Cybersecurity Threats 2022

THREATLOCKER®

Managed IT Services

In this report, we will explain the realities of cyberattacks on **[industry type here] businesses** like yours.

SIZE
Doesn't Matter

In 2020, 28% of breaches involved small business victims, according to the Verizon 2020 Data Breach Investigations Report.

What is **RANSOMWARE?**

Ransomware is a type of malware that infects your computer network and other devices. Once infected, your data is locked and encrypted, making it unusable and inaccessible until a ransom payment is received.

While a majority of ransomware encrypts data on the victim's server until the ransom is paid, we have observed an increase in double-extortion methods that take it a step further by copying the stolen data to a cybercriminal's server.

This means, even if a ransom is paid, the victim's data has already been exposed and will likely be exploited or sold illegally on the dark web. Therefore, backing up data is not enough for businesses to mitigate the threat.

It is critical that business leaders begin taking a proactive approach to prevent these attacks from compromising, releasing, and destroying sensitive data.

How do users get **RANSOMWARE?**

There are a number of ways in which ransomware is spread, including malicious email attachments and URLs. A file can be delivered in a variety of formats including Word documents, Excel spreadsheets, PDFs, zip files, and more. When a user clicks on a malicious link or file, ransomware can immediately deploy or remain dormant for days, weeks, or even months before encrypting a victim's files.

While you may think it's easy to spot a malicious email, cybercriminals are becoming more sophisticated and often conduct extensive research on their target. As a result, ransomware groups are able to deceive users with very credible and believable emails.

If you are interested in learning more about the common ways in which ransomware is spread, please continue reading on page #4.

Small and Medium-Sized Businesses
Cybersecurity Trends in 2022

Cybersecurity measures have taken a giant leap in recent years to keep up with the ever-growing number of cyber threats. Some products make for excellent antiviruses or response tactics, but it's time to start thinking about how you will prevent cyber attacks from occurring in the first place.

According to Score, ransomware ranked number one among the top five cybersecurity threats to small businesses in 2022, with business email compromise (BEC) scams right behind it. The threat of human error that leads to employees opening malicious documents and links in BEC scams is why a proactive solution to prevent ransomware from spreading throughout your device or even your network is the missing piece to your cybersecurity stack.

ThreatLocker's solutions are curated to provide the proactive security and defenses your organization needs to handle a slip in human error that could cause devastating harm to any SMB. These solutions stop malware from hurting your organization before it gets the chance.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

UK Legal
Cybersecurity Trends in 2022

Falling victim to a cyberattack is devastating for a law firm or legal service provider. Hosting the sensitive data of a client and losing it in a cyberattack not only means you may lose a certain case, lose the client, or become subject to a lawsuit for negligence, but you also risk losing the credibility that your firm holds entirely. An unfortunate example is when one law firm, Ward Hadaway, fell victim to a ransomware attack that demanded £4.75m in bitcoin for the decryption of confidential documents.

The 2021 / 2022 UK Cybersecurity Cybersecurity Census Report, published by Cybercrime Magazine, states that more than most businesses, professional service providers in legal, consulting, accounting, and other professional services organizations are the keepers of massive volumes of personal, confidential, or commercially sensitive data. Making them high-priority targets for cybercriminals, much higher than most other organizations outside of their industries.

The ThreatLocker solution is comprised of five key components: Allowlisting, Ringfencing™, Elevation Control, Storage Control, and Network Access Control (NAC). Together, each component of the solution works to help businesses stay better protected and reduce the risk of cyberattacks. Throughout this guide, we will give you the tools and resources you need to defend and protect your business whilst staying ahead of the latest cyber threats.

US Legal
Cybersecurity Trends in 2022

Cybercriminals are attracted to organizations that host large amounts of sensitive data as well as those whose reputations would be heavily tarnished by the news that a data breach has occurred, making law firms in the United States an attractive target for cyberattacks and data breaches. Losing sensitive data in a cyberattack means you may fail in a particular legal case, lose a number of clients, or become subject to a lawsuit for negligence. You also risk losing the credibility your firm holds entirely, creating an irredeemable setback for your entire organization.

Two New Jersey-based, mid-sized law firms “McCarter & English” and “Stevens & Lee” announced on April 22, 2022, that they experienced a data breach in June 2021 which remained undetected until April 2022. After their announcement, a consumer rights legal firm quickly started an investigation on behalf of Stevens & Lee’s clients, finding that cybercriminals had stolen the private information of “a very large number” of people. Unfortunately, in this scenario, the two firms’ journey to restoring their reputation as firms that use dependable data security approaches will be arduous.

The ThreatLocker solution is comprised of five key components, Allowlisting, Ringfencing™, Elevation Control, Storage Control, and Network Access Control (NAC). Together, each element of the solution works to help businesses stay better protected and reduce the risk of cyberattacks. Throughout this guide, we will give you the tool and resources you need to defend and protect your business while staying ahead of the latest cyber threats.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Financial Sector
Cybersecurity Trends in 2022

Organizations within the banking industry are prime targets for cyber attacks because of the amount of sensitive data they host. A cyberattack that compromises your clients' personal data will strip your firm of its credibility, ultimately damaging the chances of bringing in new clients and customers. Additionally, reputational damage incurred may halt business development and contribute to your company going out of business.

In February 2022, Professional Finance Company, Inc. (PFC) fell victim to a cyber attack from the Quantum Ransomware gang. The attack affected 657 entities, majority of which were in the healthcare industry, and around 1,918,941 individuals were affected. Per those healthcare clients, patient information including names, addresses, account receivable balance, and dates of birth, social security numbers, health insurance, and the medical treatment provided were all compromised by the attacking party.

Waiting too long before you initiate your organization's cybersecurity will dramatically increase your risk of a cyber attack. Investing in a reliable cybersecurity solution like ThreatLocker can put your organization one step ahead of cyber threats and reduce your chances of falling victim.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Manufacturing **Cybersecurity Trends in 2022**

As early as March of 2022, the Association of Equipment Manufacturers published an article covering what they predicted to be 2022's top manufacturing cybersecurity risks. This list includes, but is not limited to, ransomware, phishing, social engineering, insider threats, and the lack of protection.

The manufacturing industry is just as targeted as any other industry by cyber threats, if not more. Organizations within the manufacturing industry are starting to catch up and build a robust cybersecurity infrastructure in 2022. Even with this steady incline, it still falls behind other industries, making it a big target for attacks like ransomware. So, it is only a matter of time before a manufacturer, whether a small business or a significant player, experiences an industry-halting cyber attack.

Waiting too long before you initiate your organization's cybersecurity will dramatically increase your risk of a cyber attack. Thus, raising the possibility that you may need to suspend manufacturing operations, leaving you and your organization at a significant loss. Investing in a reliable cybersecurity solution can put your organization one step ahead of cyber threats and reduce your chances of falling victim.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

Government Organizations **Cybersecurity Trends in 2021**

Cybercriminals often view government organizations as an easy target. That's why you can depend on [Company Name] to ensure your systems are taken care of, data is kept secure, and help is at hand when you need it.

Government agencies hold a remarkable amount of information about citizens from passport information to social care information. It makes the public-sector prime targets for cybercrime.

If that isn't alarming enough, public-sector groups have a hard time knowing when they've been attacked. Public-sectors lag behind in terms of time to spot and contain data breaches. In 2020, the average across public-sectors to find breach was 231 days.

The purpose of this document is to help educate you on the cyber landscape today so that you understand why solutions like [Company Name], will help keep your business safe.

$1.6M

IBM Cost of a Data Breach Report 2020

Breaches found in the public-sector cost an average of $1.6 million per breach.

Retail/Wholesale **Cybersecurity Trends in 2022**

The Retail and Wholesale industry is a gold mine for cybercriminals due to the amount of personal data they hold, including employees, clients, and customers.

As the number of sellers entering the ecommerce space increases, or even just creating some form of online presence, so does the risk of cyberattacks. In fact, recent data shows that retail and wholesale organizations are more vulnerable to ransomware, with one in every five attacks targeting an online retail business (21%).

The possibility of cyberattacks puts the customers' sensitive data and personal information at a huge risk. Even if sellers don't have ecommerce sites, they can become subject to cyberattacks so long as they hold some type of online presence. Whether it be in the form of a company website, or just relying on the internet to conduct business and/or host valuable, classified data.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

Staffing & Recruiting **Cybersecurity Trends in 2022**

Cyberattacks are devastating to any agency in the staffing and recruiting sector that depends on technology and the internet for communicating and storing sensitive data.

Staffing and recruitment firms are prime targets for cyberattacks as hosts of personal data for clients, candidates, employees, and job applicants, including sensitive information like addresses, salaries, and I-9 documents. Unfortunately, a cyberattack that compromises client or candidate personal data will strip any firm of its credibility, ultimately damaging the chances of bringing in new clients and candidates. Reputational damage may halt business development and contribute to the company going out of business.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Supply Chain & Logistics **Cybersecurity Trends in 2022**

Cyberattacks on companies within the Supply Chain and Logistics Industry can be devastating to the company itself, but also to the other companies, clients, and consumers that depend on their products and/or services.

Global Trade states that a weak link in supply chains' security is actually their Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs). These supply chain organizations expect full protective services from their MSPs/MSSPs, and implicitly trust them with their security needs. A single single slip-up with ransomware from either party can be devastating to both organizations as well as those who depend on their services. This is why implementing strong zero trust cybersecurity solutions will help businesses and MSPs/MSSPs to better defend and prevent future cyberattacks from causing irreversible damage.

In addition to this, it was announced in September 2022 that the White House plans to build on the President's Executive Order to improve the nation's cybersecurity with zero trust compliance, focusing on software supply chains through secure software development practices.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Insurance Firms
Cybersecurity Trends in 2022

With the number of devices entering the market as well as the technical advancement seen from threat actors, the insurance industry is seeing a rise as both a target and as providers of cyber insurance; firms that are willing to take on the financial risk of cyber attacks in exchange for a fee. This goes to show that the threat of cyber attacks is

IAs hosts for the personal, sensitive data of millions of customers, insurance providers, and other organizations working in the insurance industry, are prime targets for cyberattacks. Without the right cybersecurity strategies in place, companies are at risk of losing countless amounts of data like names, addresses, and salaries, to name a few.

In October 2022, Kingfisher insurance fell victim to the ransomware group Lockbit, the most active ransomware group in the third quarter of 2022, committing 37% of ransomware attacks during that time period, and having a 5% increase over the previous quarter. They claimed to have acquired 1.4 terabytes of data in which they threatened to publish if Kingfisher did not respond to their (undisclosed) financial demands by November 28, 2022.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint

Defense Industry **Cybersecurity Trends in 2022**

According to the U.S. Department of Defense(DOD), "cybersecurity is a huge concern for the department, the companies, and national security." The industrial base comprises 220,000 companies, all at risk of cyber threats that serve a financial, political, or destructive purpose for

The need for cybersecurity in the defense industry will continue to rise with the exponential growth of cyber attacks. In a report published by Fortune Business Insights, it is predicted that the global defense cybersecurity market will grow to $29.81 billion by 2028, an increase of almost $20 billion more than 2021's $19.96 billion, which saw growth following the pandemic's push towards the digital space in 2020.

In a bid to better protect these organizations and to mitigate cyberattacks before they have the chance to cause any damage, the Department of Defense held a town hall in which they stated that they will be "sharing threat information, offering easy-to-implement ways the industrial base can shore up its own cyber defenses, and looking for ways to make further improvements as the threat continues to evolve."

ThreatLocker can help you manage your cybersecurity efforts to help you better protect your business from cyberattacks. Throughout this document we will give you tips and best practices to help keep your business safe and secure. You'll also see why the need for a policy-driven, endpoint security solution has never been greater.

Maritime Industry **Cybersecurity Trends in 2022**

In August of 2022, Sembcorp Marine Ltd discovered a cybersecurity incident where an unauthorized party accessed part of its IT Network via third-party software products. It was established that the personally identifiable information from all employees, previous and current, as well as non-critical data relating to operations was breached.

The marine industry is becoming increasingly targeted by cyberattacks, and this is showing no signs of slowing down. Each attack causes a huge amount of disruption and downtime, as well as huge financial losses. Although cybersecurity efforts have dramatically improved, cyberattacks are still the biggest threat to the maritime industry.

Following many news stories of the countless large-scale cyberattacks, the Maritime and Port Authority (MPA) of Singapore recently signed a Memorandum of Understanding (MOU) to strengthen cybersecurity collaborations between nine private and public players to develop cybersecurity skills and talent over the next three years to increase capabilities.

Throughout this document we will give you tips and best practices to help keep your business safe and secure. You'll also see why the need for a policy-driven, endpoint security solution has never been greater.

The Energy Sector **Cybersecurity Trends in 2022**

The energy sector is comprised of businesses related to the production and supply of energy, the basis of modern society. According to the Cybersecurity and Infrastructure Security Agency (CISA) 'Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function.'

Energy companies hold a large amount of data and operational importance, and because of this, they are huge targets for cybercriminals. It is imperative that businesses operating within this sector keep on top of their cybersecurity efforts.

The production of semiconductors have become a vital part of both the tech and energy industries. In 2022, semiconductor manufacturers were hit by several ransomware attacks which were variants of existing ransomware including LockFile, AtomSilo, Rook, Night Sky, and Pandora. For nations investing in semiconductors, like the United States which signed a bill to invest $52.7 million, this slows down economic growth and technological advancement.

Italy's state-owned energy services firm GSE fell victim to a ransomware attack that stole around 700G of data and threatened to publish it online. The ransomware in this scenario, BlackCat, is known to target mainly organizations in the energy industry. Implementing a zero trust security solution into your security stack could be the proactive defense your organization needs to fight off threat actors like these.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Property Management **Cybersecurity Trends in 2022**

Organizations in Real Estate and Property Management, like many other industries, are encountering a drastic increase in the number of cyberthreats everyday. Because of this, residents, employees, and owners constantly face the risk of having their personal data exposed and/or stolen by malicious softwares.

Bunkhouse Management, a property management company specializing in boutique hotels in the hospitality industry, announced on November 11, 2022 that they had experienced a data breach of their customer's personal identifiable information. Information breached included individuals' names, social security numbers, financial information, and health insurance information.

ThreatLocker's software and services step in to help you manage your cybersecurity efforts and protect your business from cyber attacks and security breaches by applying our ZeroTrust policies to stop malicious software at the source, denying them the chance to access your server and confidential files entirely.

Throughout this document, we will give you tips and best practices to help keep your business safe and secure. You'll also see why the need for a policy-driven endpoint security solution has never been greater.

Government
Cybersecurity Trends in 2022

Cyber threats are ever-growing alongside the constant evolution of modern technology. With this, the scope and size of their targets has grown exponentially, now including governmental organizations.

In 2022, governments of all sizes fell victim to ransomware attacks. Westmount, Quebec, Canada, a city with 21,000 residents, had municipal services and employee email shut down in November. In two weeks, the city had to decide whether or not they would pay the undisclosed ransom demanded to decrypt the ransomware. Other governments, including in the United States and Latin America, also fell victim to these harsh attacks, each experiencing their own slowdowns and ransom demands.

It is because of these massive spikes in cyber attacks in 2022 that the White House established an executive order to improve the United State's cybersecurity with the transition to a zero trust security architecture nationwide, starting in January 2023.

This guide will show you how each solution proactively defends against threat actors and malicious attacks, preventing them from spreading throughout your government's network and infrastructure. Thus, drastically reducing the threat of falling victim to phishing attacks, stolen credentials, exploited vulnerabilities, and more.

Airline & Aviation
Cybersecurity Trends in 2022

As the host of millions of customers' personal data, the Aviation Industry has become a substantial target for cyberattacks. As time passes, and technology advances, cyberattack attempts will only become stronger and more common.

In July of 2022, American Airlines had discovered that they had experienced a data breach leading to the compromise of a "very small number" of customers' and employees' personal information. It was then announced that the compromised information may have contained their date of birth, driver's license and passport numbers and medical information they provided to the airline.

When it comes to cyberthreats, response tools won't do the trick to defend your organization. [Company Name] provides solutions that take a proactive step in protecting your organization's devices, it's network, and the sensitive information of your employees and customers; taking the necessary proactive steps to stop cyber attacks before they get the chance to make an impact.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

Automotive
Cybersecurity Trends in 2022

In recent years, the number of cars with an internet connection, and some with internet reliability, has been on a steep incline. According to the Digital Journal, "The Global Automotive Cybersecurity Market size is projected to grow from $2.0 billion in 2021 to $5.3 billion by 2026, at a CAGR of 21.3%". Hackers have targeted automotive companies' servers for anything related to classified data, customer information, and industry secrets, and there are no signs of it slowing down.

The further we advance our vehicles with internet integrations, the more at risk they are from cyber threats. Studies as far back as 2015 have shown that vehicles with a weak enough cybersecurity system are capable of being hacked into. These vehicles lost control of their brakes, steering, and other functions to hackers.

When looking to the future, it is clear that automotive companies will need to expand the safety features their vehicles carry from physical crashes to virtual car hijacking. Only those with the strongest cybersecurity solutions can compete with the ever-evolving strategies of hackers.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

(Railroad & Trucking)

Goods/Human Transportation **Cybersecurity Trends in 2022**

Organizations in the Goods and Human Transportation Industry are a substantial target for cyberattacks. Not only can one negative event affect the whole global supply chain ecosystem, but it can put millions of customers' personal data at risk if not properly secured.

Mexico's transportation industry was knocked back when the Secretariat of Infrastructure, Communications and Transportation (SICT)'s servers were hacked in October 2022, delaying operations through the end of the year. Due to this halt in operations, the country's sector stopped issuing licenses, permits, and license plates for truck drivers, increasing difficulties for transporting goods over borders that checked official documentation.

Countless organizations in supply chain and logistics rely on goods and human transportation services. One security incident can leave heavy implications for other industries and the companies that operate within them.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Dental Offices
Cybersecurity Trends in 2022

Healthcare and dental organizations operate with valuable personal data that have made them prime targets of cyberattacks for many years. Even with a strong antivirus or endpoint protection and response tool, malicious software can still find ways into organizations' servers. Many times, this can even come from insider threats instead of external attacks.

In April of 2022, the United States Department of Health and Human Services (HHS) released a publication warning of the dangers and risks of insider threats to healthcare and dental providers. In an infographic, the HHS states that insider threats are persons within an organization with access to assets or insider information that they can use to impact the organization negatively

You can take action to significantly reduce the risk of insider threats by implementing proactive cybersecurity tools within your organization, such as [Company Name]'s Elevation Control which acts as a privileged access control manager. Limiting access to confidential and sensitive data to fewer trusted employees within your organization(s) helps reduce the risk of insider threats from taking action.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

Charities
Cybersecurity Trends in 2022

Organizations in the U.S.-based nonprofit and charity sector tend to be lax with their cybersecurity tactics which is why this, and the amount of personal and financial data they hold, make them a gold mine for cybercriminals.

AmTrust Financial has recently published an article stating that the three most common risks associated with charity business are online donations, Phishing scams, ransomware, and threat actors disguised as a volunteer, essentially a wolf in sheep's clothing. These three risks will only become more prevalent as cyber threats are ever-growing alongside the constant evolution of modern technology. So, threat actors have only become more sophisticated in their approach.

Waiting too long before you initiate your organization's cybersecurity will dramatically increase your risk of a cyber attack. Thus, raising the possibility that you may need to suspend all marketing and donation acceptance procedures. Investing in a reliable cybersecurity solution like [Company Name] can put your organization one step ahead of cyber threats and reduce your chances of falling victim.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

Educational Institutions **Cybersecurity Trends in 2022**

Cybercriminals do not discriminate based on whether you're a business or an educational institution. That's why you can depend on [Company Name] to ensure your systems are taken care of, data is kept secure, and help is at hand when you need it.

According to the nonprofit K-12 Cybersecurity Resource Center, there were 408 publicly documented data breaches or security attacks at K-12 schools in 2020, including student and staff data breaches, ransomware and other malware outbreaks, phishing attacks, and a range of other incidents.

If that isn't alarming enough, the average cost of ransomware attacks on educational institutions is $2.73M in downtime. Data breaches and leaks accounted for about 40% of K-12 cyber attacks, while ransomware accounted for about 12%. Denial-of-service attacks, for example, hampered access to commonly used remote learning applications.

The purpose of this document is to help educate you on the cyber landscape today so that you understand why solutions like [Company Name] will help keep your business safe.

Construction
Cybersecurity Trends in 2022

Like many other industries, organizations within the construction industry are highly vulnerable to cyberattacks without a proper cybersecurity strategy.

As the construction industry advances and begins to build its online presence via corporate communication tools, social media marketing platforms, and online portals for clients, organizations continue to put themselves at greater risk of a cyberattack.

In 2022, a new, devastating malware, named "Incontroller," that targets the construction industry, entered the market. The malware drives to shut down or sabotage a facility or disable safety controllers at various industrial sites, including power plants.

Waiting too long before you initiate your organization's cybersecurity will dramatically increase your risk of a cyber attack. Investing in a reliable cybersecurity solution like [Company Name] can put your organization one step ahead of cyber threats and reduce your chances of falling victim.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

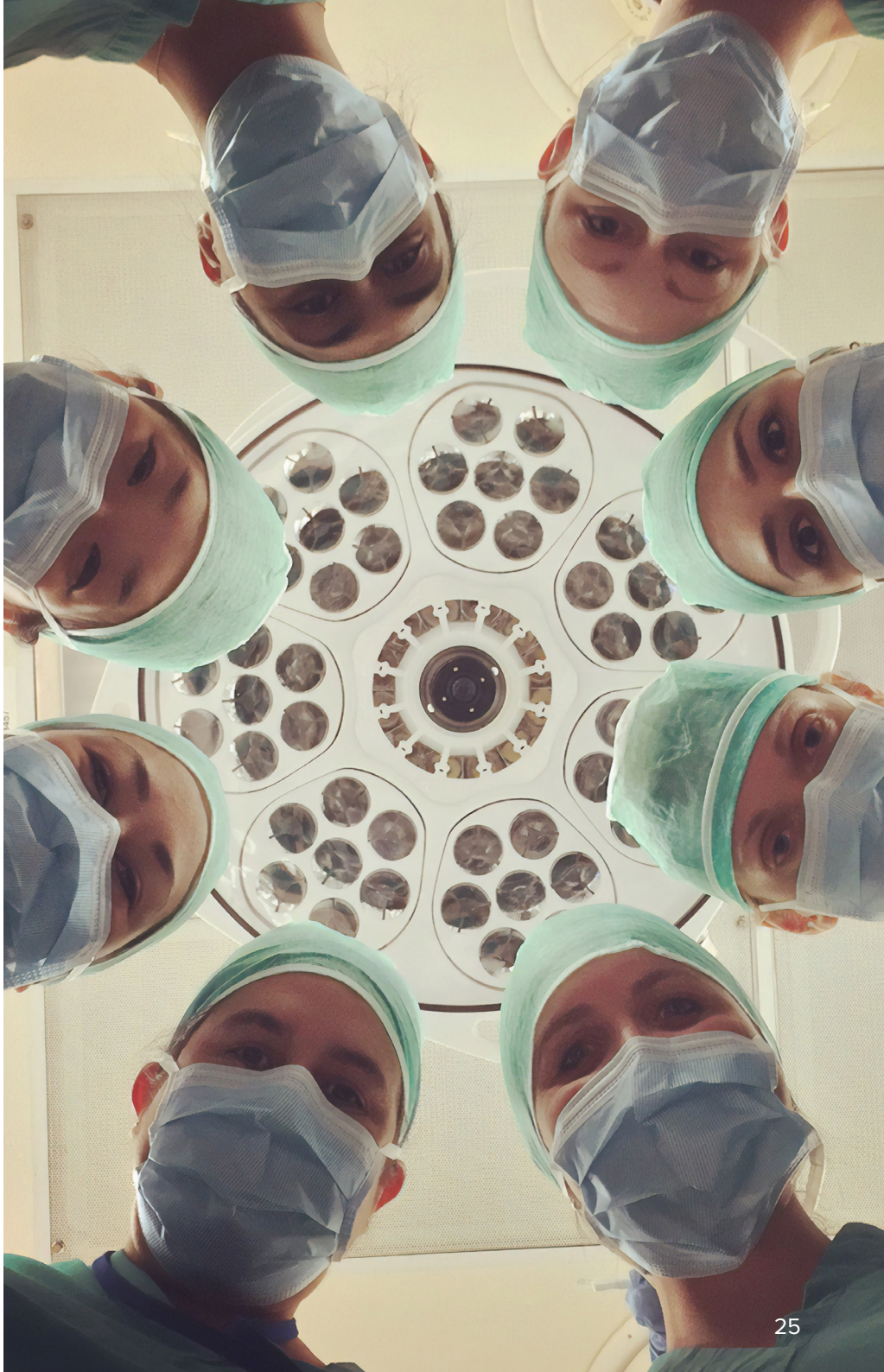
Healthcare
Cybersecurity Trends in 2022

Cybersecurity attacks were the talk of 2021 as their numbers soared to new heights. They grabbed news headlines and, more importantly, the attention of the U.S. government. Cybercriminals took advantage of hospitals and federal agencies when they shifted their focus to providing relief during the pandemic. Consequently, at the end of December of 2021, multiple healthcare/medical providers were forced to cancel surgeries, radiology exams, and other services because they had fallen victim to cyber attackers using the “Log4j” exploit accessing provider and patient data through the Java-based vulnerability.

In response to these events, an article was published by the U.S. Department of Health and Human Services in February of 2022. The author, and Director for the Office of Civil Rights, Lisa Pino, states that “prioritizing cybersecurity and patient privacy is of the utmost concern.” She strongly urges healthcare and medical providers to take action in 2022 following events in 2021 before it’s too late.

Waiting too long before you initiate your organization’s cybersecurity will dramatically increase your risk of a cyber attack. Investing in a reliable cybersecurity solution can put your organization one step ahead of cyber threats and reduce your chances of falling victim.

The purpose of this document is to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.



Banking
Cybersecurity Trends in 2022

Organizations within the banking industry are prime targets for cyberattacks because of the amount of sensitive data they host: personal finances, addresses, demographics, and more.

In June of 2022, Flagstar Bank announced that they had experienced a cyberattack in December of 2021, with hackers accessing customers' sensitive data like their social security numbers. The cyberattack had happened during Flagstar's acquisition by New York Community Bank.

Flagstar fell victim to the attack and didn't notice anything for another four months, proving that a proactive cybersecurity strategy is essential for preventing cyberattacks from happening right under your nose. Investing in a reliable cybersecurity solution like [Company Name] can put your organization one step ahead of cyber threats and reduce your chances of falling victim.

This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like [Company Name], will help keep your business safe and secure.

Utilities
Cybersecurity Trends in 2022

Organizations within the utilities industry have seen a growing increase in the number of ransomware attacks in recent years as cyber attacks spiked astonishingly everywhere. These utilities companies pose as a gold mine of personally identifiable information in the form of names, addresses, and credit/debit card numbers.

Unfortunately, a cyber attack that compromises client personal data will strip your organization of its credibility, ultimately losing customers and damaging the chances of bringing in new business. In late 2022, South Staffs Water was hit by a devastating ransomware attack that led to customers' data being leaked to the dark web. Confirmed data included names, addresses, bank details like sort codes and account numbers, and other personal data. Customers of South Staffs Water now accuse the company of trying to minimize the issue and acting recklessly.

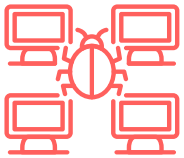
This document aims to give you an overview of the current cybersecurity landscape and to help you understand how an endpoint security solution, like ThreatLocker, will help keep your business safe and secure.

Types of Malware

Malware is a piece of malicious software designed by cybercriminals to steal your data and carry out other nefarious behaviors. Malware can be spread in many ways, including phishing, malicious URLs, downloads, browser extensions, and more.

Ransomware

Ransomware is a type of malware that infects your computer network and other devices. Once infected, your data is locked and encrypted, making it unusable and inaccessible until a ransom payment is received.



Virus

A Virus is another form of malware that, when executed, replicates itself by modifying other computer programs and inserting its own code.

Worms

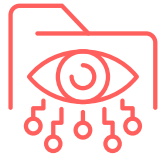
Like viruses, worms replicate in order to spread to other computers over a network. In the process, they cause harm by destroying files and data.

Trojan

A Trojan is a form of malware that can be used to steal financial information or install ransomware. This is one of the most dangerous forms of malware, as it is often disguised as legitimate software.

Keylogger

This malware records all of the keystrokes on your keyboard. This sends all of your sensitive information, including credit cards, passwords and other user credentials to a cybercriminal.



Spyware

Spyware is malicious software designed to enter your device, gather your information, and forward it to a third-party without your consent. This software is used to profit from stolen data.

The Cost of **Falling Victim**

Ransomware attacks are constantly making news headlines. However, the stories you hear often focus on large enterprise organizations.

Today, cybercriminals frequently target small to medium-sized organizations, which are often more vulnerable to these attacks. Additionally, ransomware attacks can destroy a business as a result of the financial burden inflicted from direct and indirect damage.

In addition to the ransom payout, you must factor in downtime, reputational damage, data loss, and other repercussions that may follow.

2020 Average

In 2020, the average ransom demand for SMBs was about $233,817. However, this does not factor in the downtime and damages that follow. The average cost of downtime in 2020 for SMBs was $274,200 which is nearly six times higher than it was in 2018 at $46,800.

Compromised Data

On the dark web, the average cost of stolen documents and accounting data is about $1285. Victims who have had their organizations records compromised are often left grappling with the effects years later.

Recovery Time

As of January 2021, the average number of days a ransomware incident lasts is now 19 days. This is a result of the time needed to remediate and restore systems after an attack.

How ThreatLocker®
Protects Your Business

Small to medium-sized businesses are constantly buying into the latest technologies such as next-gen antivirus software and threat detection solutions that use machine learning, artificial intelligence, advanced heuristics, blockchain, and more.

However, none of these solutions protect against the latest cyber threats, including ransomware and other forms of malware. Millions of dollars are spent on cybersecurity annually, yet companies that rely on threat detection are still getting compromised.

Most cybersecurity protections are based on looking for, finding, and stopping threats. The problem is, cybercriminals are getting smarter and entering networks undetected. End-users are constantly inviting threats through actions such as downloading various applications without your approval, clicking on links they shouldn't, and opening attachments in e-mails.

That's why a new approach of blocking everything that is not trusted and only allowing those applications that are approved is a far cleaner and more comprehensive approach to ensuring malware does not end up on your networks.

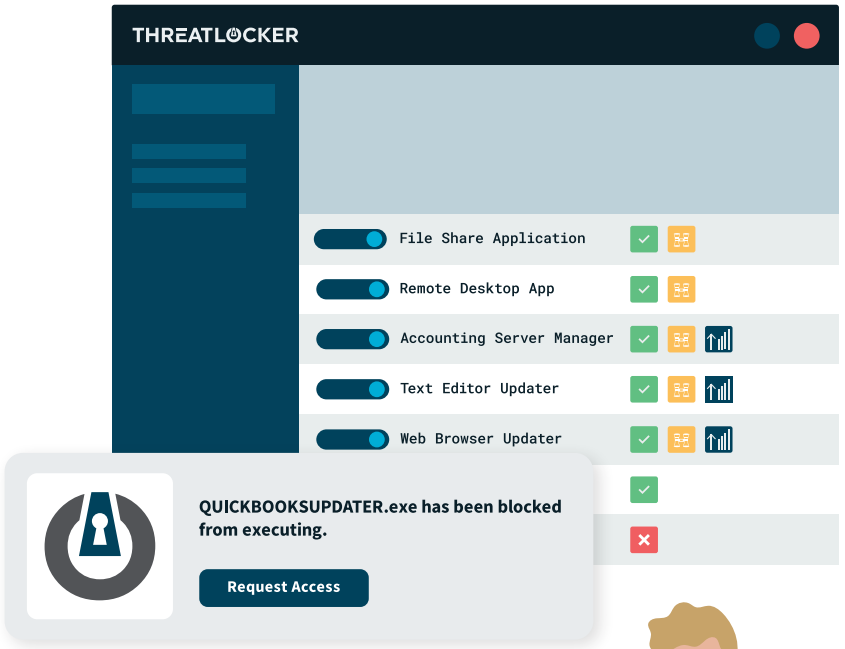
ThreatLocker® combines Allowlisting with Ringfencing and Storage Control in ways that make security simple. By combining these solutions, your applications will not be exploited.

What is **Allowlisting?**

Application Allowlisting denies all applications from running except those that are explicitly allowed. This means untrusted software, including ransomware and other malware, will be denied by default.

When the agent is first installed, it operates in Learning Mode. During this period, all applications and their dependencies that are found or running on the computer are cataloged, and policies are created to permit them. After the learning period, the IT administrator can review the list of applications, remove those that are not required, and secure the computer. Once the computer is secured, any application, script, or library that tries to execute that is not trusted will be denied. The user can request new software from the IT administrator, and it can be approved in 60 seconds.

Application Allowlisting has long been considered the gold standard in protecting businesses from known and unknown malware. Unlike antivirus or traditional EDR, Application Allowlisting puts you in control of what software, scripts, executables, and libraries can run on your endpoints and servers. This approach stops not only malicious software but also stops other unpermitted applications from running. This process greatly minimizes cyber threats and other rogue applications running on your network.

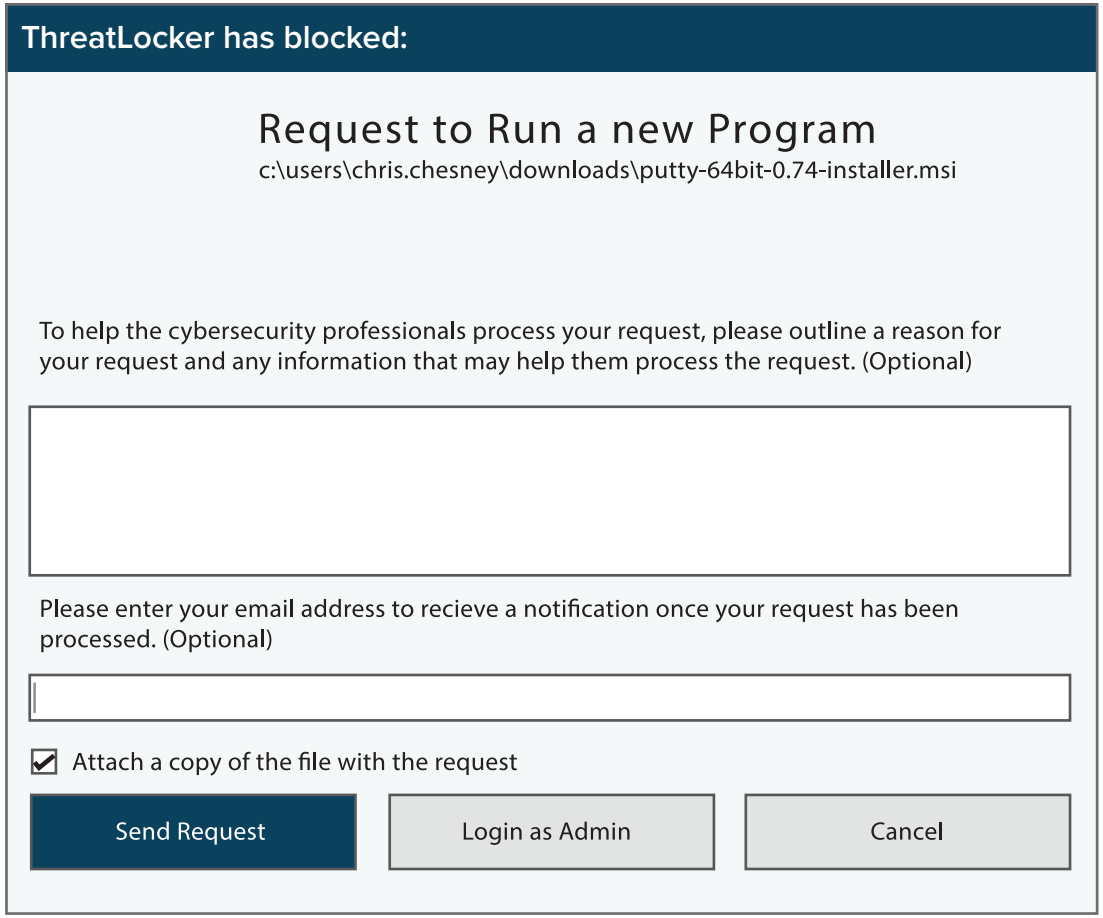


Allowlisting:
Using the ThreatLocker® solution, you can deny any application from running on your device that is not a part of the Allowlist. This helps to mitigate and stop cyberattacks from happening on your devices or across your network.

Firewall-like Application Policies:
A powerful firewall-like policy engine that allows you to permit, deny or restrict application access at a granular level.

Time-Based Policies:
Permit access to applications for a specified amount of time. Automatically block the application after the policy has expired.

Built-In Applications:
ThreatLocker® automatically adds new hashes when application and system updates are released, allowing your applications to update without interference while preventing updates from being blocked.

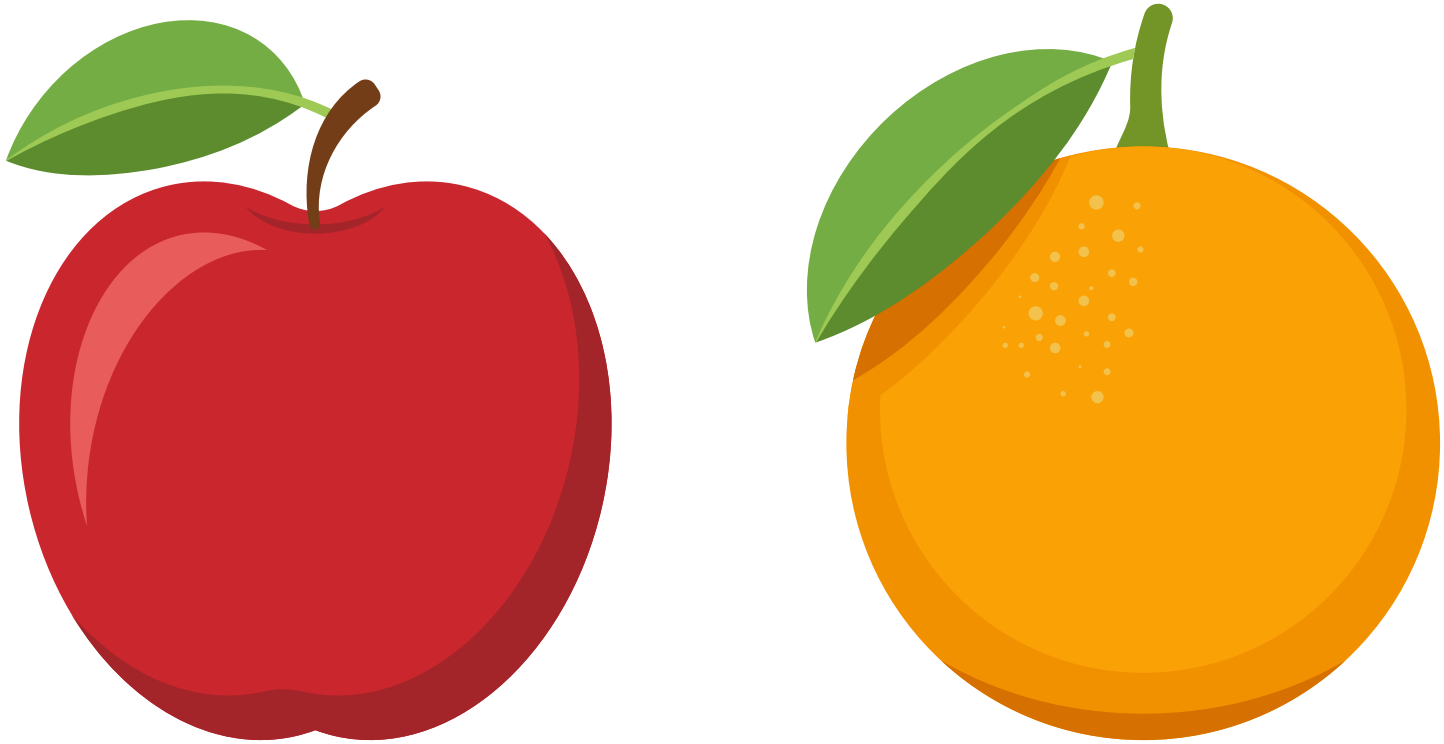


The approval center allows you to easily control what is permitted to run on your computer with a 30-second single click approval.

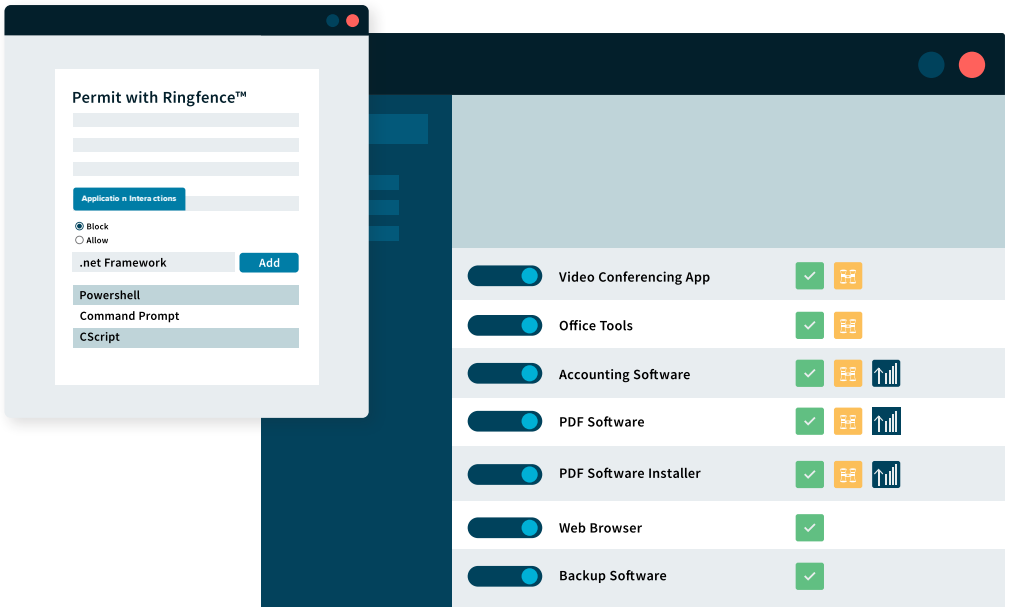
Users have the ability to request permission or ignore notifications for unapproved applications.

ThreatLocker® vs. Alternative Whitelisting Solutions

Whitelisting blocks all untrusted applications, however, it will not stop an attacker from weaponizing tools and applications against you. ThreatLocker's proprietary Ringfencing™ solution goes beyond blocking untrusted applications. Continue reading to learn more.



What is **Ringfencing™?**



Ringfencing™ controls what applications are able to do once they are running. By limiting what software can do, ThreatLocker® can reduce the likelihood of an exploit being successful or an attacker weaponizing legitimate tools such as PowerShell.

Ringfencing™ allows you to control how applications can interact with other applications. For example, while both Microsoft Word and PowerShell may be permitted, Ringfencing™ will stop Microsoft Word from being able to call PowerShell, thus preventing an attempted exploit of a vulnerability such as the Follina vulnerability from being successful.

Under normal operations, all applications permitted on an endpoint or server are able to access all data that the operating user can access. This means if the application is compromised, the attacker can use the application to steal or encrypt files. Ringfencing™ allows you to remove file access permissions for applications that do not need access and even remove network or registry permissions.

When you first deploy Ringfencing™, your device will automatically be aligned with the default ThreatLocker® policies. These policies are then automatically applied to a list of known applications such as Microsoft Office, PowerShell, or Zoom. The aim of the default policies is to provide a baseline level of protection for all endpoints. Each of these policies can easily be manipulated to fit any environment at any time. Our team of dedicated Cyber Heroes are always on hand to support any requests, 24/7/365.

Mitigate Against Fileless Malware:

Stop fileless malware by limiting what applications are allowed to do.

Granular Application Policies:

Stop applications from interacting with other applications, network resources, registry keys, files, and more.

Limit Application Attacks:

Limit application attacks like application hopping by limiting what applications can access.

Limit to Your Files:

The average computer has over 500 applications, and only a handful of those need to access your files. With Ringfencing™, you can choose which applications need to see which files.

Vulnerable Applications are the #1 Cause of Security Breaches

*Verizon Data Breach Investigation Report, 2020

Attacks against web applications are now the fastest-growing category. At ThreatLocker®, protecting your applications from ransomware and other malicious threats is one of our top security concerns.

What is **Storage Control?**

Storage Control provides policy-driven control over storage devices, whether the storage device is a local folder, a network share, or external storage such as a USB drive. ThreatLocker® Storage Control allows granular policies to be set, which could be as simple as blocking USB drives, or as detailed as blocking access to your backup share, except when accessed by your backup application.

Unified Audit provides a central log of all storage access by users on the network and those working remotely, right down to the files that were copied and the serial number of the device.

When a storage device is blocked, a user can be presented with a pop-up where they can request access to a storage device. The administrator can then choose to permit the storage device in as little as 60 seconds.

Audit Access to Files:

A full detailed audit of all file access on USB, Network, and Local Hard Drives is centrally accessible within minutes of a file being opened.

Granular Storage Policies:

Users can request permission to elevate applications and attach files and notes to support their requests.

Simple Requests for Access:

A pop-up with the option to request access to the storage device

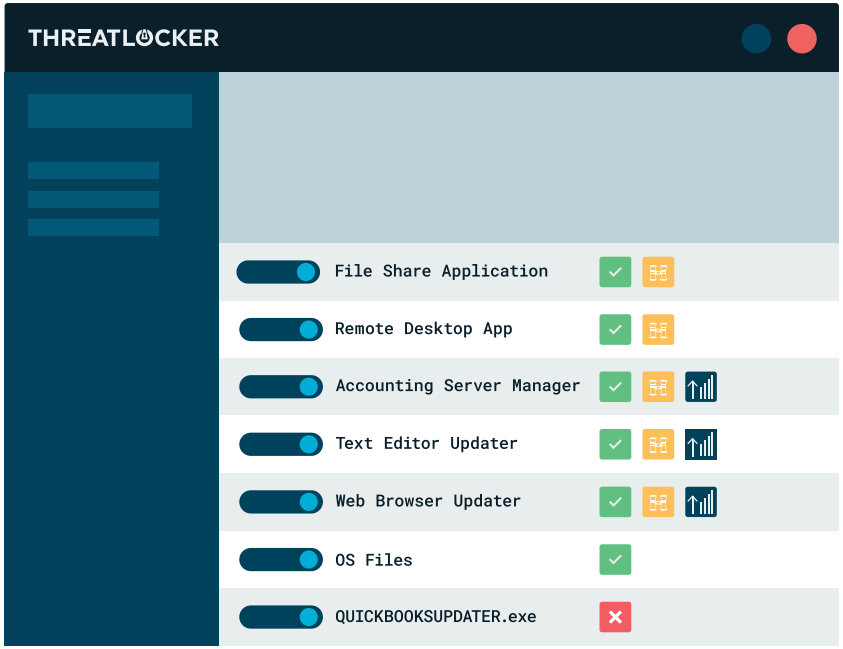
Simple USB Blocking:

USB Policies allow access based on device serial number, vendor, and/ or file type.

What is **Elevation Control?**

Elevation Control enables users to run specific applications as a local administrator, even when they do not have local admin privileges. Elevation Control puts IT administrators in the driving seat, enabling them to control exactly what applications can run as a local admin without giving users local admin rights.

When ThreatLocker® is first deployed, all existing applications are learned. Administrators can review the applications and select which can be run as a local administrator. Once enabled, a user can run the software as a local administrator without entering any credentials.

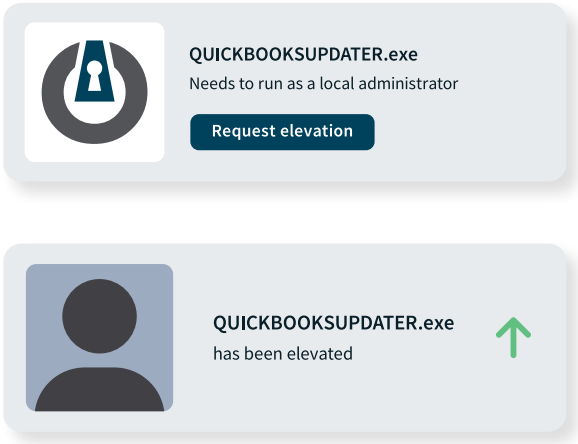


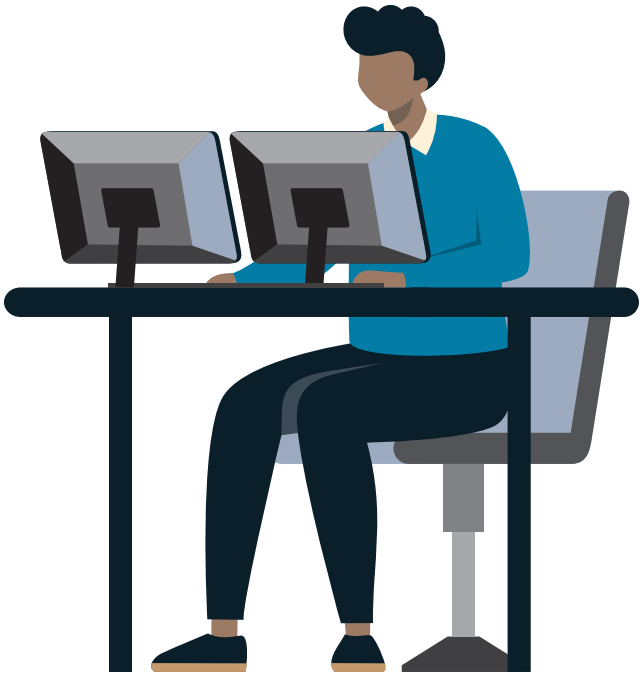
Complete Visibility of Administrative Rights:
Gives you the ability to approve or deny an individual's access to specific applications within an organization even if the user is not a local administrator.

Streamlined Permission Requests:
Users can request permission to elevate applications and attach files and notes to support their requests.

Varied Levels of Elevation:
Enables you to set durations for how long users are allowed access to specific applications by granting either temporary or permanent access.

Secure Application Integration:
Ringfencing™, ensures that once applications are elevated, users cannot jump to infiltrate connected applications within the network.





What is
Network Access Control?

ThreatLocker® NAC is an endpoint and server firewall that enables you to have total control over network traffic, which ultimately helps you to protect your devices. Using custom-built policies, you can allow granular access based on IP address, specific keywords, or even agent authentication or dynamic ACLs.

The local network is no more. Users are not only working from the office but also remotely, meaning that the network we all utilize has quickly become the internet. This dissolution of the perimeter leaves devices and data vulnerable and exposed to cyber threats. This is why you need controls on network traffic in place to protect your device and, by extension, your data. You can achieve this by implementing a Network Access Control solution (NAC).

Dynamic ACLs allow you to automatically open ports based on a computer's or group of computers' location at a point in time. With dynamic ACLs, the connection between server and client is direct, unlike a VPN that needs to connect through a central point.

Configurable:
NAC gives users the ability to configure network access to endpoints using global and granular policies.

Cloud-Based:
The cloud-managed solution provides customers with a centralized view of endpoint policies and network traffic across your organization.

Dynamic:
NAC enables users to deny all traffic to published servers while only allowing a single IP address dynamically or even a keyword. This is great for a user who is traveling often.

Enhanced Network Security:
Ensure rogue devices on your network cannot access your servers or endpoints with Dynamic ACLs.

[Company Name]
Your Trusted IT Provider

At [Company Name], we understand that as technology evolves, so do opportunities to evolve your business. In order to ensure your business evolves and thrives in today's world, we are always a few steps ahead, making security recommendations to fit your needs and mitigate the latest cyber threats. You can rest easy when you put your IT support needs in our hands.

THREATLOCKER®

companywebsite.com

phone #

e-mail address