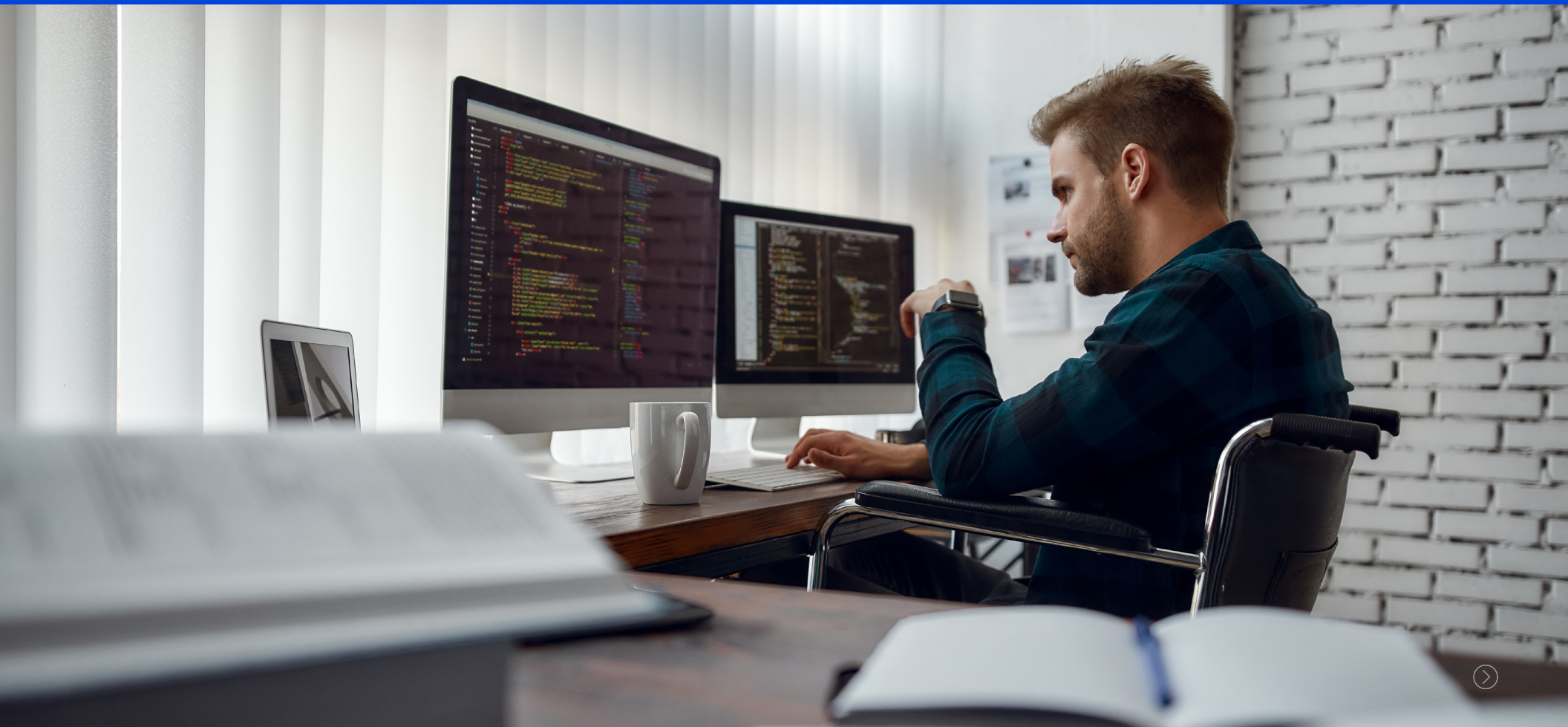
The Big Book of ZTNA Security Use Cases

citrix

Know Your ZTNA Protection Index

April 2022 Edition



Foreword

Threat actors are crafty. Hiding in the shadows, they deviously find ways to exploit the weakest cyber links in any organization. In today's world where a distributed workforce accesses many applications from multiple devices, finding weak links is just getting easier for threat actors.

This guide highlights 20 realistic cybersecurity scenarios, some that you will relate to and others that you might not have considered. It is written in such a way that everyone will be able to understand what is at risk, as well as the value Zero Trust Network Access (ZTNA) brings. The scenarios have been broken into two categories based on how zero trust should be implemented – 'Adaptive Access' and 'Data Loss Prevention and Threat Protection'.

Once you're done reviewing all the scenarios, don't forget to calculate your overall 'Zero Trust Protection Index'. For every scenario, we have listed zero trust functionality you should add to your cybersecurity roadmap in case you are currently unprotected. This is the first step to understanding your risk exposure and should be followed up by a more detailed discussion on how to get protected. This book will also teach you how Citrix Secure Private Access (SPA), a ZTNA solution, can help improve your security posture.

Pankaj Gupta
Citrix

Table of Contents

Adaptive & Contextual Access Use Cases

Least Privilege Access Based on Specific User Needs 5
Location-Aware Adaptive Authentication with MFA 6
Application Authorization Based on User Location and Device 7
Least Privilege Access Based on Dynamic User Risk Score 8
Enforce Active Endpoint Protection Before Granting Application Access 9
Enforce Latest Anti-Virus Software Version and Definitions Before Granting Access 10
Block Against Phishing Attacks 11
Enforce Data Backups to Protect from Ransomware 12
Faster Completion of M&As 13
Constant Monitoring & User Risk Score 14

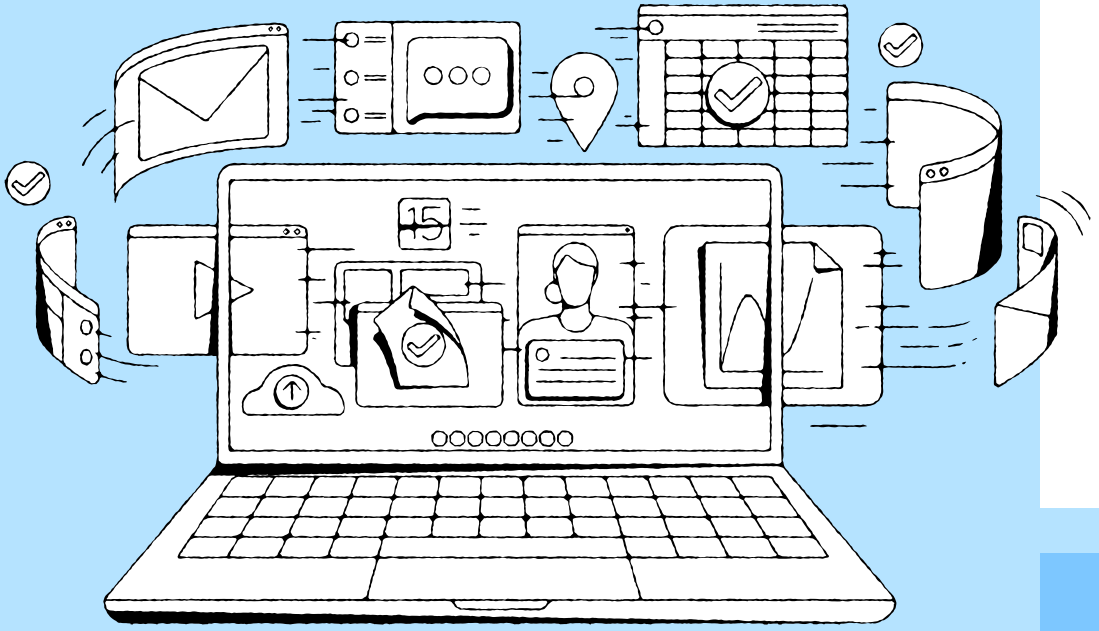
Data Loss & Threat Prevention Use Cases

Protection from Key Loggers 16
Mitigate Threats Targeting Outdated Operating Systems 17
Prevent Data Loss from Careless Screen Sharing 18
Prevent Data Loss with Remote Browser Isolation 19
Enable Secure BYOD and Prevent Malware Transfer with Remote Browser Isolation 20
Deter Data Theft for PCI Compliance 21
Protection from Screen Scraping Malware 22
Protect Against Fake Anti-Virus Software 23
Protect Users and Data with Secure Mobile Browsers 24
Manage Device Safety with Patch & Endpoint Management 25

Your Zero Trust Protection Index 26

Adaptive & Contextual Access

Least privilege application access must be given based on “context” – deep intelligence about the user, device and their risk profile. Application access levels must change dynamically as context changes. This section highlights different forms of context that should be evaluated for zero trust access.



Least Privilege Access Based on Specific User Needs

Scenario:

Hercules Athletics LLC hires a supply chain expert, a contractor from Singapore, to assist with an urgent issue. She uses her personal laptop, an unmanaged device, and will need access to only one specific internal application.

What is at risk:

Contractors and temporary workers are usually given access in full or no access at all to internal applications. If given full access, the contractor can view sensitive pricing information across multiple suppliers and accidental or intentional leak of this info could have major consequences on the company. And if they are denied access, they are far less effective at doing the job they were hired for.

How Citrix ZTNA Protects:

Policies and controls can be configured to provide access on a per application basis, without sacrificing security based on the user's identity and authorization levels, by Citrix Secure Private Access (SPA). These policies can apply to any individual or specific type of group, for example, contractors.

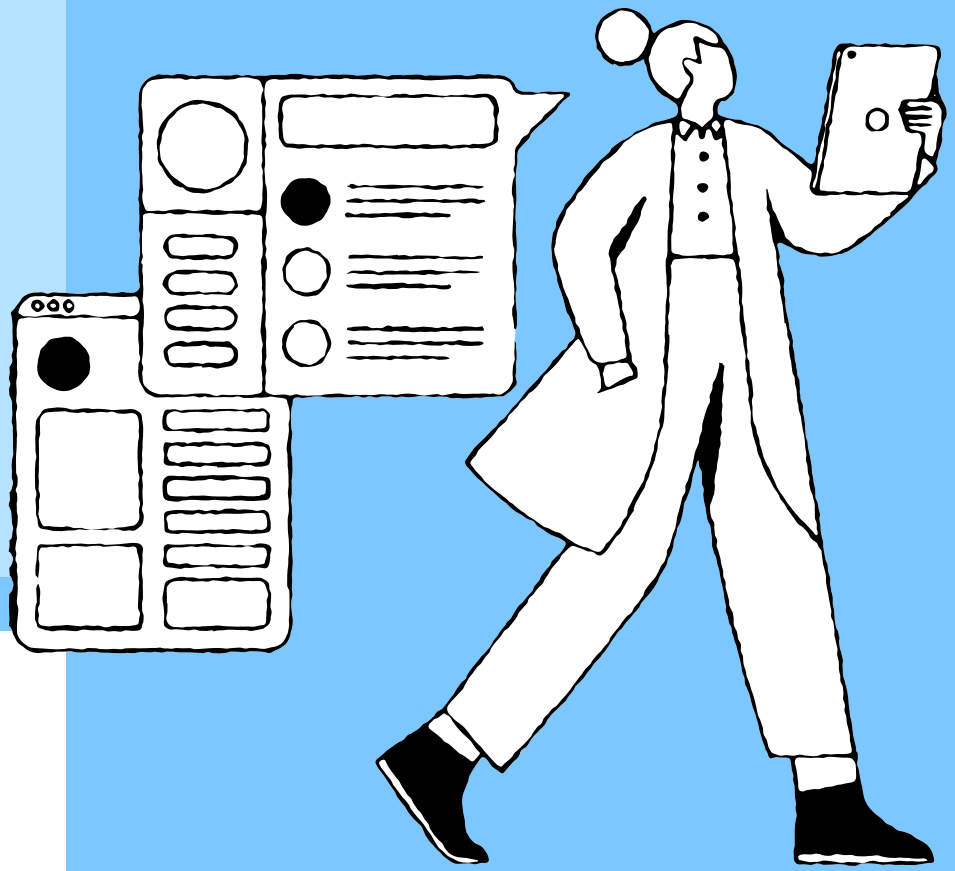
Location-Aware Adaptive Authentication with MFA

Scenario:

Ebeneezer Scrooge, located in Texas, works in Logistics and Operations and uses the same password for all personal and corporate apps. His personal email account is hacked, and his password is compromised. Before he changes his passwords, someone located outside the country attempts to access the company's expense & invoice management application with the intention of wiring themselves a small recurring payment of $75 per month to avoid detection.

What is at risk:

Reused passwords and user error make it easy for hackers to access sensitive data.



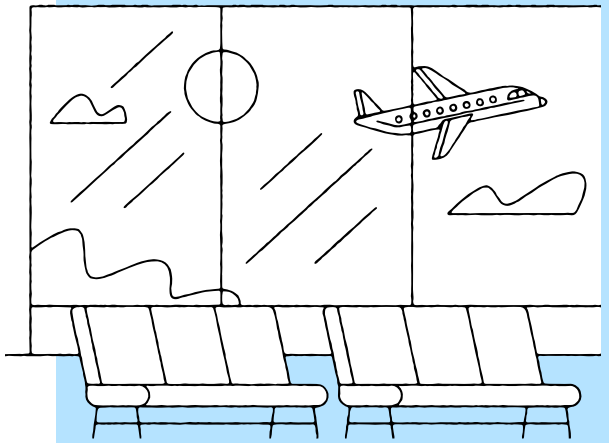
How Citrix ZTNA Protects:

Citrix's ZTNA solution detects an unfamiliar location and suspects an unauthorized user. The attempt is automatically challenged using Multi-Factor Authentication, blocking the bad actors' unauthorized access to the company's assets. Citrix offers Adaptive Authentication out of the box, allowing adaptive policies to determine dynamic login, without using a third-party solution for dynamic login. This means a more simple and seamless solution for the customer.

Application Authorization Based on User Location and Device

Scenario:

Zorro works in sales for a US based company and travels internationally on a regular basis. After completing a deal abroad, Zorro decides to extend his trip to visit his fiancé working as a nurse for a non-profit organization in a high-risk embargoed country. While visiting his fiancé, he tries to access internal applications for work while using his fiancé's iPad. He has authorization to access this information, but he is using an unmanaged device while in a country where his company restricts access.



What is at risk:

The United States has an embargo against this country, and his company takes precautions to comply with those restrictions. His company believes that embargoed countries offer greater cyber security risks. Zorro has access to pricing information across multiple suppliers and accidental or intentional leak of this info could have major consequences on the company.

How Citrix ZTNA Protects:

Adaptive authentication policies within Citrix Secure Private Access (SPA) ensure the right people get the right level of access, using real time context when application access is requested. The company's policy states that when in high-risk countries, access will only be granted when using a corporate device for a very limited set of applications. Since Adaptive Authentication finds that Zorro is using an unmanaged device in an embargoed country, his access is denied, protecting the company's data, employees, and customers.

Least Privilege Access Based on Dynamic User Risk Score

Scenario:

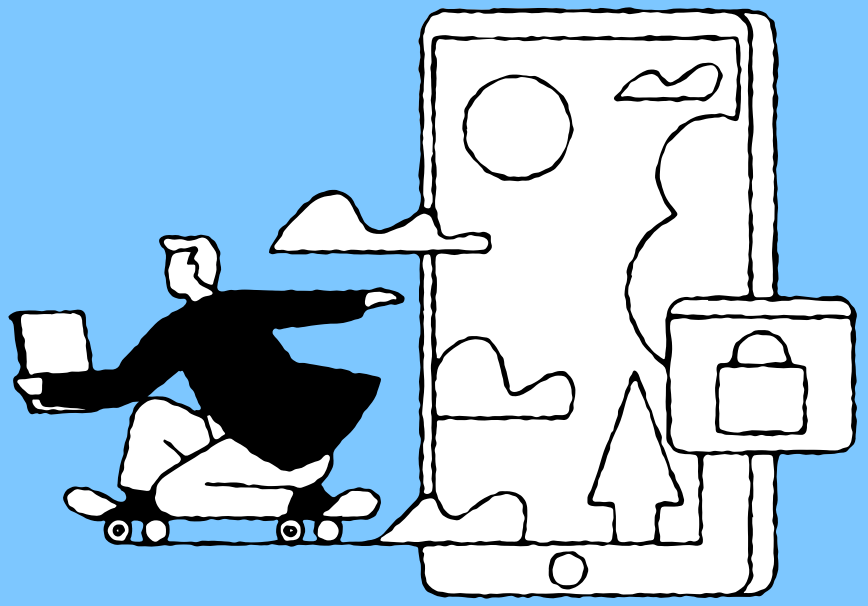
Dracula works for Blood Work Inc. His company has adopted the work-from-home model and Dracula uses a BYO device from his home in Oregon. To get his work done, he needs to access sensitive apps on a daily basis. The next morning, there is an attempted login from Transylvania with Dracula's credentials, 12 hours since his previous login.

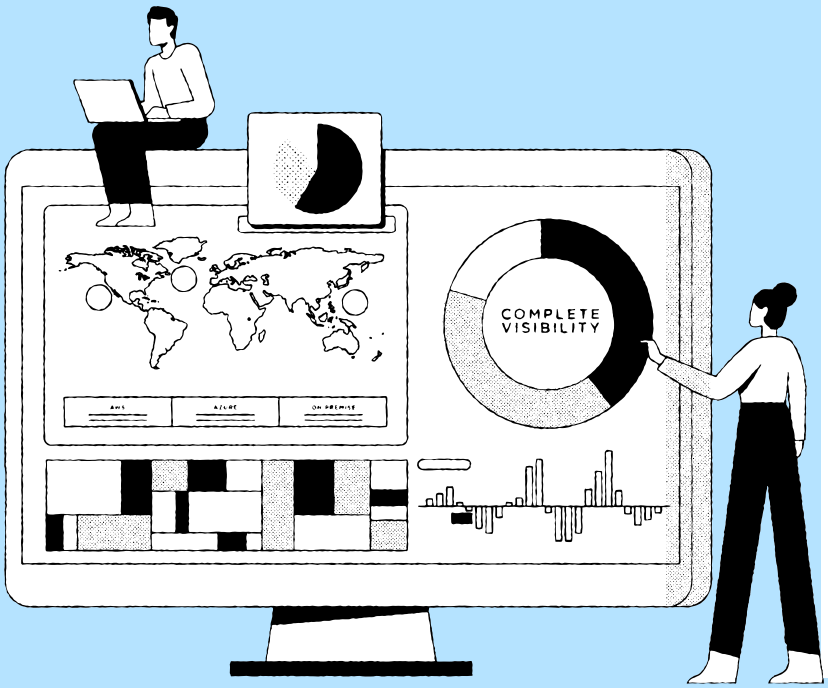
What is at risk:

Dracula has access to employee personal identifiable information (PII) such as social security numbers, dates of birth, and home addresses. Dracula's login from Transylvania could be because Dracula is vacationing there or it could be a bad actor using a Transylvania IP address for a malicious login. If it is a bad actor, they may gain access to all employee PII, threatening employee trust, and spiraling the company into legal challenges.

How Citrix ZTNA Protects:

With Citrix, Dracula's User Risk Score will automatically increase when a login happens from an unfamiliar location. This increase will push the score past what is deemed acceptable, requiring Multi-Factor Authentication (MFA). This will verify that it is Dracula logging in, preventing bad actors since they will fail the MFA challenge. Citrix Secure Private Access (SPA) has a differentiated capability being able do all this without requiring the additional purchase of 3rd party End Point Detection and Response (EDR) software.





Enforce Active Endpoint Protection Before Granting Application Access

Scenario:

Cinderella is a new employee for NextGen Virus Research Inc hired to research a life-threatening infection based on analyses of real patient data. Her company allows BYOD but enforces cybersecurity through a powerful endpoint protection platform (EPP) installed on the laptop. This software offers malware protection, enforces endpoint data loss prevention software (DLP), offers device analytics etc. However, in Cinderella's case, the software did not download correctly. In the rush to get started on her new job, she ignores the incomplete software install alerts and does not inform anyone.

What is at risk:

Since Cinderella's laptop is unprotected, she is vulnerable to threats. As Cinderella continues to access work and recreational apps from her laptop, she unknowingly puts NextGen Virus Research Inc at risk and it's only a matter of time before malware is downloaded on her laptop. This malware can exfiltrate patient data, encrypt the device for ransom, and laterally move to other apps and employee devices she collaborates with.

How Citrix ZTNA Protects:

With Citrix Secure Private Access (SPA), NextGen Virus Research Inc can monitor Cinderella's device in real time to ensure that it is protected with the latest version of her endpoint protection service. Citrix can do this on a per app basis, ensuring that highly sensitive apps are only accessed by users with secure endpoint devices.

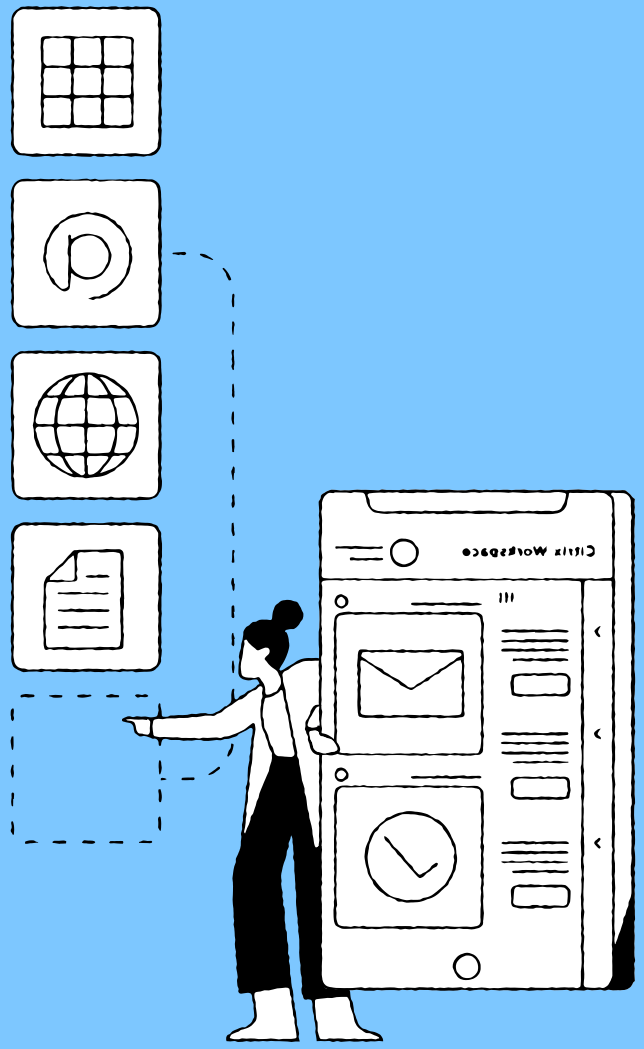
Enforce Latest Anti-Virus Software Version and Definitions Before Granting Access

Scenario:

Long John Silver works for a British ship making company and uses a corporate-managed device. His company mandates anti-virus software on the device as part of their multi-layered security architecture. However, he has inadvertently turned off his anti-virus updates.

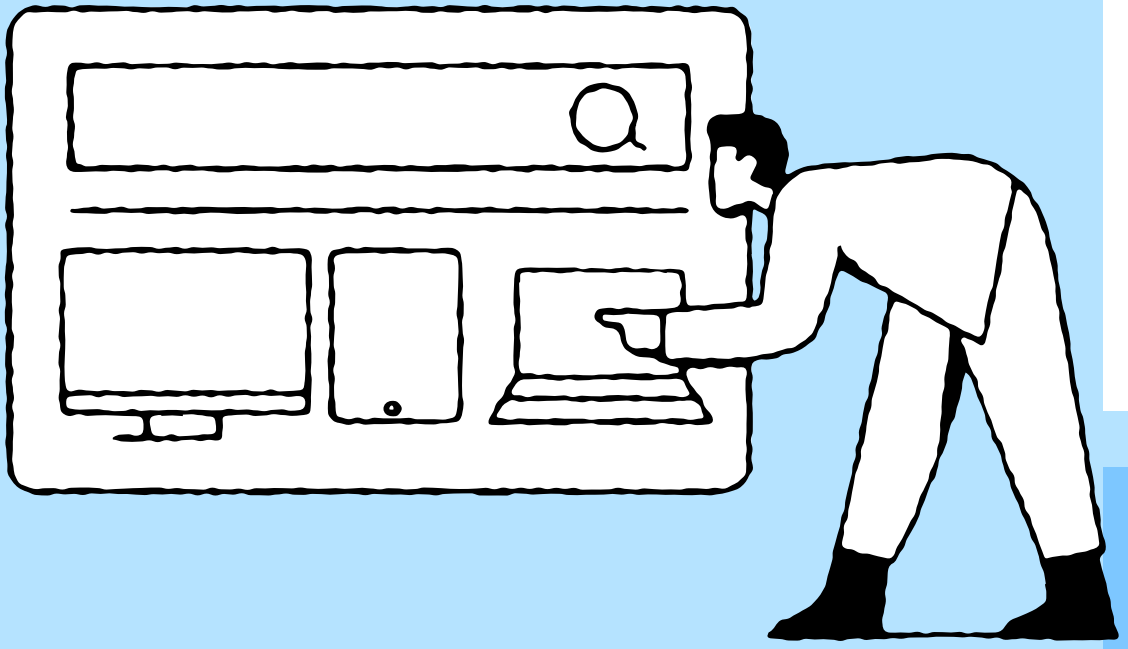
What is at risk:

Since Long John does not have the latest anti-virus version, his device is vulnerable to zero-day threats when he is working remotely from home and not behind the company firewall. This weakens his company's security architecture, creating cybersecurity risk.



How Citrix ZTNA Protects:

Citrix Secure Private Access (SPA) can monitor every device's anti-virus version and if his device does not meet version requirements set up by his IT admins, he will be denied access. Citrix Secure Private Access (SPA) can also create policies around granular checks, such as requiring an anti-virus scan take place in the last 30 days.



Block Against Phishing Attacks

Scenario:

King Arthur has been appointed CISO of Round Table Design & Construction Corp, a globally-acclaimed architecture firm. 70% of the employees are consultants that regularly access sensitive client information – from hotels, airports, client offices and their homes. They travel a lot, have long workdays, and due to this, may let their 'cyber privacy' guard down.

What is at risk:

Arthur knows that phishing is one of the most common tactics used by cybercriminals. One breach could cost him his job, and his organization all their clients.

How Citrix ZTNA Protects:

Citrix's detailed endpoint analysis of employee laptops ensures that anti-phishing software is enabled, authentic, and of the latest version. MFA then validates the identity of the user. Full, partial, controlled, or no access is granted based on the results of the identity and endpoint checks.

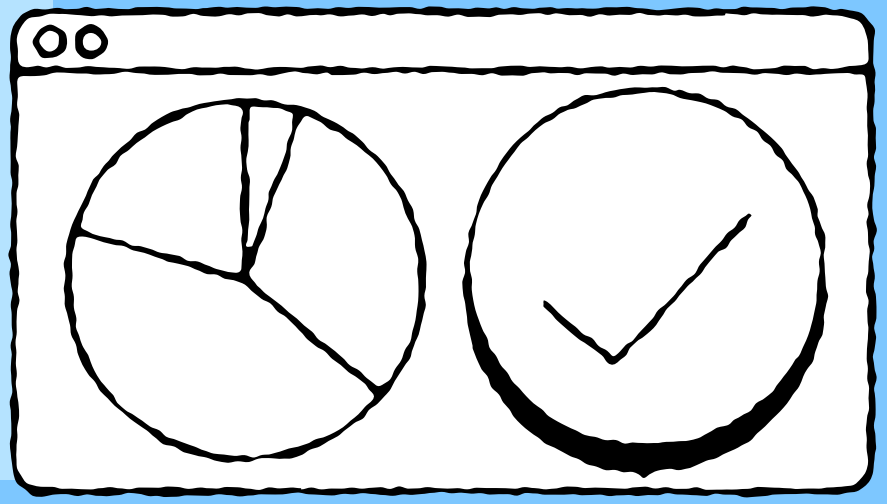
Enforce Data Backups to Protect from Ransomware

Scenario:

Sindbad is a young and ambitious Petroleum Geologist for World Oil Co. Sindbad is currently on his seventh voyage in the Mediterranean Sea and has just discovered significant oil deposits, location details of which are on his laptop. Engrossed in finding new oil deposits, Sindbad has forgotten to backabout backing up his work. The data backup client on his laptop is old, so it does not automatically upload Sindbad's files to a secure cloud.

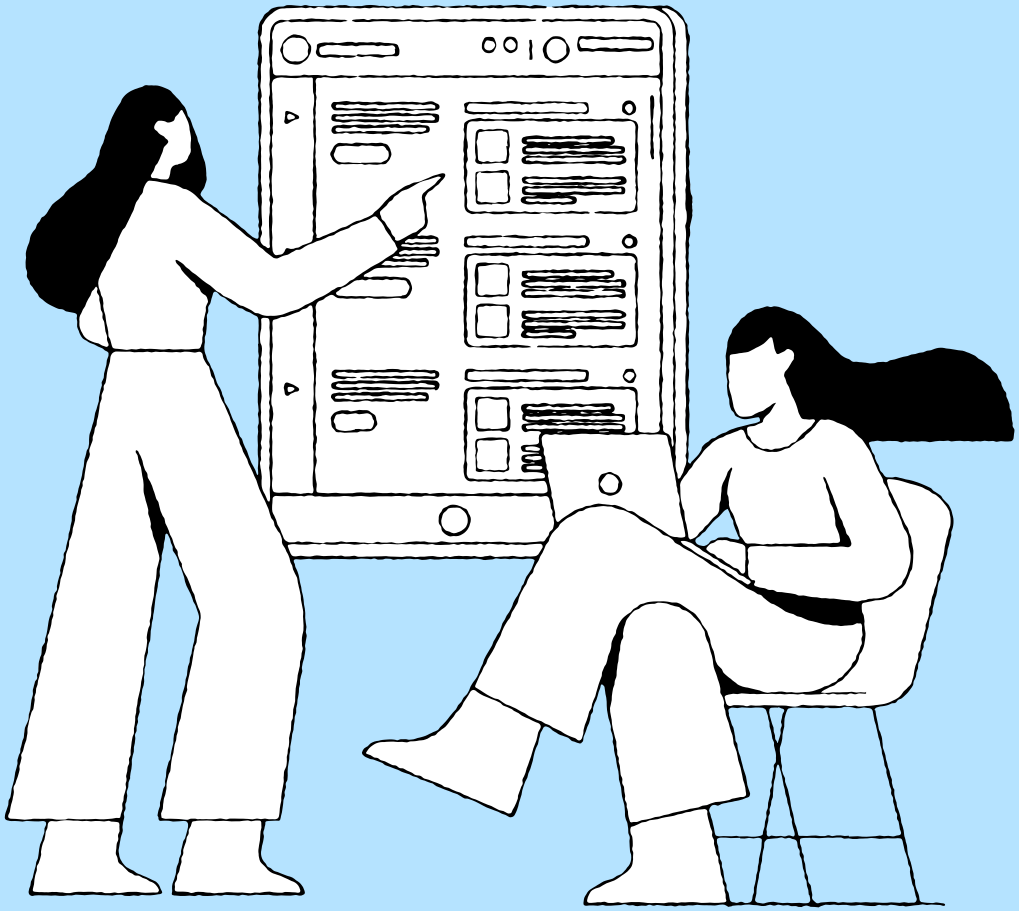
What is at risk:

If Sindbad's laptop, which is usually never behind a firewall, is attacked by ransomware, hackers will encrypt the lucrative information and perhaps may even sell it to competitors or on the dark web. This can result in millions of dollars of ransomware payments and lost revenue for World Oil Co.



How Citrix ZTNA Protects:

All endpoint devices, especially high-risk endpoints, should have a data backup service. With Citrix's ZTNA solution, IT admins can ensure that an authentic and updated backup service is installed on endpoint devices so the impact of ransomware and other malware is reduced.



Faster Completion of M&As

Scenario:

Zeus Lightning Co., the biggest home lighting manufacturer, just acquired Thor Thunder Inc., the biggest sound system company. Now, salespeople from both companies need access to each other's CRM and BI applications to drive revenue growth for the company's shareholders.

What is at risk:

Integrating a new company after M&As takes time, delaying return on investment, impacting employee morale, and impacting stock price. A rush job, however, could expose the newly merged company to data breaches or cause app performance related challenges.

How Citrix ZTNA Protects:

With Citrix Secure Private Access (SPA), an agent is pushed to the employees' laptops. This gives them application-level zero trust access to internal applications within hours, without any noticeable added application latency.

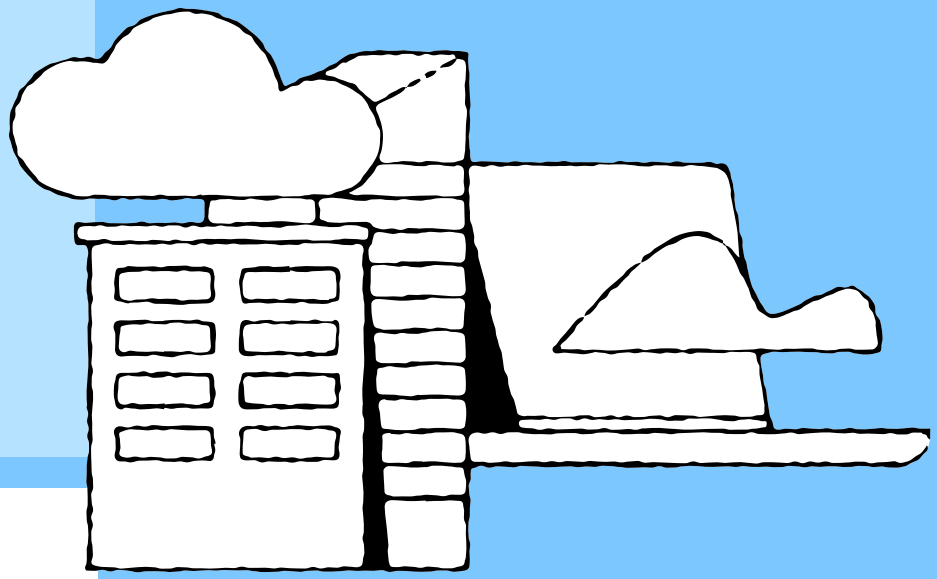
Constant Monitoring & User Risk Score

Scenario:

Lucifer works for a major defense contractor. He works on a corporate device designing next-gen military aircraft. However, Lucifer learns that he will be let go in an upcoming wave of layoffs. Disgruntled, he decides to download as many aircraft designs and blueprints as he can before he leaves. He intends to use them to help his chances as he approaches competitors for a new role.

What is at risk:

If Lucifer can take all the stolen files with him, he will create significant legal challenges for himself, his current, and future employers. This type of information is extremely sensitive, and simply allowing it to be taken will be seen as a failure on Lucifer's former employer.

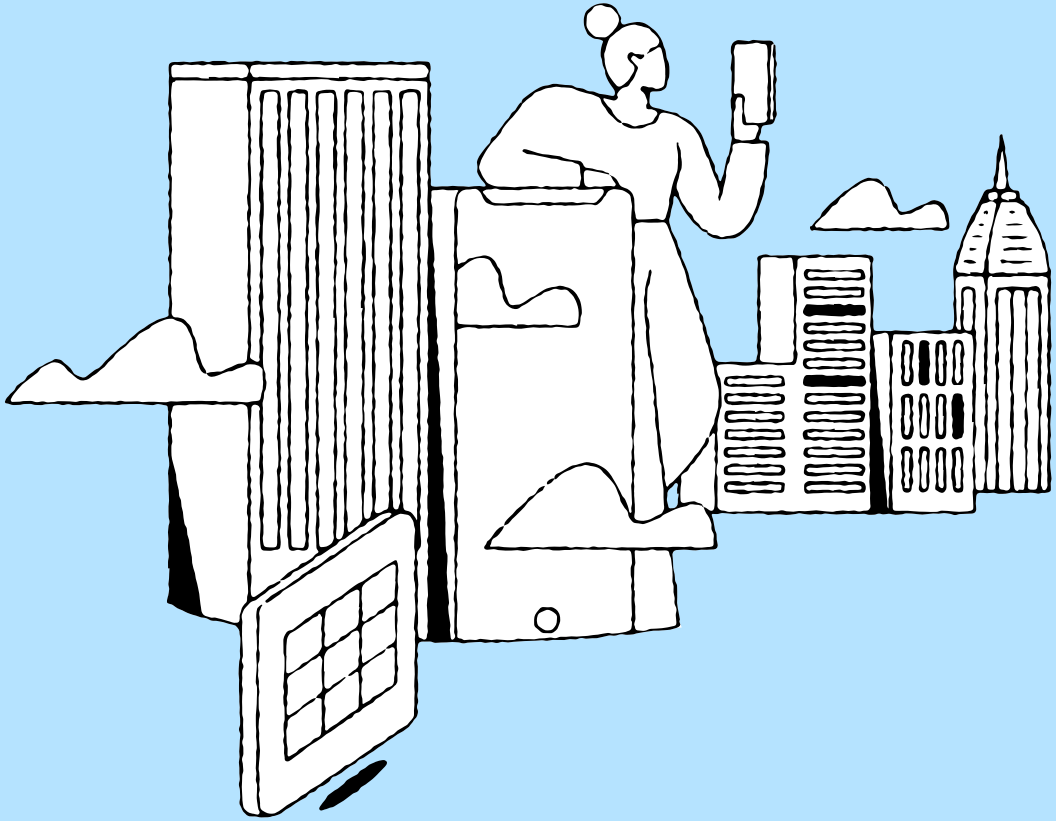


How Citrix ZTNA Protects:

With Citrix Secure Private Access (SPA), all employees, including Lucifer, can be given watermarked access to sensitive data, creating a deterrence for theft. Also, Citrix Secure Private Access (SPA) collects data throughout the user's session. If Lucifer downloads irregular amounts of data, Citrix will raise his user risk score. This will trigger an alert and an automated block of any downloads by Lucifer.

Data Loss & Threat Prevention

Adaptive, least-privilege access, as discussed in the previous section, is essential. However, for most organizations this is not enough. This section highlights scenarios where additional protections to block threats and data loss are critical to stop a breach.



Protection from Key Loggers

Scenario:

Dr. Jekyll is an executive for Medicine Corp. He is in a hotel in New York, traveling for business. He streams a movie online via an unfamiliar website on his corporate computer. Little does he know, while trying to stream the movie, he was tricked into downloading a keylogger which will record everything he types.

What is at risk:

The next time Dr. Jekyll logs in, the key logger will record all his credentials, which are then delivered to the bad actor. With the stolen credentials, bad actors can steal his identity as well as sensitive trade secrets.

How Citrix ZTNA Protects:

Medicine Corp's IT Administrators have enabled key logger protection for all employees with access to sensitive corporate information. Only Citrix's ZTNA solution can do this. All characters typed are scrambled and nothing is revealed to the bad actors.

Mitigate Threats Targeting Outdated Operating Systems

Scenario:

Mr. Hyde uses a personal laptop to access an order processing internal app. His laptop is running an outdated Windows OS version that is already past its End-of-Life (EOL).

What is at risk:

An outdated OS is one of the key risks for any organization. When a new OS is released, its vendor often announces End-of-Support or End-of-Life for their much older products. This leaves old operating systems with unpatched security vulnerabilities, making it easy for bad actors to launch cyber-attacks. The burden is placed on the user, and unless they update their personal devices, bad actors can wreak havoc using attacks that would be protected against with OS updates. The 2017 WannaCry outbreak impacted over 160,000 outdated Windows users. Because Mr. Hyde has not updated his OS version, he is left vulnerable to attacks and data is exposed. Many times, once a device is infected with malware, it can propagate laterally from one device to another.

How Citrix ZTNA Protects:

Citrix Secure Private Access (SPA) automatically identifies which OS every device is running. Policies can be put in place that determine the minimum acceptable software and its version. That way, if a device does not meet these requirements, it will have its access restricted, or even fully denied. This protects the application and the rest of the company's network from bad actors exploiting unpatched vulnerabilities of an outdated OS.

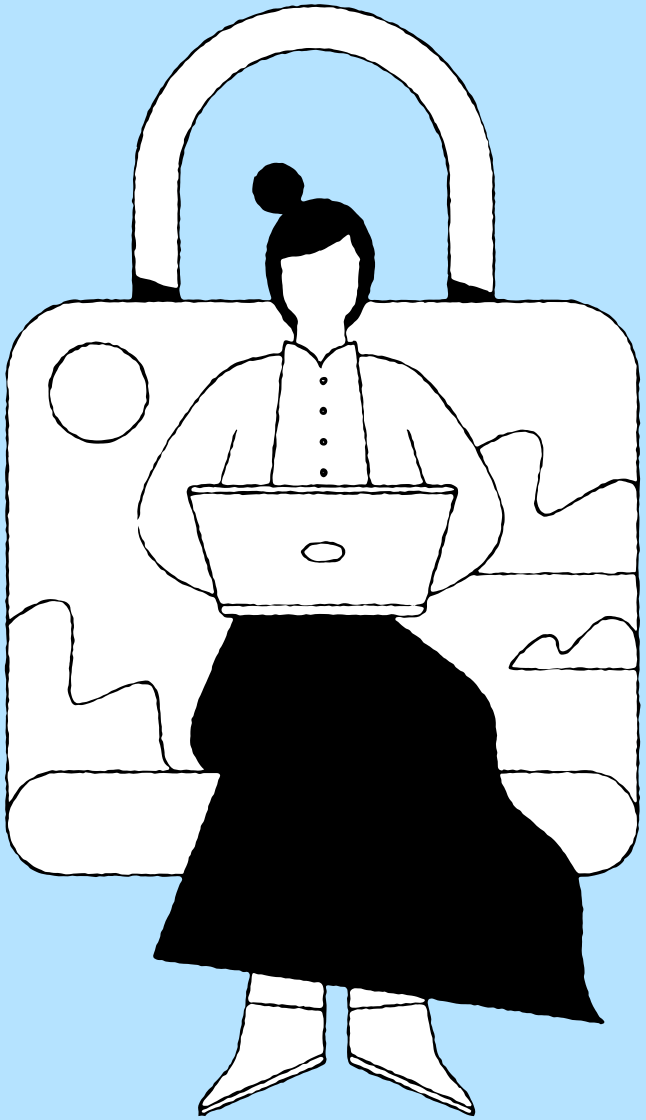
Prevent Data Loss from Careless Screen Sharing

Scenario:

Robin Hood is working on a large deal and is urgently trying to get approved pricing before his customer presentation. He receives the approved pricing sheet containing all discount information. Shortly after, he begins the customer presentation in an online meeting. However, he does not close out of the pricing sheet while presenting his desktop to the customer.

What is at risk:

Robin is afraid the customer saw the discount sheet. If he revealed the margins they are selling, it could ruin the deal and cause serious issues.



How Citrix ZTNA Protects:

Since Robin is protected by Citrix's ZTNA solution, Citrix automatically blacks out the application containing the pricing information while Robin is screen sharing, for other participants on the call. Only Citrix's ZTNA solution can do this. His company has set up the policy to block this application for all sales coded employees while they are screen sharing.

Prevent Data Loss with Remote Browser Isolation

Scenario:

Aladdin works in finance and regularly accesses key information that is regulated by the SEC using his personal laptop. This is an unmanaged device, and he regularly works in the office using their secure Wi-Fi. While driving home from work, he stops at a restaurant to grab some food to-go. When he comes back to his car, his window has been broken and his work bag has been stolen. Aladdin's company requires frequent password resetting, and sadly, there is a notebook containing his current laptop password in the bag as well.

What is at risk:

Once the thief unlocks the laptop, he will have access to all files downloaded on the hard drive, including confidential information.

How Citrix ZTNA Protects:

Aladdin's IT Administrators require Finance employees to use remote browser isolation when accessing any app with sensitive information. While using an Isolated Browser through Secure Private Access (SPA), downloading and screen captures are all blocked. As a result, no data resides on the laptop. This ensures sensitive information can not be revealed.

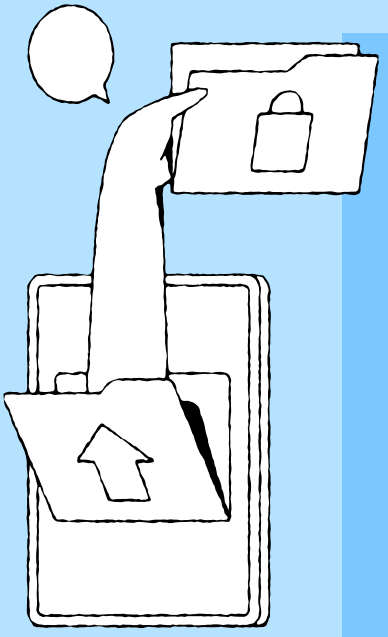
Enable Secure BYOD and Prevent Malware Transfer with Remote Browser Isolation

Scenario:

Rapunzel is preparing the company balance sheet for the annual shareholder review. While heading home she receives a call from the CEO, telling her she needs to access their corporate managed finance web app once again in order to make some final changes. She uses her personal laptop, an unmanaged device. Unknown to Rapunzel, her device was recently infected with malware while she was shopping online.

What is at risk:

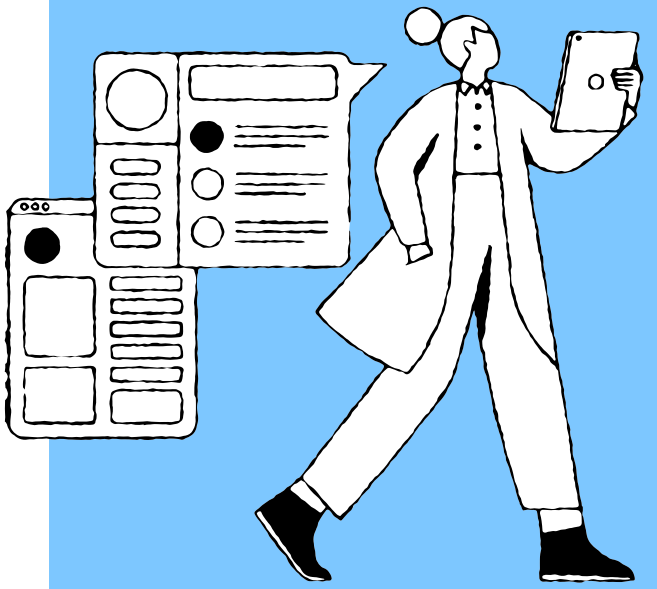
When accessing a sensitive web app through an unprotected native browser on a potentially insecure personal device, even via VPN or basic ZTNA solutions, malware can move from Rapunzel's device to the company's network and financial application. This puts company data, customers, reputation, and revenue at risk. For instance, in this case, financial data can be leaked before the shareholder review, affecting the stock price of the company, damaging shareholder and customer trust, and creating legal compliance liabilities for the company.



How Citrix ZTNA Protects:

Citrix Secure Private Access (SPA) includes remote browser isolation (RBI) functionality. This prevents malware from reaching the corporate network, as well as lateral movement of malware from a native browser or device to the rest of the network and applications. IT Administrators can ensure that any unmanaged device accessing sensitive applications, such as financial applications, will need to use RBI. With RBI, Rapunzel's browsing experience is isolated from the actual application – her personal laptop does not directly transfer any browsing data to or from the financial application. Instead, she only receives screen updates on her device. This creates a win-win situation. Rapunzel can still use the application just as if it's a native browser and her company remains safe because the malware from her device cannot make it to company's sensitive applications. IT Administrators can also enable functions like disabling screen captures, copy/paste, and downloading, in addition to URL filtering and session monitoring.

Deter Data Theft for PCI Compliance



Scenario:

Poseidon Watercraft has recently hired an offshore support firm to help with customer service. Customer support reps deal with issues such as handling returns and helping customers order products over the phone, by accessing to credit card information. However, Poseidon Watercraft is concerned about meeting PCI Compliance requirements, fearing that credit card information may be at risk by sharing it with offshore contractors.

What is at risk:

Monitoring and managing offshore contractor behavior can be complex, leading to loss of customer payment data to cybercrime. Poor enforcement of PCI requirements can lead to legal challenges and brand damage.

How Citrix ZTNA Protects:

With Citrix Secure Private Access (SPA), Poseidon Watercraft can create rules that impede the misuse of cardholder information, increasing traceability by law enforcement if information is stolen. Employees of the offshore support firms will have their screens watermarked with a user ID and IP address, holding the user accountable for any information leaked, as well as preventing keyloggers, disabling copy/paste, printing, screen captures, and downloads. Citrix's ZTNA solution allows Poseidon Watercraft to gain the benefit of offshore assistance, without putting themselves and their customers' data at risk.

Citrix Secure Private Access (SPA) helps meet the following PCI requirements – Requirement 4: Encrypt transmission of cardholder data across open, public networks, Requirement 8: Identify and authenticate access to system components, Requirement 10: Track and monitor all access to network resources and cardholder data, and Requirement 12: Maintain a policy that addresses information security for all personnel.

Protection from Screen Scraping Malware

Scenario:

Elon works at Smart Vehicle Inc. as an R&D engineer. He was hired during the pandemic, so he works from home using his personal laptop. He has been working on a new innovation using his company's development application. However, his son recently streamed a basketball game illegally from a questionable website, and unknowingly downloaded a screen scraper.

What is at risk:

Now, whenever Elon works on this laptop, the screen scraper will send screenshots of all his work to a bad actor. Since Elon works with sensitive source code and blueprints, the screen scraper could steal intellectual property to sell it on the dark web, resulting in stolen IP, corporate blackmail, and lost competitiveness.

How Citrix ZTNA Protects:

Citrix ZTNA allows IT Admins to block screen scraping malware. They can create a rule that enables screen scraping protection per user or user group, such as all employees in R&D. Even though the malware is installed, Citrix Secure Private Access will black out any screenshots taken, giving the bad actor nothing useful. This feature is unique to Citrix Secure Private Access (SPA) and cannot be found anywhere else on the market.

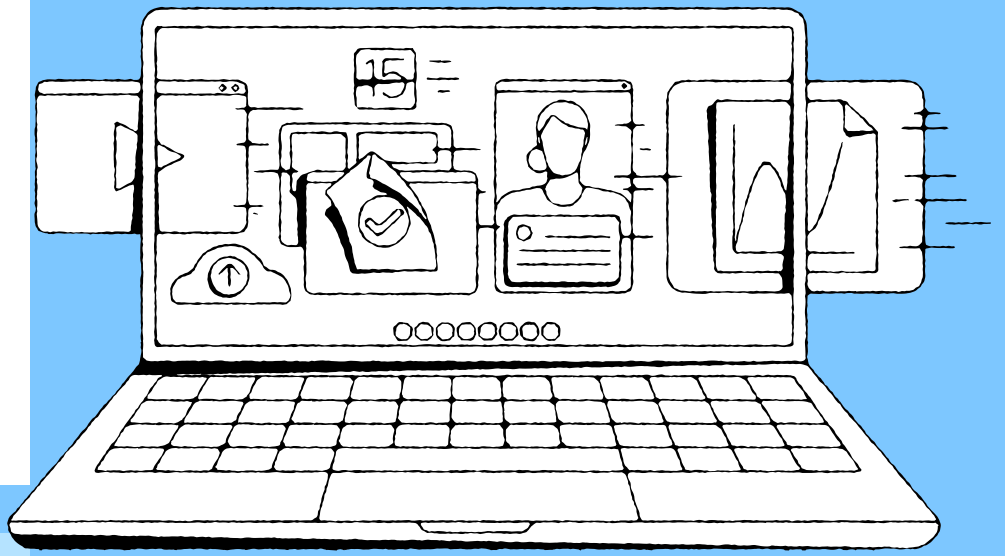
Protect Against Fake Anti-Virus Software

Scenario:

Dr. Frankenstein is a new sales agent in Hawaii for ProtectLife, a boutique life insurance provider in North America. After purchasing his work laptop from an electronics retailer, he was asked to download an antivirus (AV) by ProtectLife's IT team and send them a screenshot of the successful installation. Unfortunately, Dr. Frankenstein downloaded his AV from a sponsored search engine result, falling for a scam by hackers to download a fake AV.

What is at risk:

Since Dr. Frankenstein's laptop now has a fake AV, any customer information that he collects could be sent to bad actors who can use it against ProtectLife and its customers. This creates compliance and legal risk, threatening ProtectLife's reputation in the market.



How Citrix ZTNA Protects:

With Citrix Secure Private Access (SPA), ProtectLife can discover that Dr. Frankenstein does not have an authentic anti-virus installed on his laptop. They can inform him immediately and Citrix Secure Private Access (SPA) will only grant access to applications once he removes the fake AV and installs an authentic, updated AV with the latest virus definitions.

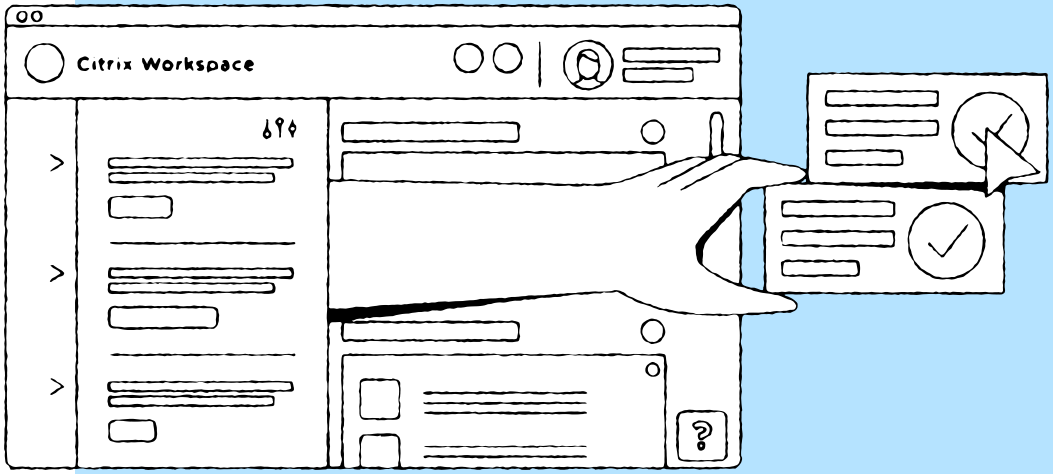
Protect Users and Data with Secure Mobile Browsers

Scenario:

Captain Ahab works in sales for Fresh Lobster Co. His work takes him all over the world, and he is constantly on the move finding restaurants to purchase his company's high quality lobsters. Since Ahab is constantly moving, he uses his mobile phone for 60% of his work, frequently using his mobile browser to access internal apps that give information on supply chain, sales updates, and pipeline data.

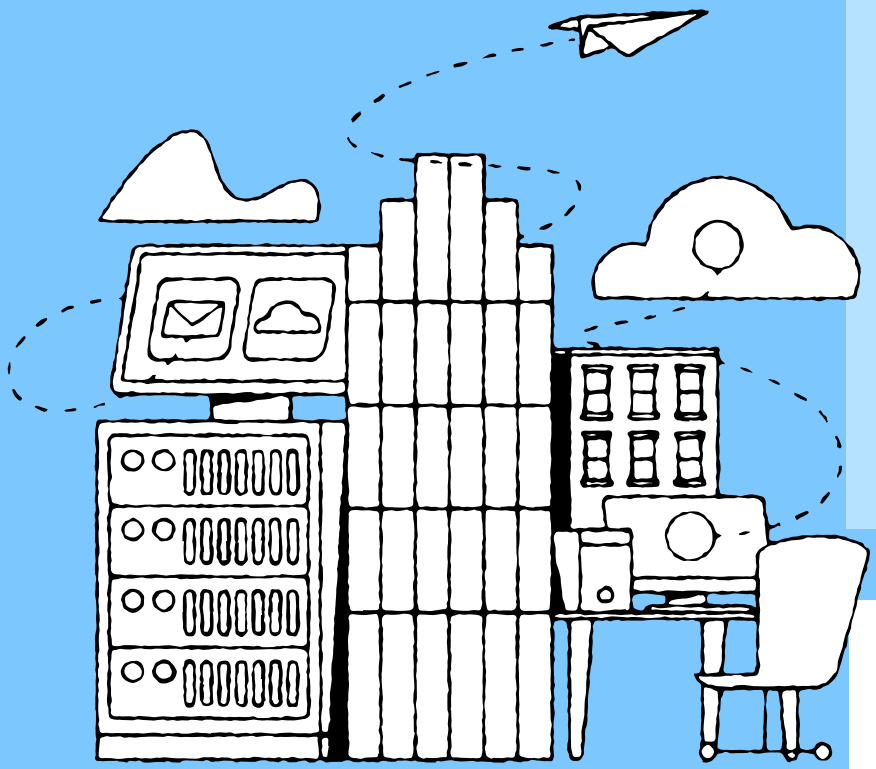
What is at risk:

Fresh Lobster Co does not have any special mobile browser technology. Since Ahab is often using public WiFi, it would be all too easy for a bad actor to plant malware on his device and breach Fresh Lobster Co's data. A bad actor could then blackmail the company or sell sensitive data to the dark web.



How Citrix ZTNA Protects:

With Citrix Secure Private Access (SPA), Ahab is able to use the same exact capabilities of his laptop's Workspace browser. This ensures multiple layers of protection and prevents a bad actor from accessing Fresh Lobster Co's internal applications.



Manage Device Safety with Patch & Endpoint Management

Scenario:

Sherlock is an energetic lad, brimming with enthusiasm. He hopes that one day he'll be the CEO of the US based airline company he works at. For now, however, he works as an offshore support representative. While Sherlock does all he can to be courteous and helpful to his customers, technology isn't his forte and he often ignores the alerts on his laptop.

What is at risk:

Latest versions of applications and operating systems include security patches for vulnerabilities. Hackers look for endpoints that have not been patched, using these vulnerable endpoints to enter an organizational network and laterally move from there. Once hackers have breached the network, they look for customer payment data, personally identifiable information, and company secrets. This puts Sherlock's employer, its customers, and Sherlock's dreams at risk.

How Citrix ZTNA Protects:

Enterprises can and should use patch management software to ensure that employees are only using the latest and most secure operating systems. Citrix Secure Private Access (SPA) can check if patch management client is enabled such that the endpoint is up-to-date with all required security patches. If not, a more robust policy can be enforced to restrict certain sensitive applications access or even take a more drastic measure of not allowing access to any applications.

Your ZTNA Protection Index

	Have It	Need It	Risk It
Adaptive & Contextual Access Use Cases			
Least Privilege Access Based on Specific User Needs	☐	☐	☐
Location-Aware Adaptive Authentication with MFA	☐	☐	☐
Application Authorization Based on User Location and Device	☐	☐	☐
Least Privilege Access Based on Dynamic User Risk Score	☐	☐	☐
Enforce Active Endpoint Protection Before Granting Application Access	☐	☐	☐
Enforce Latest Anti-Virus Software Version and Definitions Before Granting Access	☐	☐	☐
Block Against Phishing Attacks	☐	☐	☐
Enforce Data Backups to Protect from Ransomware	☐	☐	☐
Faster Completion of M&As	☐	☐	☐
Constant Monitoring & User Risk Score	☐	☐	☐
Data Loss & Threat Prevention Use Cases			
Protection from Key Loggers	☐	☐	☐
Mitigate Threats Targeting Outdated Operating Systems	☐	☐	☐
Prevent Data Loss from Careless Screen Sharing	☐	☐	☐
Prevent Data Loss with Remote Browser Isolation	☐	☐	☑
Enable Secure BYOD and Prevent Malware Transfer with Remote Browser Isolation	☐	☐	☐
Deter Data Theft for PCI Compliance	☐	☑	☐
Protection from Screen Scraping Malware	☐	☐	☐
Protect Against Fake Anti-Virus Software	☐	☐	☐
Protect Users and Data with Secure Mobile Browsers	☐	☐	☐
Manage Device Safety with Patch & Endpoint Management	☑	☐	☑

Your Current ZTNA Protection Index (all ticked green boxes) ___/20

Your Desired ZTNA Protection Index (all ticked green and yellow boxes) ___/20

Next Steps

Congratulations!

You've explored 20 different scenarios that could cause a breach! Your first step to building a robust, zero trust architecture for your organization is now complete!

If your Zero Trust Protection Index is less than 10, then you are at a high risk. It's important to identify scenarios most relevant to you and begin exploring solutions. We'd suggest starting with adaptive, context-aware access.

If your Zero Trust Protection Index is between 10 and 15, identify the specific area where you need additional protection – 'Adaptive and Contextual Access' or 'Data Loss Prevention and Threat Protection'.

If your score is over 15, that's great! You're well on your way but don't leave yourself unprotected for any scenarios. Use your Zero Trust Protection Index to identify your gaps and the insights within the scenarios to see how to close them.

Citrix has been advising organizations on their zero trust strategy and we would like to help you as well. Contact your Citrix representative for a detailed conversation.

Request a Meeting

Comprehensive Cybersecurity from Citrix

Citrix offers a portfolio of powerful cybersecurity functionality, extending from endpoint devices to hybrid multi-cloud applications. These cybersecurity functions help Citrix:

- Protect Access to IT-managed Apps: Adaptive, context-aware zero trust access to all apps – virtualized apps, DaaS, non-virtualized apps, SaaS, legacy client server – with unique and granular security controls.
- Protect Apps and APIs: Protect your most valuable assets and data with Web Application Firewall, Bot management, API protections and DDoS protection.
- Protect Internet Access: Comprehensive, cloud-delivered security service that includes SWG, CASB, firewall, malware protection, DLP and more.

Combining the above functionality into a unified platform, you get a comprehensive cybersecurity portfolio, all delivered with ease through a familiar and trusted vendor – Citrix.

Special thanks to Brian Huhn, Akshay Kakar, An Nguyen,
Andre Leibovici, Dan Feller, Pradeep Vasu, Jacob Rutski, Vijaya Raghavan,
Praveen Raghuraman, and Citrix Secure Private Access Engineering team.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States