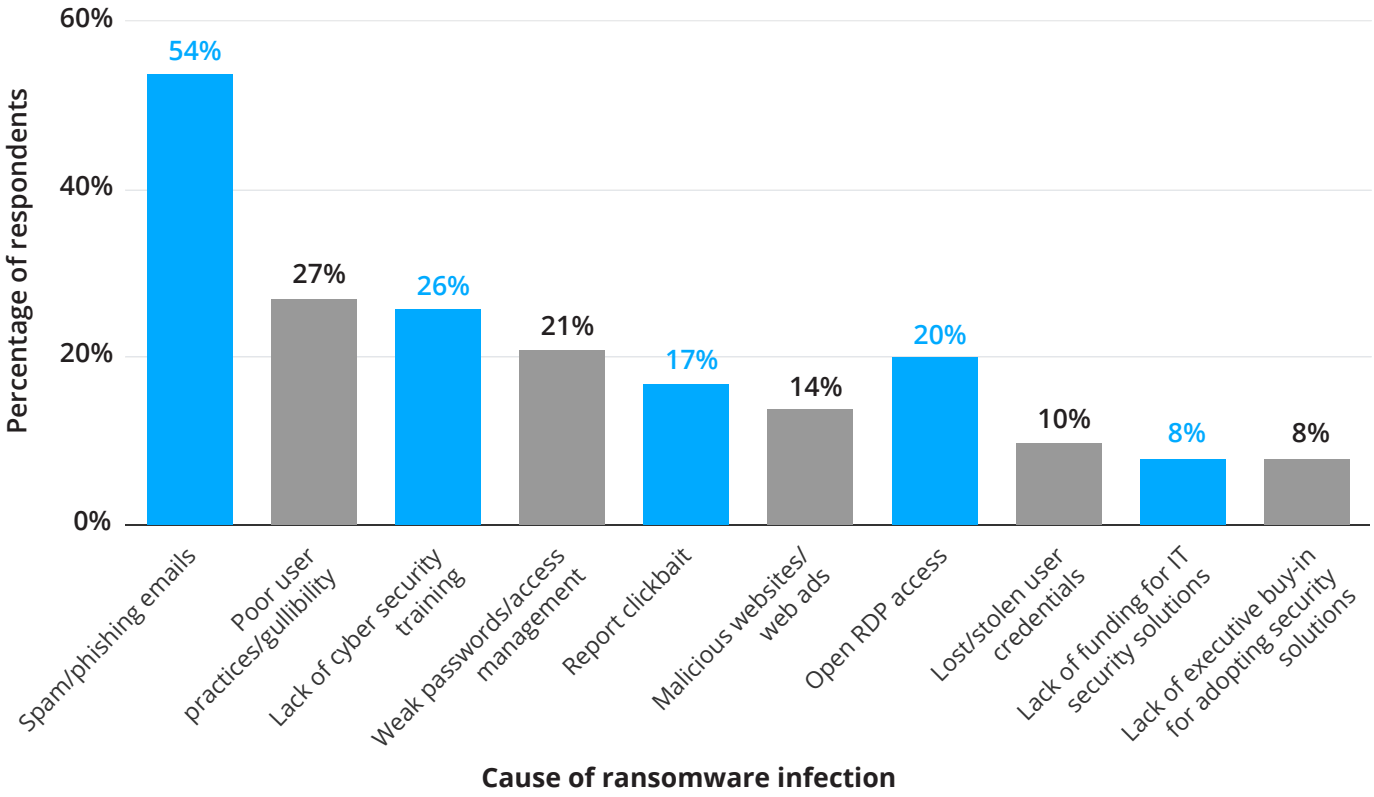


Table 1: Costs Associated with Ransomware Incidents in 2020 in the US, Canada, and Europe (USD)		
	2020 Data	Earlier Data (Where Available)
Avg. ransom demand	$847,344	-
Avg. ransom paid	$312,493	$115,123 (2019)
Highest ransom demand	$30,000,000	$15,000,000 (2015-2019)
Highest ransom paid	$10,000,000	$5,000,000 (2015-2019)
Lowest ransom demand	$1,000	-
Avg. cost of forensic engagement	$73,851	$62,981 (2019)
Avg. cost of forensic engagement, small and midsize business	$40,719	-
Avg. ransom demand, small and midsize business	$718,414	-
Avg. cost of forensic engagement, large enterprise	$207,875	-
Avg. ransom demand, large enterprise	$2,923,122	-

With the rapid adoption of digital solutions and the cloud came increased productivity and flexibility. But the global pandemic essentially pushed the workforce to work from home, and in doing so, provided a fertile and large attack surface for cybercriminals to attack. Hackers took advantage of the opportunities presented and launched aggressive attacks on the remote and mobile workforce.



In the past months, there have been an alarming number of cyberattacks directed towards non-IT companies. Since they do not have proper employee training and best practices, they are an easy target for attackers.

Many healthcare organizations have been in the news during the early days of the pandemic for being victims of data breaches. Reports indicate that about 25% of attacks occur on manufacturing companies, followed by professional services (17%) and government organizations (13%).

(https://securityintellgence.com/posts/ransomware-2020-a tack-trends-new-techniques-affecting-organizations-worldwide/)

There is no code of conduct for these cybercriminals or groups. Their methods of attacks and the selection of their targets have no logic. No organization is too small or remote not to be a target. By now, it is clear that the question of ransomware attacks is no longer an "if" but rather a "when."

Ransomware is here to stay!

What Makes Ransomware Attacks Different?

Ransomware is a clear and focused act of extortion. Although it is technically a subset or a type of malware, Ransomware is much more complex because it encrypts data and holds the decryption key for ransom.

Ransomware as a Service (RaaS)

Gone are the days when an attacker has to write code and keys to infect or attack a business. One of the primary reasons why Ransomware is becoming more dangerous is the evolution of the Ransomware as a Service or RaaS model.

RaaS is based on the popular subscription-based Software as a Service (SaaS) business model. This service enables the cybercriminals to use off-the-shelf malware to launch Ransomware attacks. The developers of the malware have different business models to profit from each Ransomware attack.

All the attacker needs to do is log in to the RaaS portal on the dark web, pay with the accepted cryptocurrency, and upload a request for a ransomware attack for a target he is seeking to exploit. Several communities offer training, video material, malware, and many other benefits to plot a Ransomware attack. Many portals even offer after-attack status, payment solutions, and additional information as well.

The RaaS model is dangerous because:

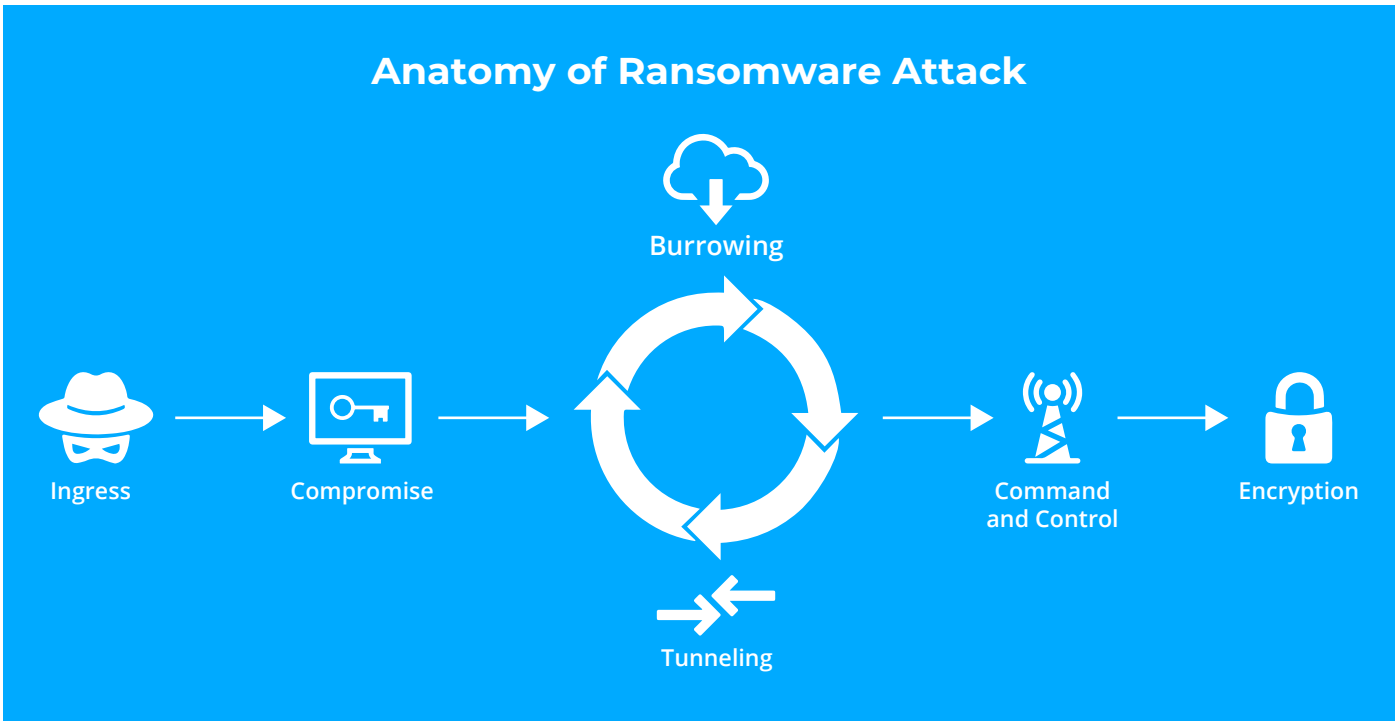
- It has made launching an attack easier. All you need to do is to create an account on the RaaS portal and pay using bitcoins.
- It has made Ransomware reusable. Successful infection can be modeled or copied to infect similar businesses across the world.
- It has created competitiveness among the criminals to offer better pricing or more sophisticated malware.
- RaaS operators also share kits with videos, whitepapers, and other supporting material to help criminals launch a cyberattack—attracting more criminals to launch their own ransomware attacks.
- RaaS operators use different monetary models: They sell, lease out, partner, or share profit revenues with other bad actors to perform a ransomware attack.
- Cybercriminals who purchase RaaS do not need to know how to write code or have an extensive understanding of their software. They will drop it into the network of whatever business they want to target with a simple "click next" to complete the process.

Prevention

Having a war-like mindset is necessary now. You must prepare up your defenses and prevent an attack. That is the only way.

Having specialist vendors who offer a combination of people, processes, the tools necessary to perform the network and endpoint threat monitoring, detection, and response for your organization. Some of these include:

- Managed Security Service Providers (MSSP)
- SOC as a Service (SOC)
- Security Information and Event Management (SIEM)
- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)
- User Behavioral Analytics (UBA)
- Co-Managed SIEM/SOC Services



Ransomware attacks typically play out as follows:

- The attacker either uses a fake website,a phishing email, or a trojan to trick you or someone at your company into downloading a malicious file or malware.
- The malware spreads across the network to infect other systems (generally doesn't infect the first system). Often, the malware lays dormant until it reaches its desired target or system to avoid detection.
- Depending on the Ransomware, the malware will either encrypt the entire operating system or some selected files or file types. At that point, you will be completely locked out of your system or unable to access your files.
- The victim will then receive a message demanding payment in exchange for: decryption of the data, to prevent their system from being permanently damaged, or sensitive data from being released. The malware can also remain dormant and undetectable. This dormant period can often be 200+ days after initial compromise.

Common Methods of Infection:

Let us look at a few primary ways ransomware is introduced or spread:

Phishing emails:

Are the most common attack vector. Attackers craft phishing emails to trick a victim to open an attachment or click on a link containing a malicious file.

Compromised Credentials:

The attacker, either through an email or any other social engineering attack (by posing as a legitimate member of your team or vendor), obtains your employee credentials. Credentials are often harvested on the dark web from other major data breaches like LinkedIn, Uber, etc. without your company or users knowledge that they have been compromised.Later, use the stolen credentials to infect and spread the Ransomware file.

Drive-by downloads/Malicious websites, URLs:

These are malicious downloads that happen when a user visits a compromised website or malicious URL. The file downloads occur without the user's knowledge and spreads through the network.

Unchecked USB sticks:

This happens when you reuse an infected USB stick without formatting or running an anti-virus check.

Remote desktop protocol (RDP):

RDP is a common communications protocol used in offices to communicate, access, and control systems, data, and resources remotely within a network. Unsecure or misconfigured RDP is a quick way Ransomware spreads from one infected device to another in an organization's network.

Supply chain vulnerabilities:

Many attacks exploit software that is out of date or has vulnerabilities that have not effectively been updated to the latest version with new security features to prevent against the exploit.

Pirated Software:

Often, pirated software often has bread crumbs or loopholes that make it easy for attackers to exploit and inject a malware.

Mitigation and defense techniques

Risks of Paying The Ransom

Paying the ransom is sometimes an option, but it is an elevated risk. You should always work with a security consultant who can advise on overall process and handle the negotiations - ideally, have one on retainer - and you should inform law enforcement.

For most ransomware, it is in the attacker's interest to provide decryption keys upon receiving payment. A reputation of following through allows for the attacker to promote further payouts by other victims and leads to increased financial gain for the attacker.

However, some ransomware may go for a "double-dip," which means they will continue to withhold the decryption key and ask for more money once you pay the initial ransom demand. Sometimes, you may never receive a decryption key, and attackers will continue to ratchet up the price to see how much they can get from you. Other ransomware only exists to disrupt or destroy. NotPetya is considered to have been a “wiper” disguised as Ransomware. Even when payment was been made, the attackers will not provide decryption keys.

Blue Sentinel

Intelligent Response. Immediate Action. Around The Clock

Blue Sentinel is a combined Managed Detection Response (MDR) Service and Vulnerability Assessment Service that focuses on complete coverage for your business with out-come-based security.

Blue Sentinel, with its team of dedicated cybersecurity engineers provides a complete cyber service with the flexibility to scale to your needs and customized solutions to ensure you have a 24/7/365 coverage service that is built for you.

Through vulnerability assessments and proactive threat hunting, our security engineers actively look for evidence of a cyber-attack or event, collecting threat intelligence from open source intelligence and industry renowned threat intelligence feeds, identifying key indicators of compromise, and using our teams to respond to identified threats.

Businesses Don’t Just Want Alerts; They Want To Know That The Threats Have Been Addressed

Constant Vigilance, Rapid Response, Dashboard Visualization

In addition to the team of dedicated cybersecurity engineers, the Blue Sentinel delivers a range of visualization options, from dashboards to customized reports. These deliverables and ongoing reports are built for you, providing the information you need to be in control of your cyber posture at all times.

Comprehensive. Effective. Readable.

Our dashboards constantly monitor the cybersecurity threat landscape for your business and presented it efficiently, allowing you to share and educate your business’s cyber stance, from the C Suite to the Shop Floor.

By presenting Blue Sentinel’s assessments in interactive dashboards, your business can isolate weaknesses and potentially identify the shortcomings of your current cyber tools and software. By displaying the vulnerabilities more clearly, your business can better justify the necessary steps needed to remain safe.

Comprehensive. Effective. Readable.

Businesses are now more aware than ever of the impact a cyber-attack can have, from extortion and production downtime to reputational damage and potential litigation. Yet, the steps to address threats are often seen as an IT cost rather than a cost of doing business.

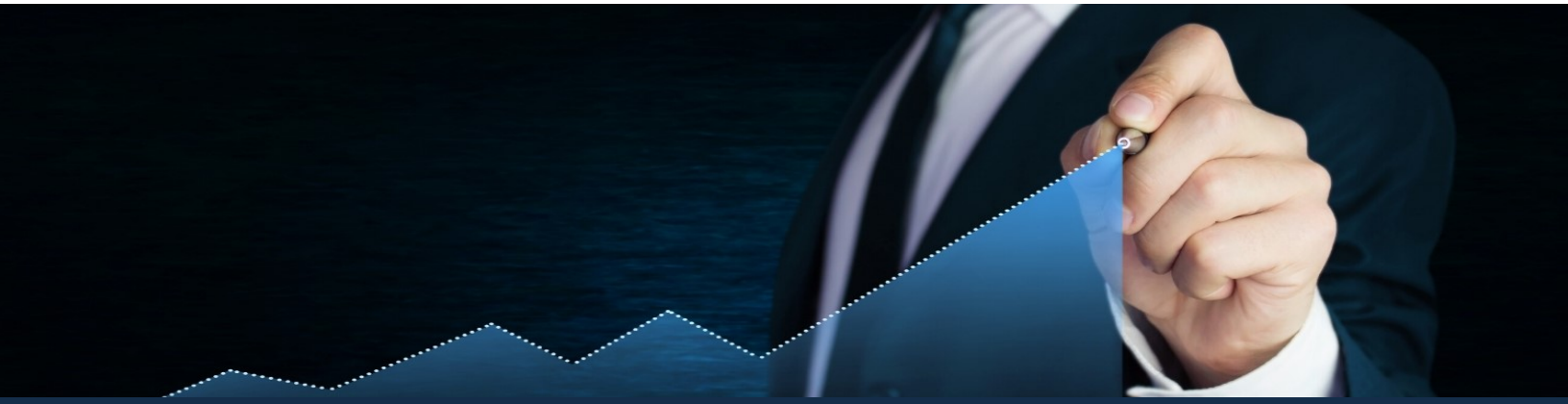
Blue Sentinel takes cyber security off your plate by being your in-house defense and response team at a fraction of the cost of assembling a team in house. If we see an event, behavior, or any suspicious activity, our security operations center will respond immediately to protect your business and people. A cybersecurity strategy that has data-driven threat intelligence and built-in analytics is critical, and Blue Sentinel delivers

WINDES

AUDIT | TAX | ADVISORY

Windes is a recognized leader in the field of accounting, assurance, tax, and business consulting services. Our goal is to exceed your expectations by providing timely, high-quality, and personalized service that is directed at improving your bottom-line results. Quality and value-added solutions from your accounting firm are essential steps toward success in today's marketplace. You can depend on Windes to deliver exceptional client service on each engagement. For 95 years, we have gone beyond traditional services to provide proactive solutions and the highest level of expertise and experience.

The Windes team approach allows you to benefit from a wealth of technical expertise and extensive resources. We service a broad range of clients, from high-net-worth individuals and nonprofit organizations to privately held businesses. We act as business advisors, working with you to set strategies, maximize efficiencies, minimize taxes, and elevate your business to the next level.



Headquarters

3780 Kilroy Airport Way

Suite 600

Long Beach, CA 90806

562.435.1191

Orange County Office

2050 Main Street

Suite 1300

Irvine, CA 92614

949.852.9433

Los Angeles Office

515 Flower Street

Eighteenth Floor

Los Angeles, CA 90071

213.239.9745

www.windes.com