SureTech

SureTech IT Solutions

Baseline Audit Report

Prepared by

RAYTECH.

October 29, 2024

SureTech

Your Customized Audit Report

In the following pages you'll find your customized Audit Report. It contains all of the information gathered from your IT environment into one easy-to-read document. Upon reading, you will have a much better understanding of your IT plan and what you're spending.

Based on our technical analysis of your IT environment, we have customized a selection of audit items spread across one or more main areas of technology.
Each of these areas will give you important insight into the strengths and weaknesses of your IT plan.

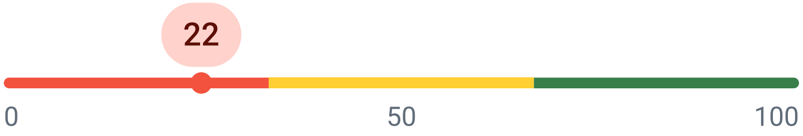
Your Audit Score

Using the results of your audit, we calculated your overall score. The higher your audit score, the greater efficiency at which you are spending on technology. Our goal is to drive your audit score as close to 100 as possible.
The comparative Analysis page allows you to easily compare your baseline plan with other plans presented in this document to see qualitative, quantitative and financial results.

How to Read your Report

Each audit item has been color coded to make it easy to visualize your results. Red indicates an audit item that requires immediate attention, yellow indicates an audit item that needs improvement and green indicates an audit item that is satisfactory.
In addition to a summary page, you will find dedicated pages with color coded summary statements for each individual audit item. Any audit item that isn't satisfactory is described in greater detail and its relative importance is explained in a single statement.

Audit Score



Infrastructure

🟥	🟥	🟥
🟥	🟥	🟥
🟥	🟨	🟥

Security

🟥	🟥	🟥
🟥	🟥	🟥
🟥	🟨	🟥

Managed Support & Services

🟨	🟥	🟨
🟨	🟨	🟥
🟥	🟨	🟨

Telecommunications

🟩	🟩	🟩
🟩	🟥	🟨
🟥	🟨	🟥

PCI Compliance

🟨	🟨	🟥
🟥	🟨	🟥
🟩	🟥	🟩

Cyberattack Risk

🟥	🟨	🟥
🟥	🟩	🟥
🟥	🟥	🟩

Microsoft Cloud

🟥	🟨	🟨
🟨	🟥	🟨
🟥	🟨	🟥

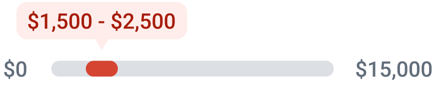
🟥 Requires Immediate Attention 🟨 Needs Improvement 🟩 Satisfactory

Baseline Plan Summary

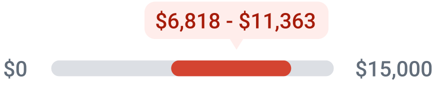
The results of each category of your base plan audit is summarized here using color-coded boxes. Utilizing a weighted scoring system, the results were combined and averaged into an overall audit score. Individual category scores and details for each audit item are shown in subsequent pages. Your base monthly IT expense is shown as a range and has been converted into effective IT monthly expense based upon your audit score. This helps to level the playing field when comparing plans.

Financial Summary

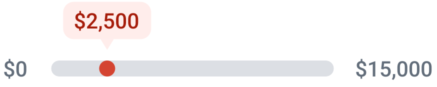
Monthly IT Expense



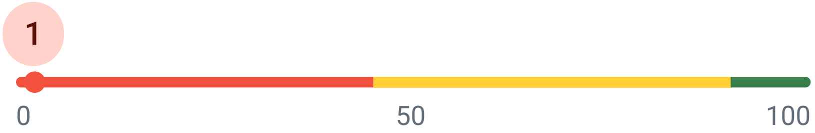
Effective Monthly IT Expense



One-time Cost



Infrastructure



Infrastructure is the foundation upon which all of your technology rests. Just like with a house, it's extremely important to verify its integrity before you begin to build on top of it. Poor initial design decisions can lead to downtime, lost sales and ultimately drive up your total cost of ownership. This detailed analysis page represents an overview of the state of your Base Plan Infrastructure. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Infrastructure audit score. easy identification and the results for this section are reflected in the Infrastructure audit score.

Business Continuity

There is no business continuity in the current environment.

Server

The server is over 5 years old, out of warranty or running a non-supported operating system.

Backup & Disaster Recovery

The current BDR solution does not meet compliance standards and needs to be replaced.

Remote Accessibility

Employees don’t have the ability to work from home or cannot perform key job functions when outside of the office.

Cloud to Cloud Backup

Hosted applications are not currently backed up and depend on vendor support for recovery.

Disaster Recovery Plan

No data recovery plan.

High Availability

There is no high-availability in place which means that any network outage will lead to work stoppage.

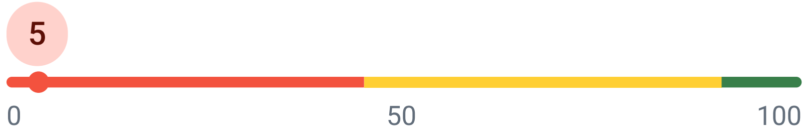
Data Compliance

The office has met some of the Regulatory Compliance requirements from HIPAA or FINRA.

Workstations

Remote workstations such as laptops & home computers are excluded from being monitored, patched, and secured.

Security



Security is arguably the most important section of your audit report. With so much riding on the security of your infrastructure, you can't afford to have any deficiencies. Fortunately, there's an abundance of security solutions available to help mitigate the risks and protect your data. This detailed analysis page represents an overview of the state of your Base Plan Security. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Security audit score.

Security Awareness Training

There is no ongoing security awareness training program in place to educate and provide occasional staff testing.

Endpoint Encryption

There is no endpoint encryption in place.

Managed SOC

There is currently no Managed SOC solution implemented.

Dark Web Monitoring

Employees and key exec passwords found on the dark web.

Managed DNS

There is no managed DNS and local DNS servers are pointed to the ISP's DNS servers.

Next Generation Endpoint Protection

Using old Anti Virus software that does little to protect from new risks.

Application Whitelisting

No application whitelisting is enacted at this location.

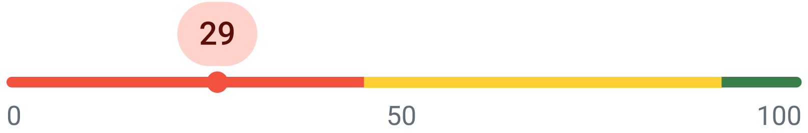
Anti-Phishing

Anti-phishing is in place but not completed in a proactive manner.

Content Filtering

There is no content filtering in the environment.

Managed Support & Services



Managed Support & Services is the customized/user defined category as per business need.

🟨 Onsite Support

Onsite Support is billed against blocks of hours at a discounted rate.

🟥 Help Desk Support

Remote Help Desk Support is not included and is billed hourly as needed.

🟨 Monitoring

Monitoring of server(s) and workstations is included in the plan but remediation is manual.

🟨 Inventory & Asset Management

Inventory & Asset Management is manual, included at no additional cost and reviewed quarterly.

🟨 Windows & Application Updates

Windows updates on server(s) and workstations are automated but not all are up to date.

🟥 Virtual CIO Services

vCIO services are not provided by current IT consultant.

🟥 Proactive Maintenance

Proactive maintenance of server(s) and workstations is manual and not included in the plan.

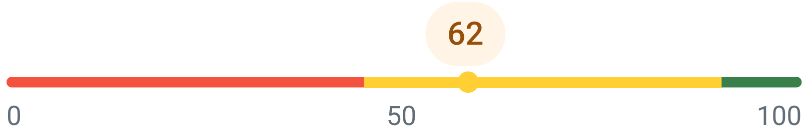
🟨 Mobile Device Management

Mobile device management (MDM) is in place for some but not all smartphones with email accounts configured.

🟨 Vendor Management

Vendor Management is billed hourly for all vendors with a valid support contract.

Telecommunications



Telecommunications is one of the fastest evolving areas of technology. Traditionally viewed as a separate cost center, the proliferation of voice over IP (VoIP) solutions has helped many businesses save more money while greatly improving upon their business continuity. This detailed analysis page represents an overview of the state of your Base Plan Telecommunications. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Telecommunications audit score.

🟩 Unified Communications

Remote workers are integrated into their phone system.

🟩 Enterprise Feature Set

The VoIP platform contains the same features as an enterprise phone system.

🟩 Transcription

Voicemail can be sent via email with transcription.

🟩 Telephony Continuity

The VoIP phone service will continue to route calls to other unified communication devices during power/internet outages.

🟥 Multi-Site Coordination

There is no ability to utilize phones or transfer calls seamlessly in other remote locations.

🟨 Future Proof Scalability

Needs Improvement.

🟥 Portability

There is no ability to move the current phone system without relocating phone lines or porting numbers to another carrier.

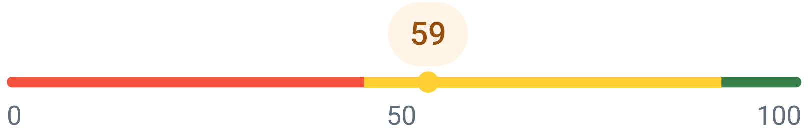
🟨 Ongoing Maintenance Fees

Vendor Management is billed hourly for all vendors with a valid support contract.

🟥 Fixed Fee Billing

Proactive maintenance of server(s) and workstations is manual and not included in the plan.

PCI Compliance



Payment Card Industry (PCI) compliance is a set of regulations developed to ensure that the credit card industry is properly managing and securing customer data. Before it was formed in 2006, there was no clear industry standard that all credit card companies had to follow, and that's a problem for any company that deals with big data. This detailed analysis page represents an overview of the state of your PCI Compliance. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the PCI Compliance audit score.
has context menu

Annual PCI SAQ

Annual PCI SAQ was completed and business was aware of the requirements to maintain PCI compliance except for their end-of-life device.

Credit Card Fee Recoupment

The business does not pass along a fee to their customers.

Credit Card Fees

Effective rate above industry standard.

EMV Chip Acceptance

The current payment device is not compliant and associated fees are being charged as a result.

Payment Software Integration

Vendor Management is billed hourly for all vendors with a valid support contract.

PCI DSS Compliance

The business is not currently compliant according to PCI DSS standards.

Point to Point Encryption

Point-to-point encryption is enabled, ensuring secure data transmission for PCI compliance and protecting sensitive cardholder information.

Secure Payment Gateway

The customer is not using a secure payment gateway which increases security vulnerabilities to their payment solutions.

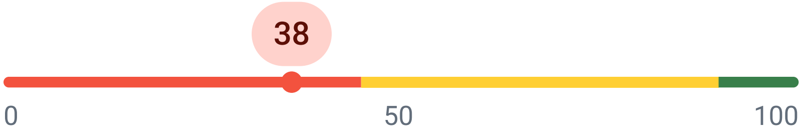
Tokenization

Tokenization ensures PCI compliance by replacing sensitive card data with secure tokens, reducing the risk of data breaches.

Baseline Plan

Category Details

Cyberattack Risk



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc vulputate libero et velit interdum, ac aliquet odio mattis. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur tempus urna at turpis condimentum lobortis.

Password Policy

A password age policy exceeding 90 days can lead to security risks, as users may choose weaker passwords or forget them, increasing vulnerability.

Password Management

Relying on password management software can be risky if the stored passwords aren't strong enough, leaving users vulnerable to breaches.

Dark Web Monitoring

Account credentials may have been compromised, posing a security risk. Immediate action is needed to secure your account.

Endpoint Encryption

BitLocker encryption is not enabled, exposing sensitive data to theft, increasing the risk of data breaches and non-compliance with security standards.

Anti-Virus

Anti-Virus is corporately managed by a cloud based subscription and all endpoints are up to date.

Data Encryption Policy

Sensitive data was detected, requiring immediate action to secure and protect the information from potential exposure.

Data Compliance

Sensitive data has been compromised, exposing individuals to identity theft, fraud, and privacy violations, undermining trust in the organization.

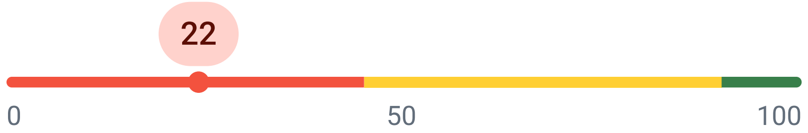
Vulnerability Management

Critical external vulnerabilities detected can expose systems to severe attacks, risking data breaches and compromising overall security.

Content Filtering

Content filtering is enabled to ensure a safe and secure environment by blocking harmful or inappropriate content.

Microsoft Cloud



The Microsoft Cloud is an open cloud platform made up of products and solutions that empower organizations to thrive in a changing world. It offers a variety of tools to help businesses manage challenges and meet their goals, drive value faster, and build for the future. It also helps protect and defend your business with security, compliance, identity, and management solutions that work across all your platforms, clouds, and apps.

Cloud Storage

Unrestricted additional storage providers in Microsoft Cloud pose security risks, leading to potential data leaks and compliance issues.

Admin Role Overlap

Admin Role Overlap in Microsoft Cloud leads to excessive access permissions, increasing security risks and complicating role management.

Third Party Applications

Blocking Chrome from allowing third-party cookies disrupts user experience, causing issues with website functionality and personalized content.

Azure Site Recovery (ASR)

Failure to configure ASR rules to block download scripts increases vulnerability to malware, putting systems at greater risk of attacks.

Microsoft Defender

Defender Antivirus monitoring is not enabled, leaving systems vulnerable to threats and compromising overall security integrity.

Data Loss Prevention

DLP policies are not configured in Microsoft Cloud, leaving sensitive data vulnerable to leaks and unauthorized access.

Endpoint Detection & Response (EDR)

EDR Block Mode is not enabled, leaving systems vulnerable, allowing potential threats to execute without immediate detection or prevention.

Virtual Meeting Software

Lobbies for Meetings in Microsoft Teams is not enabled, allowing participants to join meetings without waiting for approval.

Transport Layer Security (TLS)

Deprecated versions of TLS have been identified; upgrade to newer versions is required.

Baseline Plan

Business Impact Summary - ***Severity*** - *1 of 2*

Requires Immediate Attention

Business Continuity

Infrastructure

🟥 **Problem State:** There is no business continuity in the current environment

Impact: No business continuity in place means that if there is an outage, there is no quick way to regain business operations and there may be downtime.

Backup & Disaster Recovery

Infrastructure

🟥 **Problem State:** The current BDR solution does not meet compliance standards and needs to be replaced

Impact: Without a BDR solution that complies with regulatory compliance you are subject to not meeting required regulatory framework and standards to maintain your existing liability coverage.

Cloud to Cloud Backup

Infrastructure

🟥 **Problem State:** Hosted applications are not currently backed up and depend on vendor support for recovery

Impact: If there is a vendor outage or breach, there is no third party backup to protect hosted applications and integrity of data, which is a critical single point of failure that can result in data loss.

Disaster Recovery Plan

Infrastructure

🟥 **Problem State:** No data recovery plan

Impact: You have identified this as critical to your operations. If data loss happens, company will be fined daily and have to go through government audit. This will greatly impact production and delivery.

Security Awareness Training

Security

🟥 **Problem State:** There is no ongoing security awareness training program in place to educate and provide occasional staff testing

Impact: Internal staff members are the largest threat vector for security breaches and training is a key element to ensure that they take some responsibility in the security posture of the organization.

Baseline Plan

Business Impact Summary - ***Severity*** *- 2 of 2*

Requires Immediate Attention (cont.)

Managed SOC — Security

🟥 **Problem State:** There is currently no Managed SOC solution implemented

Impact: MSPs that implement a Managed SOC solution are able to provide a comprehensive cyber security offering to their customers. They also are able to leverage resources by outsourcing to a company that provides this service with dedicated, experienced cyber security professionals.

Dark Web Monitoring — Security

🟥 **Problem State:** Employees and key exec passwords found on the dark web

Impact: High risk for a data breach. A data breach could not only cause financial loss, it could interrupt operations for days or weeks which would be profoundly important for client retention.

Next Generation Endpoint Protection — Security

🟥 **Problem State:** Using old Anti Virus software that does little to protect from new risks

Impact: If the business is hacked and is offline for more than 30 minutes, supply chain impact can have devastating and rippling effects on business and profits.

Application Whitelisting — Security

🟥 **Problem State:** No application whitelisting is enacted at this location

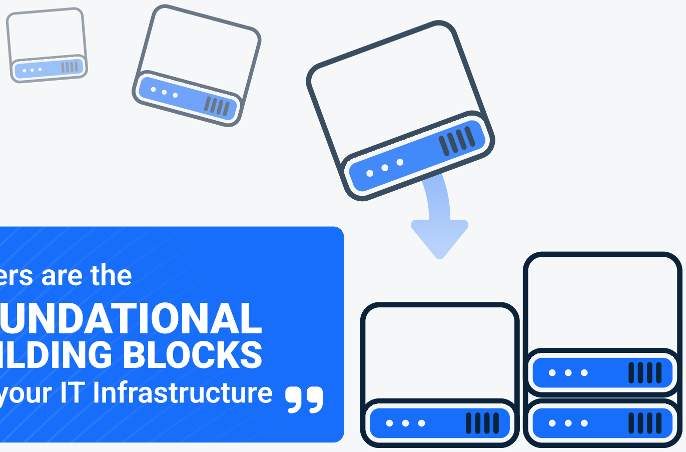
Impact: Users are able to install and run any applications including those that may be malicious or harmful to the environment.

Endpoint Encryption — Security

🟥 **Problem State:** There is no endpoint encryption in place

Impact: Workstations are subject to compromise by malicious actors which can jeopardize company data through an attack through the employee vector.

Servers



> Servers are the **FOUNDATIONAL BUILDING BLOCKS** of your IT Infrastructure

Servers provide a centralized location to store and share data and enable you to manage security. They can also be utilized to run applications, host your email, or to provide specialized functions such as running a database. Servers need to be properly maintained, patched, and secured against unauthorized access.

Upgrading Server OS Increases:

- Performance
- Scalability
- Availability
- Manageability

Migrating to the Cloud Improves:

- Speed
- Resiliency
- Cost
- Security

Windows Server 2016

END OF LIFE:

January 12, 2027

Why is this Important?

If your office has **servers** onsite or co-located in a data center, it's important that they run a supported operating system. If not, Microsoft won't release any more security updates or patches and your server could become vulnerable to hackers. In addition, maintaining a valid warranty ensures a faster and more affordable support from the manufacturer. Owning servers carries a whole host of responsibilities, including backup, security, maintenance, and, if applicable, adherence to legal and regulatory compliance standards dictated by HIPAA and FINRA.

Did You Know?

The average **server life span** is:

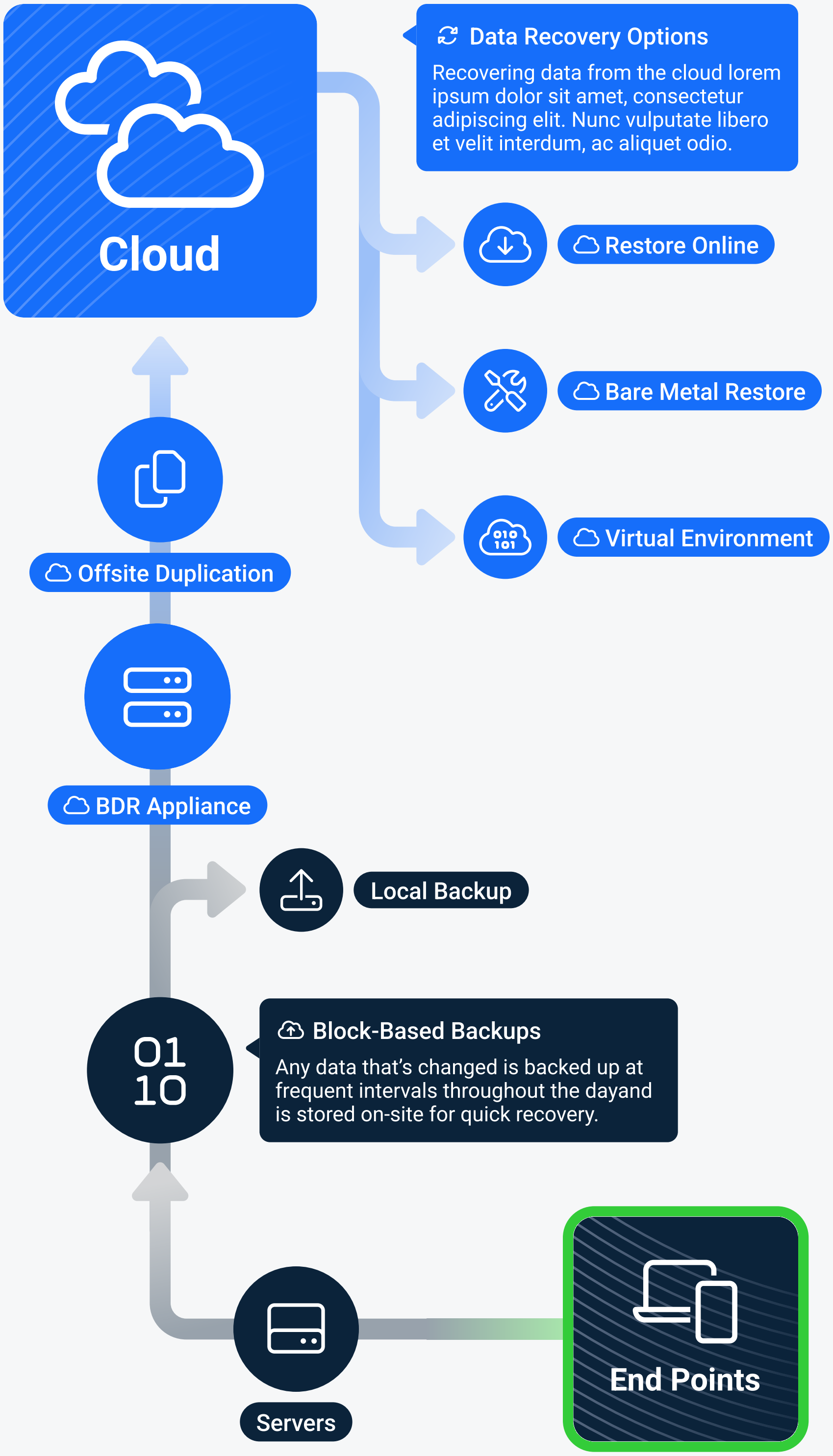
3-5 Years

Life cycles are getting shorter due to higher demands from newer technology

Infrastructure

⬜ 🟥 ⬜
⬜ ⬜ ⬜
⬜ ⬜ ⬜

Backup & Disaster Recovery



Cloud

Data Recovery Options

Recovering data from the cloud lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc vulputate libero et velit interdum, ac aliquet odio.

- Restore Online
- Bare Metal Restore
- Virtual Environment

Offsite Duplication

BDR Appliance

Local Backup

Block-Based Backups

Any data that's changed is backed up at frequent intervals throughout the dayand is stored on-site for quick recovery.

Servers

End Points

Why is this Important?

Backup & Disaster Recovery (BDR) is one of the most important areas of concern in your IT infrastructure. Everything is working against you; hackers, viruses, bad weather, hardware malfunction, rogue employees, accidental deletion, etc. You need to make sure that your critical data and the servers that they reside on are backed up and highly available with a copy offsite in case of disaster. Traditional tape backups are no longer a viable option and with great BDR offerings available, no small business should ever be down for extended periods of time.

Did You Know?

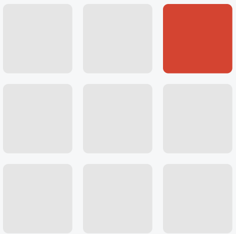
24%

of organizations chose **cost savings** as the most important reason to utilize cloud backup

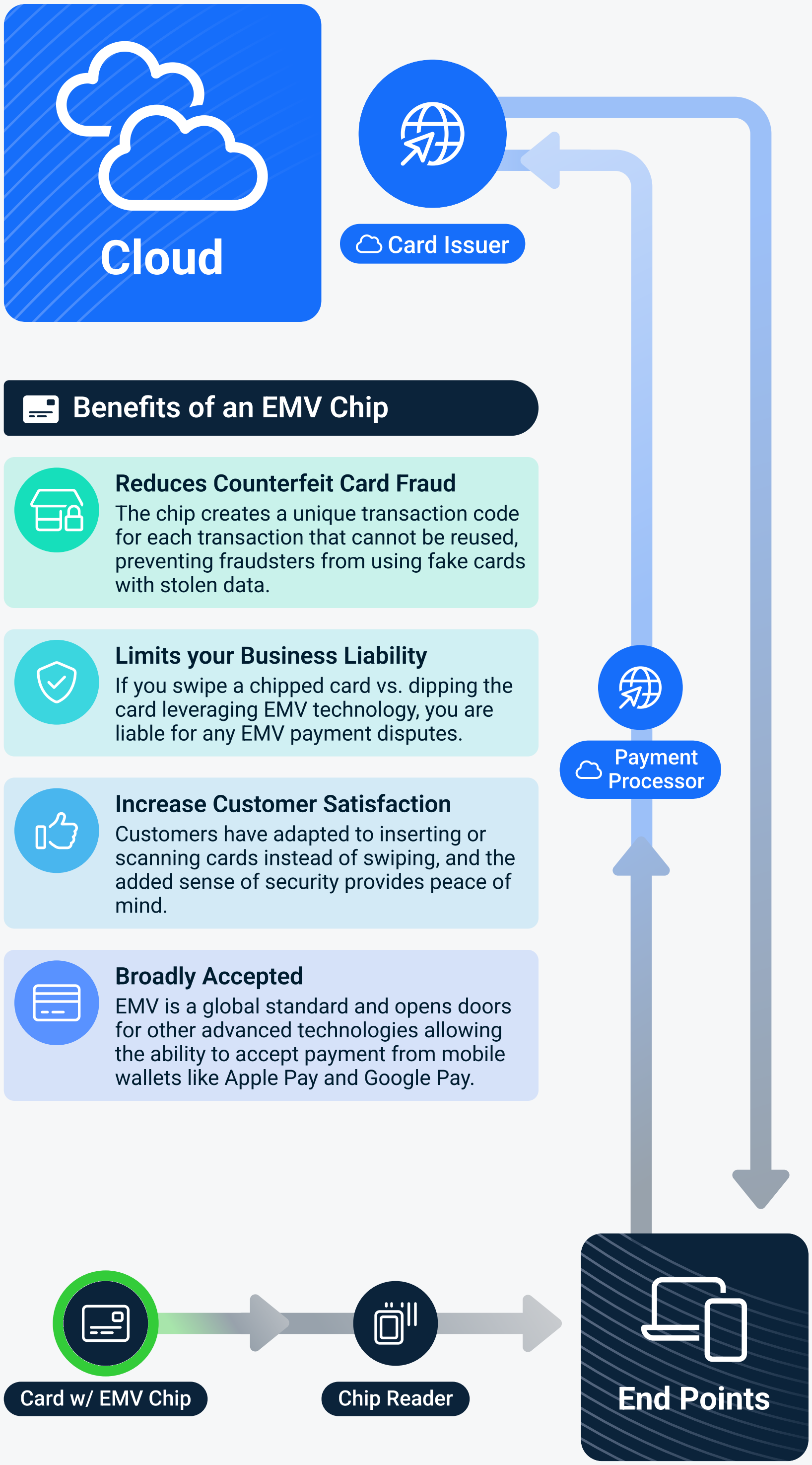
94%

of companies asking users to back up their own data said users **don't follow policy!**

Infrastructure



EMV Chip Acceptance



Benefits of an EMV Chip

Reduces Counterfeit Card Fraud
The chip creates a unique transaction code for each transaction that cannot be reused, preventing fraudsters from using fake cards with stolen data.

Limits your Business Liability
If you swipe a chipped card vs. dipping the card leveraging EMV technology, you are liable for any EMV payment disputes.

Increase Customer Satisfaction
Customers have adapted to inserting or scanning cards instead of swiping, and the added sense of security provides peace of mind.

Broadly Accepted
EMV is a global standard and opens doors for other advanced technologies allowing the ability to accept payment from mobile wallets like Apple Pay and Google Pay.

Why is this Important?

EMV, short for **Europay, Mastercard, and Visa**, is a set of standards governing card authentication technology that utilizes a chip embedded in a credit card rather than a magnetic strip. Credit card which follow the EMV standard will include a chip containing the card's information in addition to the standard magnetic strip. EMV card readers require the card to be inserted into a terminal, providing authentication that the card is valid. For retailers, it is incredibly important to understand the requirements that need to be met to ensure that you are not liable for any fraud.

Did You Know?

441,000

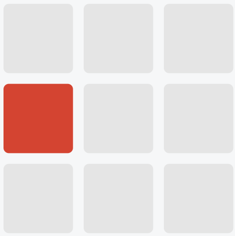
reported cases of **credit card fraud** were reported in 2022 alone.

- FTC Consumer Sentinel Network 2021 Report

The good news is, EMV has helped **reduce in-store credit card fraud** by

75%

Infrastructure



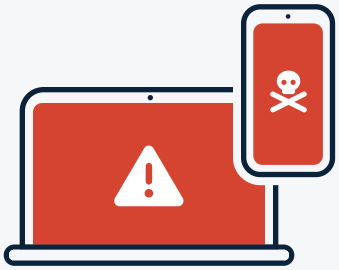
Workstations

Modern Workstations

As the world modernizes, so do the methods utilized by online threats. As mobile phones and other personal devices become commonplace in offices, it is vitally important to protect and manage all endpoints against these threats. In order to protect personal data, financial information, and intellectual property, workstations need to the latest operating system and modern software.

Up-to-Date Workstations

- Latest OS Version
- Protected
- Monitored
- Managed



Unprotected Endpoints

- Outdated OS
- Open to Attacks
- Unmonitored
- Unmanaged

Windows 10

END OF LIFE:

January 12, 2027

Why is this Important?

Workstations are the driving force behind technology in your office. It is important that they are running a supported operating system especially if you need to adhere to legal or regulatory compliance guidelines. Maintaining a valid warranty ensures faster and less costly support from the manufacturer. With cloud solutions, offices are able to employ Bring Your Own Device strategies and save money on future upgrades. It's common for end users to not only have a workstation but also a tablet, smartphone and possibly a laptop thereby increasing the threat landscape.

Did You Know?

There are more than

1.4 Billion

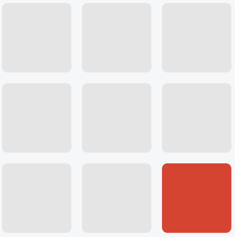
monthly active devices running **Windows 10** or **Windows 11**.

17%

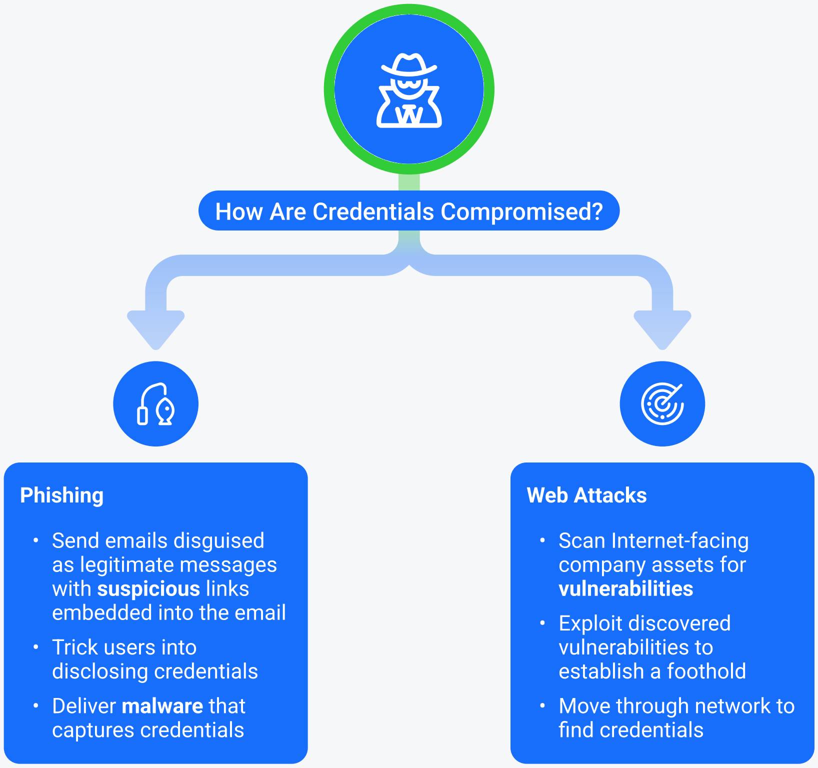
of all current Windows PCs were running Windows 7 as of July 2021.

TechAdvisor - 2021

Infrastructure



Dark Web Monitoring



How Are Credentials Compromised?

Phishing

- Send emails disguised as legitimate messages with **suspicious** links embedded into the email
- Trick users into disclosing credentials
- Deliver **malware** that captures credentials

Web Attacks

- Scan Internet-facing company assets for **vulnerabilities**
- Exploit discovered vulnerabilities to establish a foothold
- Move through network to find credentials

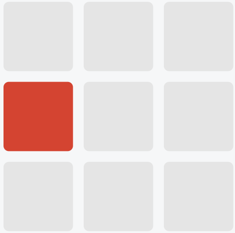
How are Compromised Credentials Used?

- **Identity theft**
- **Send spam from compromised email accounts**
- **Deface web properties and host malicious content**
- **Install malware on compromised systems**
- **Compromise other accounts using the same credentials**
- **Exfiltrate sensitive data**

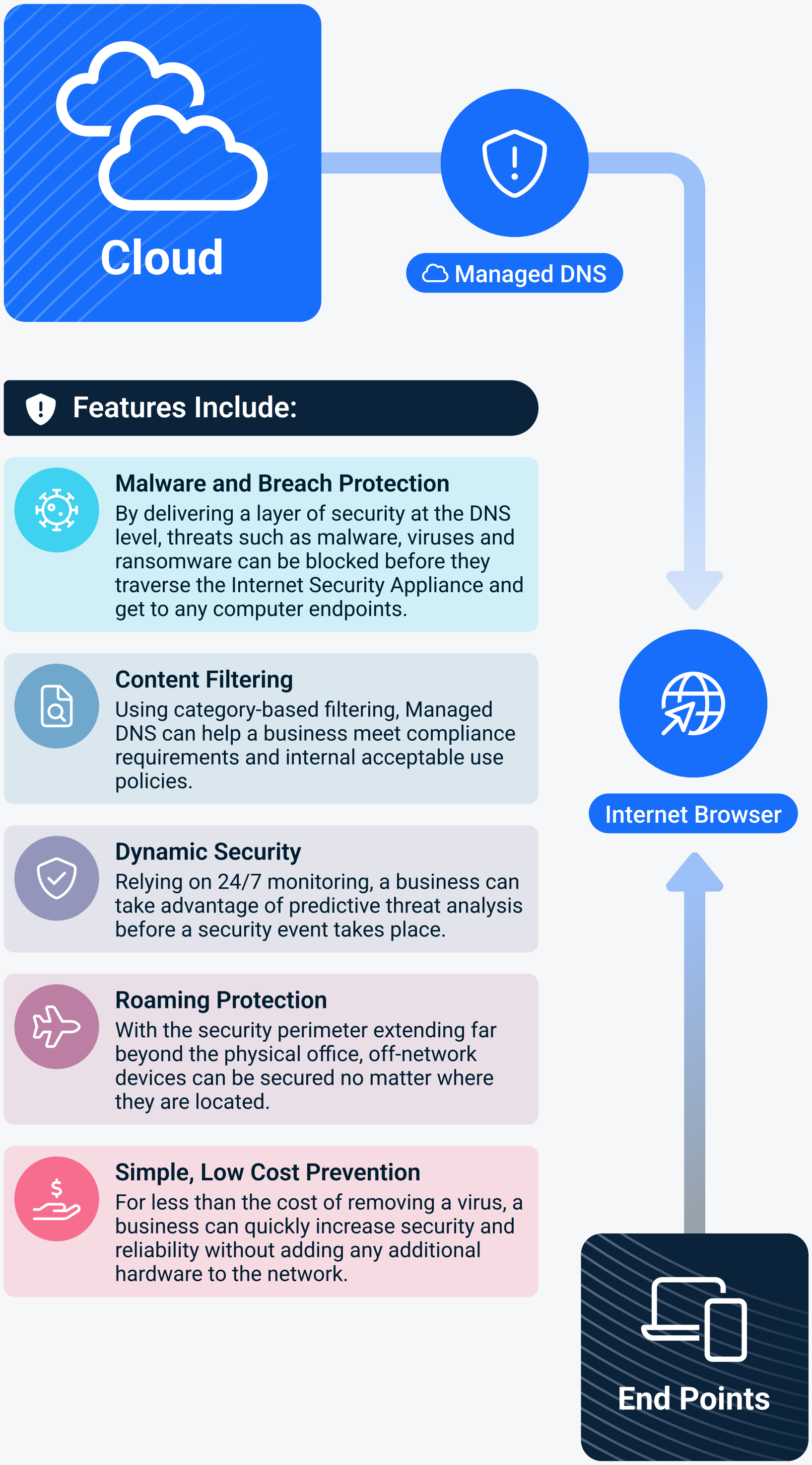
Why is this Important?

Your business is at constant risk of a security breach. When identity information is accessed and stolen, it is often traded on the “Dark Web”. This underbelly of the Internet is shrouded in mystery, hidden from most search engines and can only be accessed by a special web browser. **Dark Web Monitoring**, or cyber monitoring, allows you to monitor your personal information and receive notifications if your credentials, passwords, or other personally indentifiable information is found online. Dark Web Monitoring is also the best way to check on the effectiveness of your security awareness training program.

Security



Managed DNS



Features Include:

Malware and Breach Protection
By delivering a layer of security at the DNS level, threats such as malware, viruses and ransomware can be blocked before they traverse the Internet Security Appliance and get to any computer endpoints.

Content Filtering
Using category-based filtering, Managed DNS can help a business meet compliance requirements and internal acceptable use policies.

Dynamic Security
Relying on 24/7 monitoring, a business can take advantage of predictive threat analysis before a security event takes place.

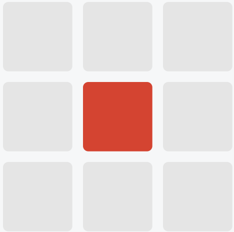
Roaming Protection
With the security perimeter extending far beyond the physical office, off-network devices can be secured no matter where they are located.

Simple, Low Cost Prevention
For less than the cost of removing a virus, a business can quickly increase security and reliability without adding any additional hardware to the network.

Why is this Important?

Everything that you do on the internet requires a connection to a **DNS Server** that tells your computer where to go for content that is being served up in your browser. Typically, you would use the DNS servers provided by your Internet Service Provider (ISP). Unfortunately, most ISPs don't provide any protection from internet threats and their servers can be overloaded causing the illusion of slow speeds and sluggish performance. You should consider using a cloud-managed DNS security service to add an additional layer of protection and speed in your office and on the road when using laptops and mobile devices.

Security



Next Gen Endpoint Protection

Key Components of Next Gen Endpoint Protection

Prevention
Reputation-based preemptive block & prevention policies - Protect from known threats.

Dynamic Exploit Detection
Protect from application and memory based exploits, drive by downloads.

Dynamic Malware Detection
Full system monitoring to protect from evasive, packed malware, social engineering/spear phishing.

Mitigation
Quarantine files and endpoints before they are able to gain access to sensitive data and systems.

Remediation
Automatic remediation to undo system changes and any damage that might have occurred.

Forensics
Real-time analysis & root cause forensic investigations that help prevent breaches in the future.

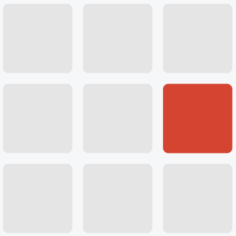
Why is this Important?

Effective protection against modern, sophisticated threats requires an innovative approach in the way they are detected, blocked, mitigated, remediated, and analyzed. With fewer threats being comprised of file-based malware, signature-based anti-virus and other static solutions could be considered inadequate protection. A **Next Generation Endpoint Protection (NGEPP)** solution protects against all major types of cyberattacks and doesn’t depend on signatures or heuristic file analyses. NGEPP detects threats dynamically, based on behavior and protects endpoints across all attack vendors.

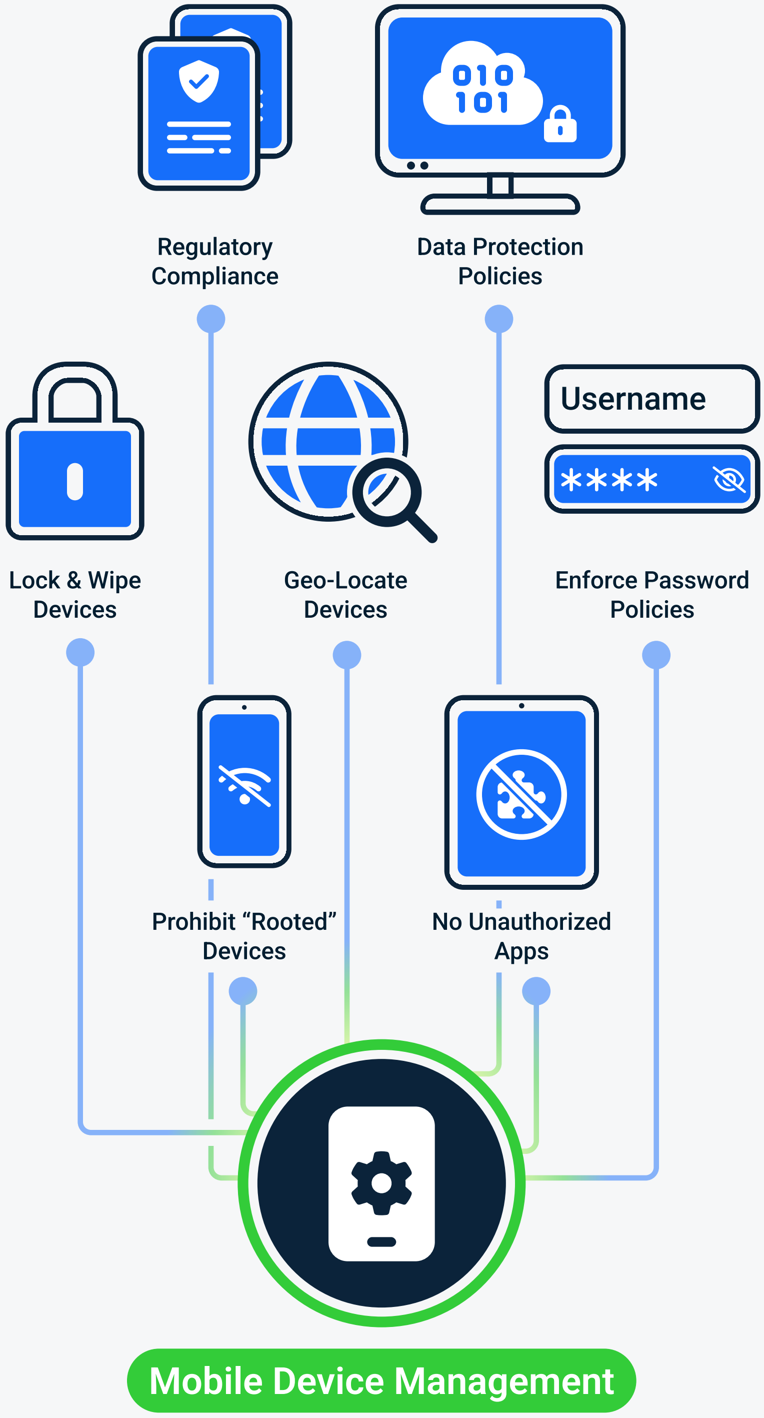
Did You Know?

A next generation endpoint protection solution needs to stand on its own to secure endpoints againsy both legaxy and advanced threats throughout various stages of the walware lifecycle. Administrators must be confident they can completely replace the protection capabilities of their existing legacy, static-based solution with one laneled as next generation endpoint protection.

Security



Mobile Device Management



Why is this Important?

Mobile Device Management (MDM) is a growing area of concern for many businesses. With so many employees bringing their own device to the office, corporate data such as email and file sharing could be at risk. Without an MDM solution, the business owner has an implied risk (of data loss) with zero control over these devices. Mobile Device Management allows the business to set and manage corporate policies that can optimize the functionality and security of a mobile communications network while reducing support costs and minimizing downtime.

Did You Know?

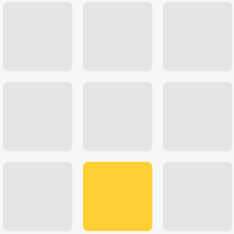
45%

of companies **aren't prepared** to support mobile communications network using MDM

61%

of companies that let employees use personal mobile devices have **higher employee satisfaction**

Managed Support & Services



Annual PCI SAQ

Types of PCI SAQs and Applicability

1 **SAQ A**
For merchants, who handle card-not-present transactions (excluding face to face channels) and outsource all the payment processing to PCI DSS validated third parties service providers.

2 **SAQ A-EP**
Applicable only for E-Commerce channels, with websites that do not get sensitive data directly and has outsourced all the payment processing third-party service providers.

3 **SAQ B**
This is for merchants that use various types of standalone, dial-out terminals, and imprint machines that do not have electronic cardholder data storage.

4 **SAQ B-IP**
This is applicable for merchants that use standalone, PTS-approved payment terminals with an IP connection to the payment processor and no storage for CHD.

5 **SAQ C**
For merchants with payment application systems with an internet connection and no electronic cardholder data storage.

6 **SAQ C-VT**
For merchants that enter the data of each transaction manually into virtual internet-based virtual terminal solutions provided by a PCI DSS validated third-party service provider.

7 **SAQ P2PE-HW**
For merchants using only PCI SSC-listed P2PE solution validated hardware payment terminals with no electronic cardholder data storage.

8 **SAQ D for Merchants**
All merchants that were not covered in the above list must go for SAQ.

9 **SAQ D for Service Providers**
When a Payment Card Brand defines a service provider, then it is eligible for Self-Assessment Questionnaire.

Next Steps: Download the appropriate **SAQ**, complete the survey, and after you make sure you're compliant, complete an **Attestation of Compliance**.

Why is this Important?

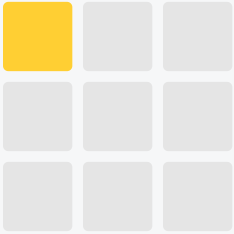
The annual **Self-Assessment Questionnaire (SAQ)** is designed as a validation tool used to assess the security of cardholder data for merchants. The growing popularity of card-based and online transactions has made it extremely convenient for consumers to conduct transactions. With the growth of cashless transactions, there has been a corresponding increase in fraud, identity theft, and other cyber-crimes. To reduce these instances, the PCI SSC has made it mandatory that every merchant or service provider who stores processes and/or transmits cardholder data (credit, debit, or prepaid card) needs to be PCI DSS compliant.

Did You Know?

For merchants and service providers that handles less than 6 million transactions annually, PCI DSS offers the option of Self-Assessment Questionnaires (PCI SAQ). This ensures the security of your business and cardholders data.

The 9 types of available PCI SAQs are shown to the left. You'll need to choose (or SISA will help you choose) the right one based on your particular payment and transaction scenario.

PCI Compliance



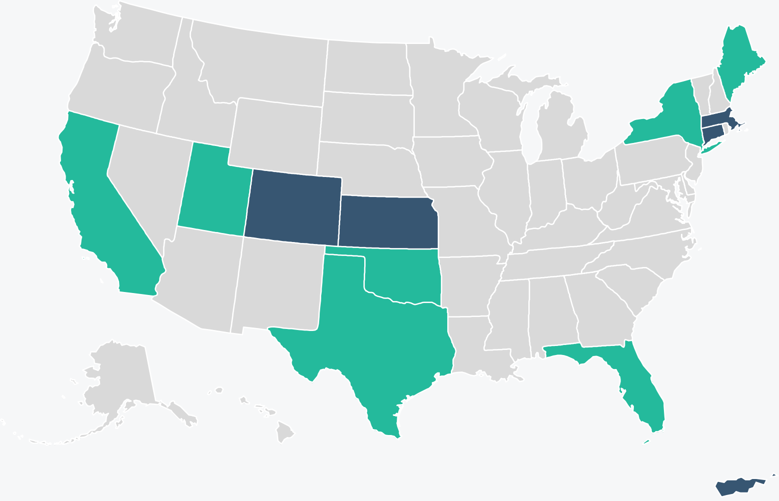
Credit Card Fee Recoupment

What is Recoupment?

Credit card fee recoupment is when an **extra fee is charged by a merchant** to a customer when the customer chooses to use a credit card for payment. This extra fee is designed to cover the cost the merchant incurs by accepting the credit card payment.

Recoupment is **not** allowed in all states, however. Several states and localities have enacted legislation regulating or **preventing passing credit card processing fees to the customer**.

Below is a map of all states that have either passed laws **banning the practice** or have laws that are **unenforceable** due to recent court rulings.



States/Territories with **legal bans** on Credit Card Fee Recoupment:

- Massachusetts
- Kansas
- Connecticut
- Puerto Rico
- Colorado

States with **unenforceable laws**:

- Texas
- California
- Florida
- New York
- Maine
- Oklahoma
- Utah

Why is this Important?

The primary benefit of **Credit Card Fee Recoupment** is the burden of credit card fees is pass on to the customer eliminating the cost to your business while still allowing your customers their choice of payment method. While credit card fee recoupment is becoming more acceptable every day, it is important to consider your customer. The initial cost savings could end up costing you significantly more overall if your customers do not accept it.

Did You Know...?

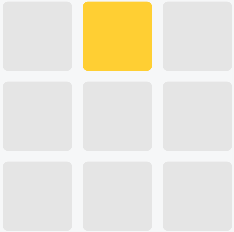
64.5%

of customers are not willing to pay an extra fee to use a credit card.

Age Breakdown:

18-35:	**52%**
36-49:	**63%**
50-64:	**70%**
65+:	**75%**

PCI Compliance



Credit Card Fees

Processing Fees Consist of the Following

Interchange Fees

The cost of interchange is set by each card network and covers risk, fraud, and operational expenses. Interchange is a **set cost** and **cannot be negotiated**. The fee is impacted by card type, transaction amount, business classification, and how the payment is processed.

Markup

The markup over interchange and assessments is the only area where you have the **ability to negotiate** credit card processing costs. Typically, about 20% to 25% of the total processing fee is made up by markup costs.

Assessment Fee

This is a small fee that all merchants incur when processing credit card transactions. The fee comes directly from the card brands and are **non-negotiable**.

Note: This is how Visa and Mastercard make their money.

Credit card fees can be billed in multiple ways, with pros and cons to each model. However, not all transactions clear at the same rate. A qualified transaction will process at a lower rate than a non-qualified transaction. Below are the different pricing models that you can choose from:

Types of Payment Processor Pricing Models

Interchange Plus

Merchants are charged a percentage of the transaction, as well as a fixed per-transaction fee. This is the most commonly used model due to its transparency and cost-effectiveness.

Flat Rate

Processors charge a fixed fee for all credit and debit card transactions regardless of the type of card used for payment.

Subscription Model

Merchants are charged a flat monthly service fee, along with a small per-transaction fee. The wholesale fee is separate from the markup fee.

Tiered Model

Processors charge a fee based on the card type, any risk associated with the transaction, and overall transactional volume of the business.

Why is this Important?

Credit Card Processing Fees are the fees a merchant pays for credit or debit card sales determined by the card issuer, the card network, and the payment processor. To get the best possible pricing for your credit card processing service, you need to understand the different pricing models that processors use and how they work. Credit card processing companies charge various fees, some you never have to pay. As a business, having a fundamental knowledge of how credit card processing fees are designed will help you choose a processor with the best rate and lowest fees.

Did You Know...?

For U.S. businesses that do between $10,000 and $250,000 in annual payments, the per-transaction fee amounts averages between

2.9% - 4.4%

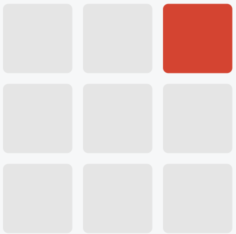
Square - 2020

U.S. merchants that accepted credit, debit, and prepaid cards as payment paid processing fees totaling

$116B

Square - 2020

PCI Compliance



Payment Software Integration

Benefits of integrating Payment Software

Save Time

Transaction details are sent straight to an ERP or account software without human interaction. This frees up more time in the day for employees to complete other tasks that they may not have normally been able to accomplish.

Save on Overall Expense

Payments are automatically updated to the software (e.g., General Ledger), removing the need for an employee to manage Accounts Receivable. It also lowers processing fees by automatically submitting line-item transaction details to the point of sale, reducing overall business expenses, and minimizing production costs.

Increase Cash Flow

Payments are automatically applied to accounting software and posted to Accounts Receivable and General Ledger which ensures businesses get paid ASAP.

Reduce Human Error

From entering data incorrectly, double entry, or applying incorrect data to accounts, accounting mistakes are bound to happen. With integrated credit card processing, payments are seamlessly passed into the account software.

Improve Your Workflow

One of the benefits of integrated credit card processing is that businesses can simply enter credit card data directly into the accounting software, and the integrated payment system takes care of the rest.

Strengthen Security

Cloud-based accounting is a software that runs on servers and allows businesses to access data from anywhere using the internet. It protects businesses from system administration costs and server failures. Many cloud-based accounting software are also PCI compliant, which helps protect credit card information in the event of a data breach.

Why is this Important?

A **Payment Software Integration** is a connection between a website or application and a payment processor or payment gateway. This allows credit card payments to be accepted directly from the application or website. An integrated payment solution offers a seamless checkout experience keeping your customers on your website or in your software application, reducing abandoned purchases. A payment software integration reduces human error by automating the payment process when compared to manually inputing transaction details.

Did You Know?

57%

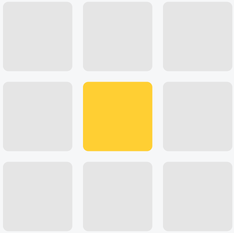
of SMBs are investing in technology for their customers, proving that **payment software** is increasingly important for business success.

Worldpay from FIS 2020 PACE report

40%

fewer abandoned purchases were reported by SMBs that invested in **integrated payment solutions**, due to a seamless checkout experience that kept customers in the application or website.

PCI Compliance



PCI DSS Compliance

PCI Compliance is mandated by credit card companies, and requires several operational and technical standards to be met. **These requirements are listed below:**

1. **Install and maintain a firewall configuration to protect cardholder data**
2. **Do not use vendor-supplied defaults for system passwords and other security parameters**
3. **Protect stored cardholder data**
4. **Encrypt transmission of cardholder data across open, public networks**
5. **Use and regularly update anti-virus software or programs**
6. **Develop and maintain secure systems and applications**
7. **Restrict access to cardholder data by business need to know**
8. **Assign a unique ID to each person with computer access**
9. **Restrict physical access to cardholder data**
10. **Track and monitor all access to network resources and cardholder data**
11. **Regularly test security systems and processes**
12. **Maintain a policy that addresses information security for all personnel**

Why is this Important?

The **Payment Card Industry Data Security Standard (PCI DSS)** is an information security standard that was created to increase controls around cardholder data to reduce credit card fraud. It is important to protect the data of your business, employees, and customers. The purpose of PCI DSS is to aid in protecting card data from hackers and thieves. PCI DSS standards help keep your data secure and can prevent costly data breaches which can range from tens of hundreds of thousands of dollars, which could potentially result in the business shutting down for good.

Did You Know?

27.9%

of organizations are PCI DSS Compliant - an alarming number in the face of rising security threats.

The SSL Store - 2020

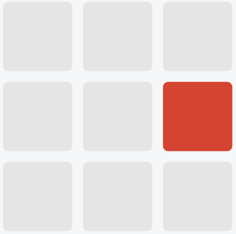
The average merchant, at the time of data compromise, **was NOT compliant** with at least

47%

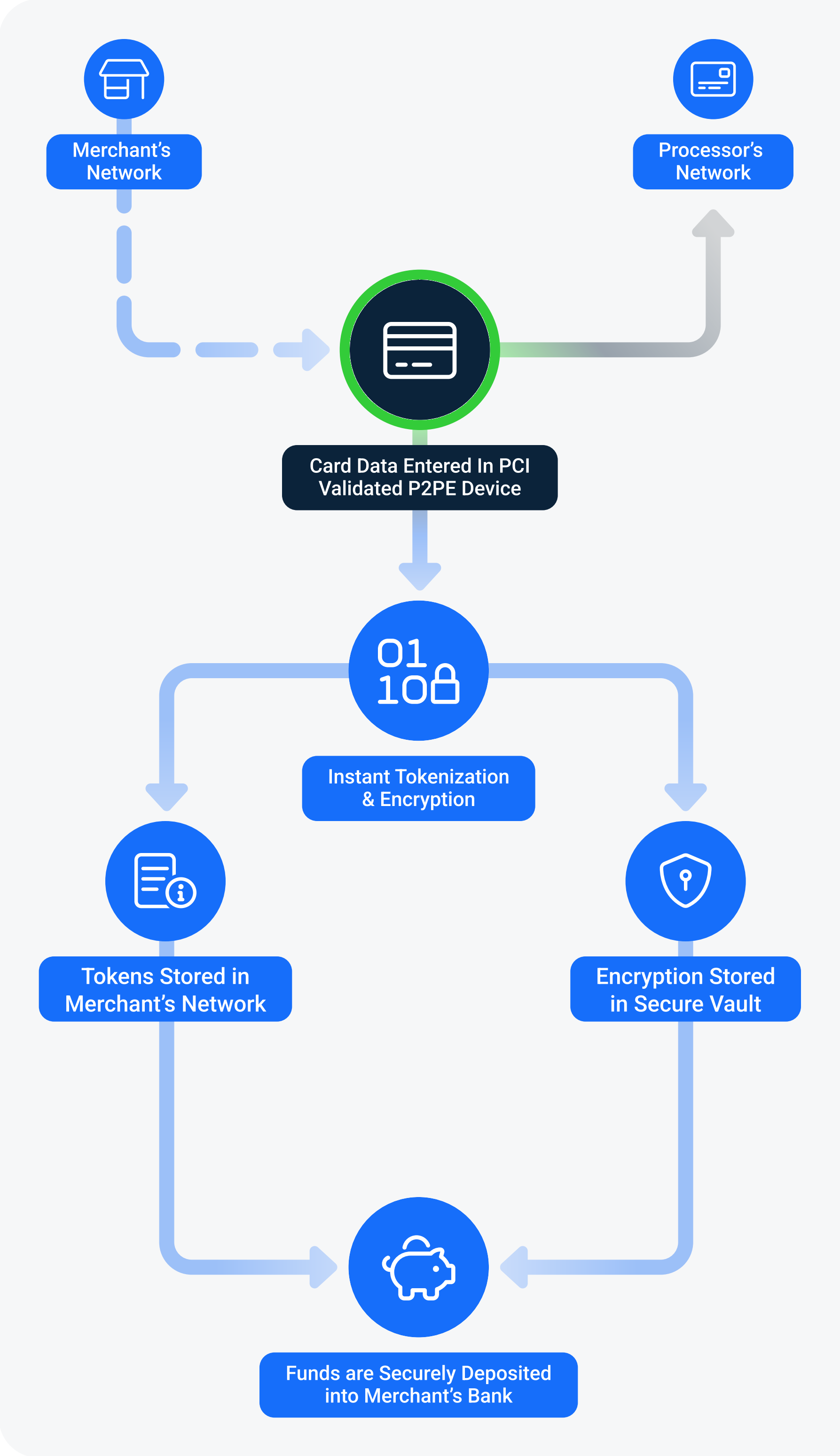
of PCI DSS requirements.

SecurityMetrics - 2017

PCI Compliance



Point-to-Point Encryption


Merchant's Network
Processor's Network
Card Data Entered In PCI Validated P2PE Device
01 10
Instant Tokenization & Encryption
Tokens Stored in Merchant's Network
Encryption Stored in Secure Vault
Funds are Securely Deposited into Merchant's Bank

Why is this Important?

Your customers want to know that they are protected however they choose to pay. **Point-to-Point Encryption (P2PE)** is an in-store protection solution that converts customer card data into meaningless code, making it unusable in the event of a cyberattack and removing the incentive for cyber-crime. P2PE encrypts payment card data from the point of capture, such as when the card is read by a card payment terminal, until it reaches the secure decryption endpoint.

Benefits

Increased Security

Reduces where and how PCI DSS applies to your environment due to the increased security of customer data.

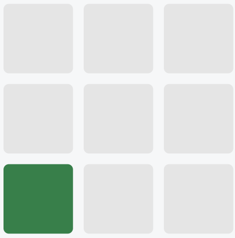
Shorter Assessments

Can significantly shrink the PCI self-assessment requirements by removing up to eight sections and hundreds of questions.

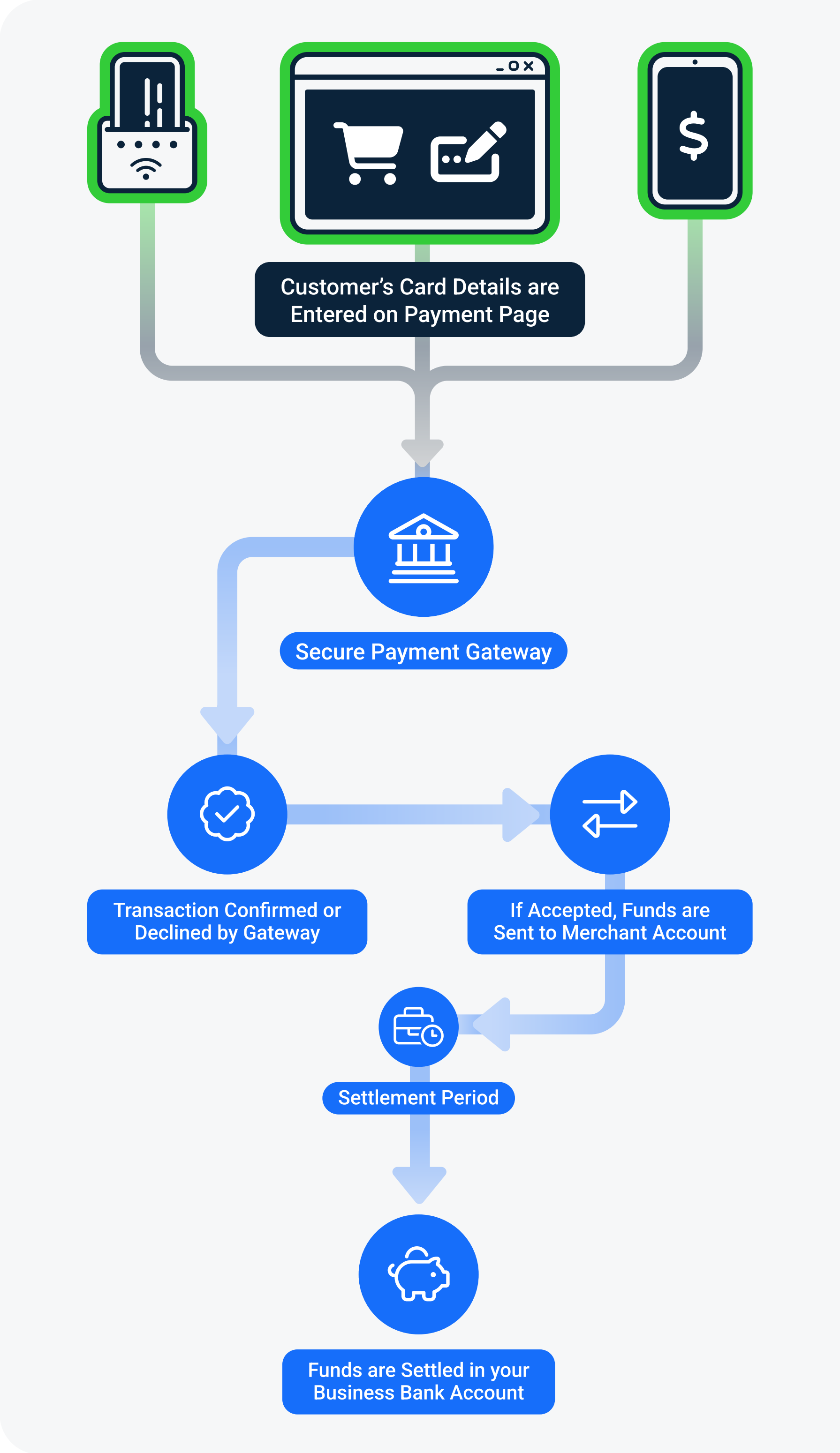
Theft Deterrence

Payment card data is devalued even if compromised in a breach because it cannot be decrypted.

PCI Compliance



Secure Payment Gateway



Customer’s Card Details are Entered on Payment Page

Secure Payment Gateway

Transaction Confirmed or Declined by Gateway

If Accepted, Funds are Sent to Merchant Account

Settlement Period

Funds are Settled in your Business Bank Account

Why is this Important?

A **Secure Payment Gateway** is a technology that securely captures and encrypts sensitive credit card details from a customer and transmits that data to a payment processor to complete a transaction. If you have a gateway that is PCI compliant and employs payment tokenization safeguards, your business and your customers will be protected. Your gateway should have the highest level of PCI compliance, a tier-1 level. The highest level tells you that your provider goes through annual third-party audits and vigorous precautions to ensure payment security.

Benefits

Omnichannel

Payment Gateways can accept transactions from many sources including virtual terminals, mobile devices, and more!

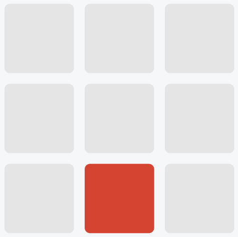
Vault

Gateways can store multiple payment methods per customer, enabling recurring payments and fast checkout without the need to re-enter payment details.

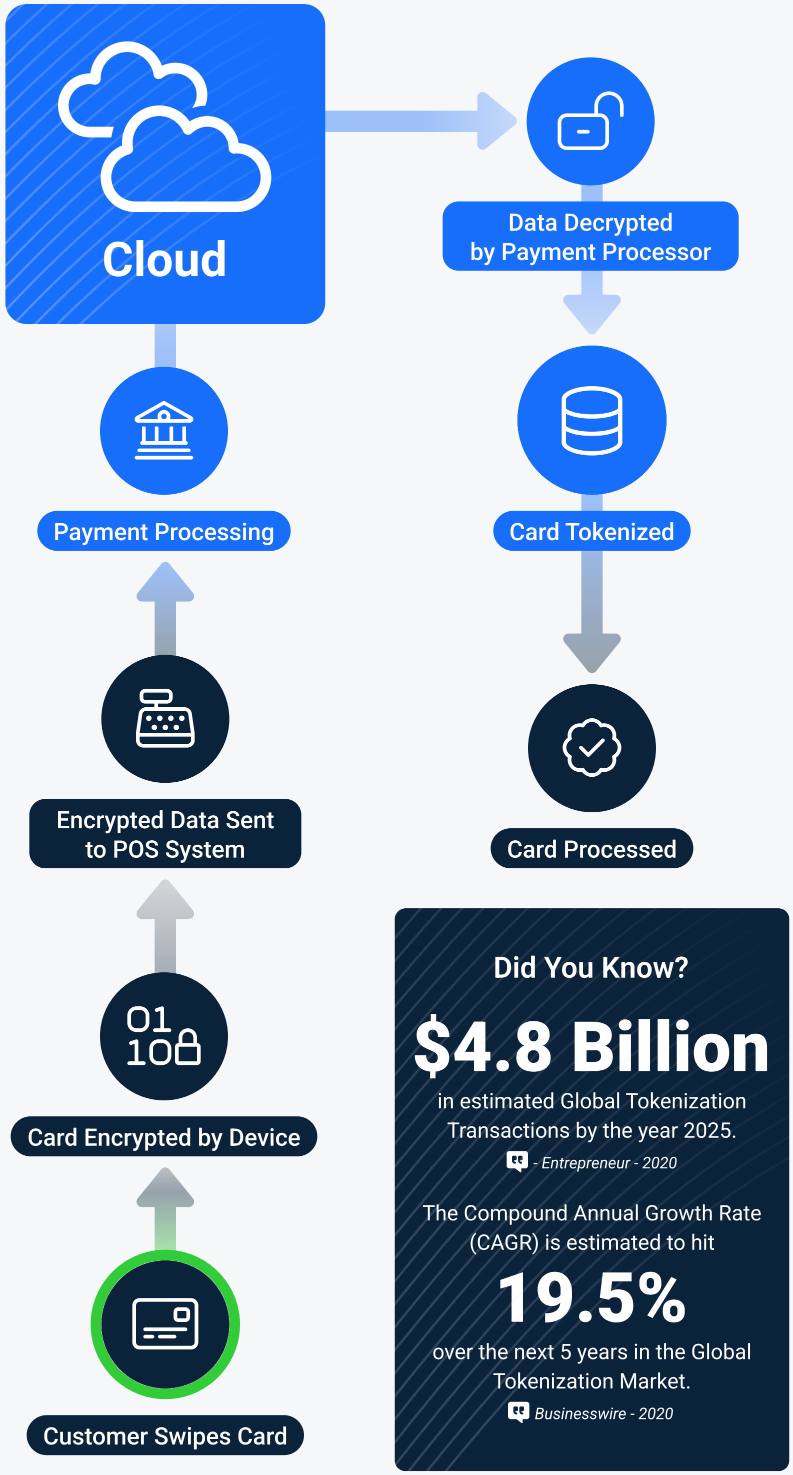
Security

Industry standard encryption and tokenization technologies allow Payment Gateways to protect sensitive data, reducing PCI scope.

PCI Compliance



Tokenization



Did You Know?

$4.8 Billion

in estimated Global Tokenization Transactions by the year 2025.

- Entrepreneur - 2020

The Compound Annual Growth Rate (CAGR) is estimated to hit

19.5%

over the next 5 years in the Global Tokenization Market.

Businesswire - 2020

Why is this Important?

Tokenization is the process of protecting sensitive data by replacing it with an algorithmically generated number called a **token**. This token can be securely passed through the internet without exposing real credit card data. Tokenization can work in multiple ways and can drastically reduce the financial impact of a data breach. Tokenization makes achieving and maintaining PCI Compliance significantly easier.

Benefits

Reduced Risk

The token cannot be mathematically reversed without the original key used to create the token rendering the compromised data virtually worthless.

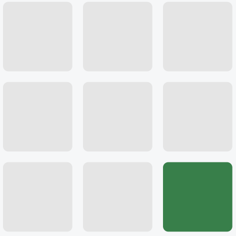
Easier PCI Compliance

Tokenization satisfies requirements by never letting sensitive cardholder information touch your systems in the first place.

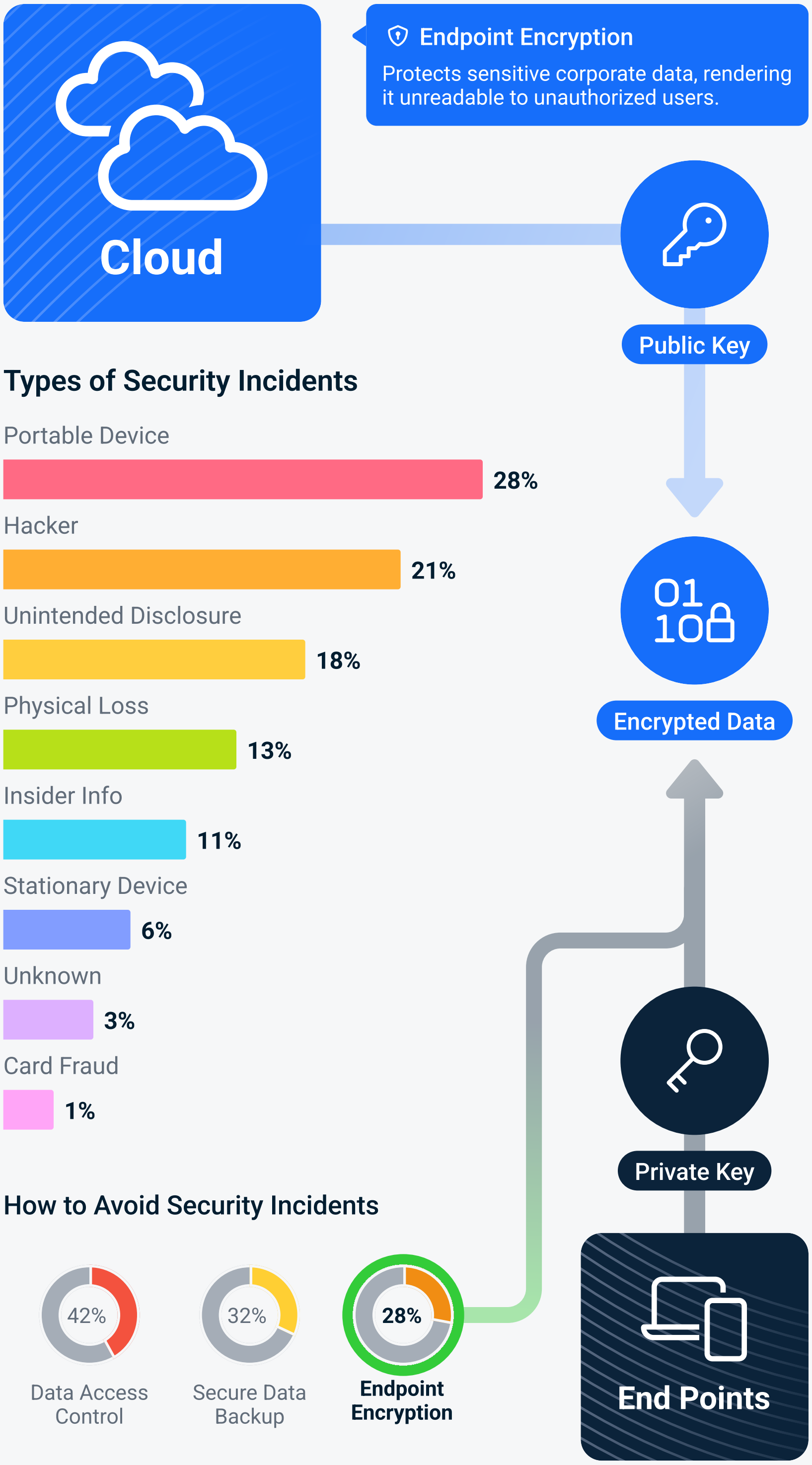
Flexibility

It can generate both single-use tokens, like for one-off purchases using a credit card, or multi-use tokens, like when credit card numbers are stored to enable faster e-commerce checkout experiences for future purchases.

PCI Compliance



Endpoint Encryption


Endpoint Encryption
Protects sensitive corporate data, rendering it unreadable to unauthorized users.
Cloud
Public Key
Encrypted Data
Private Key
End Points

Types of Security Incidents

How to Avoid Security Incidents

Why is this Important?

These days, network security is often focused on preventing attacks originating from outside of your network. It's easy to get caught up in the hype with all the latest data breach headlines in the news. The reality, however, is that you are more likely to suffer a loss of data that's stored on portable devices such as laptops, tablets, USB devices and the ubiquitous smartphone. The best way to protect your sensitive data is to use **encryption on all of your endpoints**. That way, even if a device is lost or stolen, the data residing on it is unreadable to anyone who doesn't possess a passphrase or key to decrypt it.

Did You Know?

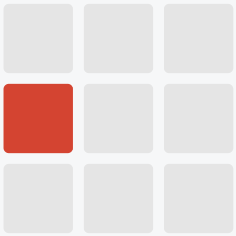
29%

of security incidents is a result of **insider information** or **unintended disclosure**.

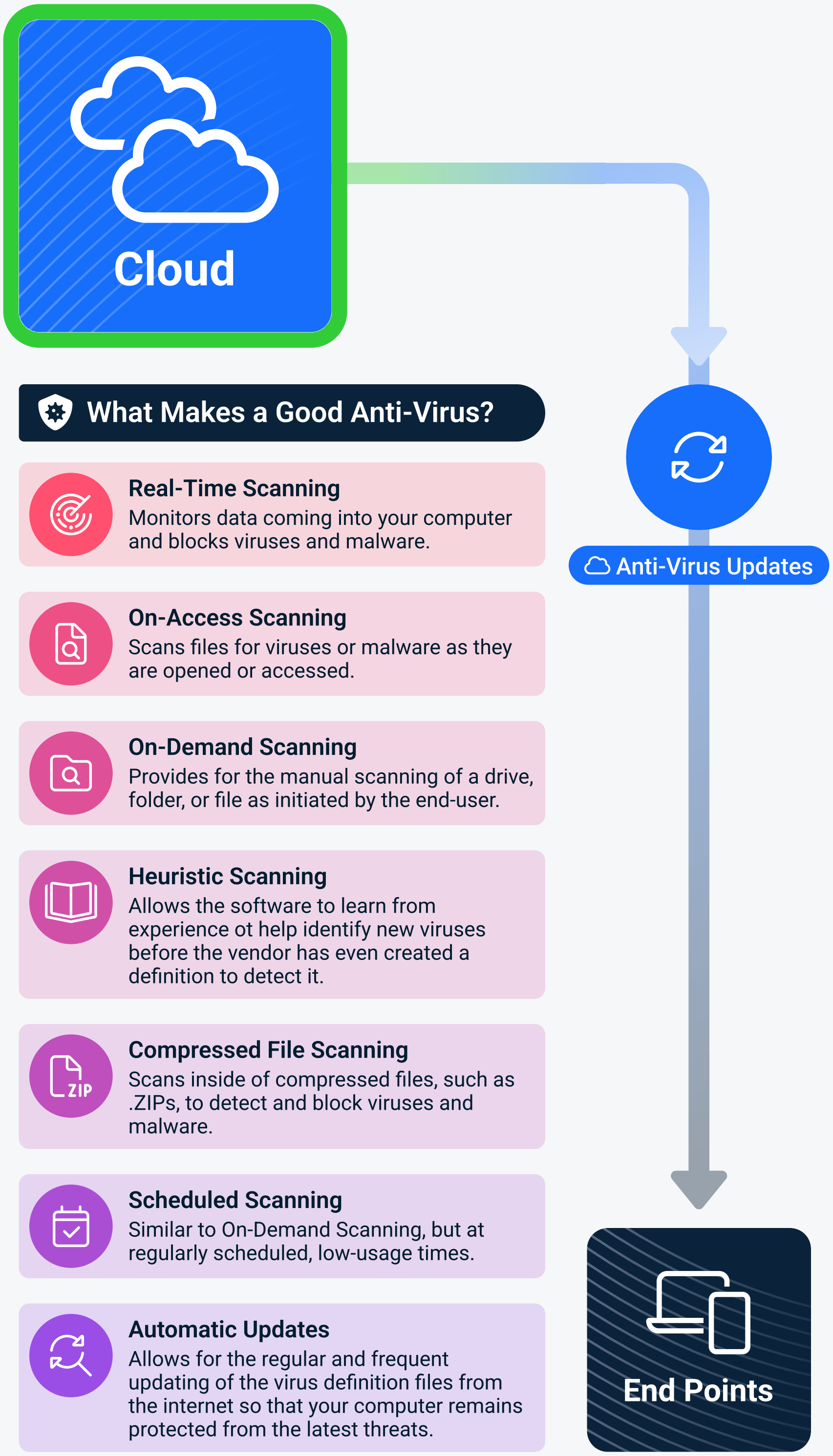
7%

of all corporate laptops will be **lost or stolen** sometime during their useful life.

Cyberattack Risk



Anti-Virus



What Makes a Good Anti-Virus?

Real-Time Scanning
Monitors data coming into your computer and blocks viruses and malware.

On-Access Scanning
Scans files for viruses or malware as they are opened or accessed.

On-Demand Scanning
Provides for the manual scanning of a drive, folder, or file as initiated by the end-user.

Heuristic Scanning
Allows the software to learn from experience ot help identify new viruses before the vendor has even created a definition to detect it.

Compressed File Scanning
Scans inside of compressed files, such as .ZIPs, to detect and block viruses and malware.

Scheduled Scanning
Similar to On-Demand Scanning, but at regularly scheduled, low-usage times.

Automatic Updates
Allows for the regular and frequent updating of the virus definition files from the internet so that your computer remains protected from the latest threats.

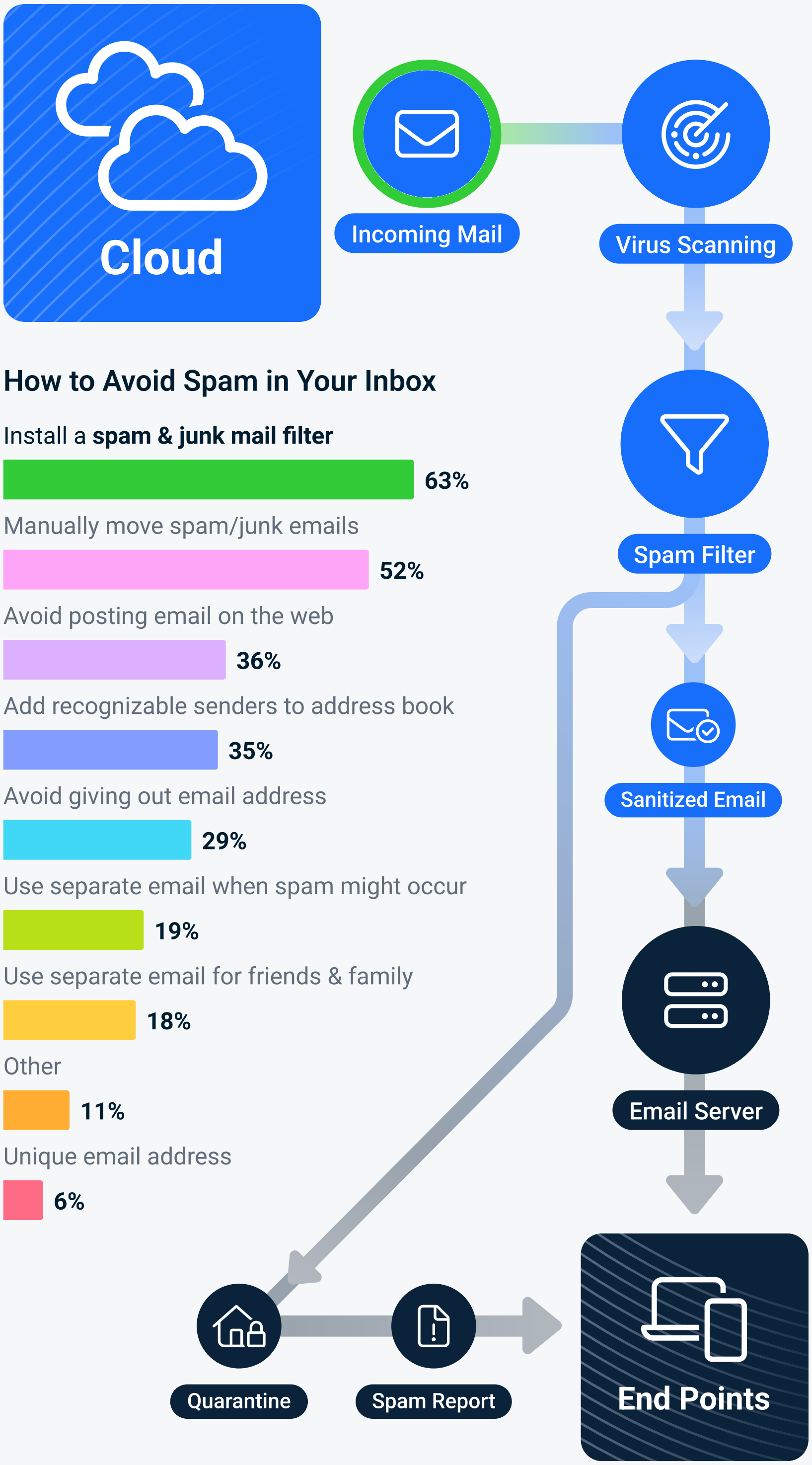
Why is this Important?

It goes without saying that every endpoint on a network should be protected with up-to-date **Anti-Virus software**. When a security threat or malware breaches all the other layers of protection, this is the last line of defense. The anti-virus software should be centrally managed and monitored with automatic updates and license renewal. It should also provide thorough protection without weighing down the system that it is protecting. When choosing a vendor, be sure to read the ratings published by an independent anti-virus testing lab such as ICSA or West Coast Labs.

Cyberattack Risk

⬜	⬜	⬜
⬜	🟩	⬜
⬜	⬜	⬜

Anti-Spam & Virus Filter


Cloud
Incoming Mail
Virus Scanning
Spam Filter
Sanitized Email
Email Server
End Points
Quarantine
Spam Report

How to Avoid Spam in Your Inbox

Install a **spam & junk mail filter**
63%
Manually move spam/junk emails
52%
Avoid posting email on the web
36%
Add recognizable senders to address book
35%
Avoid giving out email address
29%
Use separate email when spam might occur
19%
Use separate email for friends & family
18%
Other
11%
Unique email address
6%

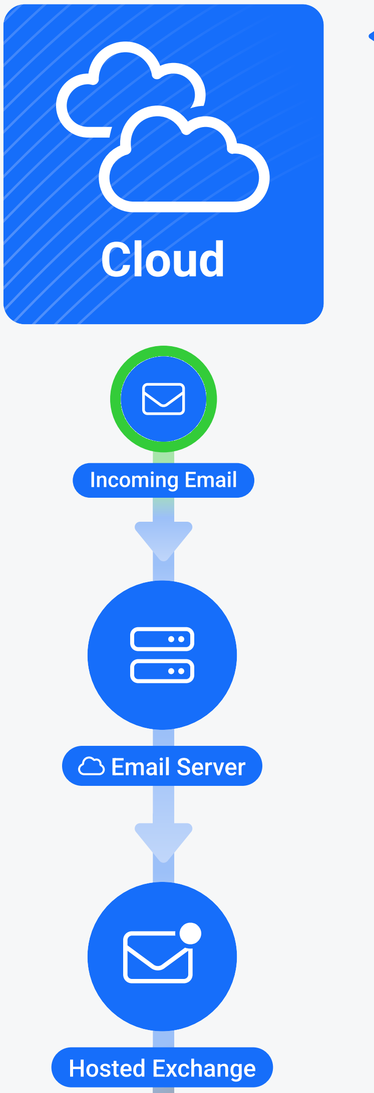
Why is this Important?

One of the main ways viruses and other malware infiltrate a network is through email. With so much riding on the high availability of an electronic communication system, **it is important to add a 3rd party layer of filtered protection**. Most filters will allow for the simple release of quarantined messages and include a daily report of held email for review. You should consider a filter separate from your email server or hosted provider. That way, if there is any type of outage and email can't be delivered, your anti-spam filter will hold the messages and deliver them when the server becomes available.

Did You Know?

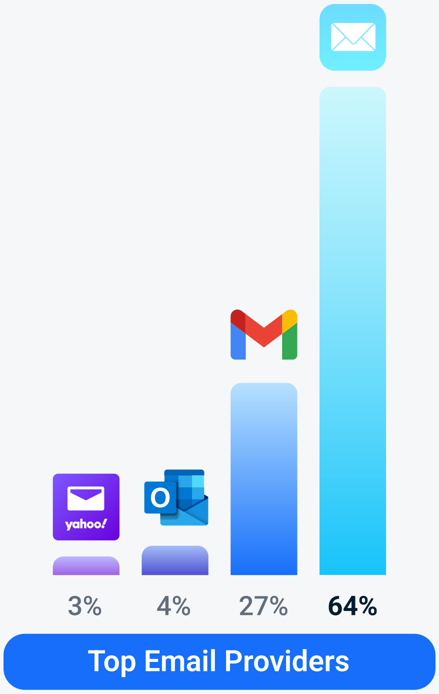
Since 2001, the threat landscape has dramatically changed from unorganized, electronic vandalism to funded, organized theft of personal data, intellectual property and financial information. Protection against these threats begins with modern software and workstations running the latest operating system. Today, many offices allow employees to bring their own devices to the office. While this increases flexibility and productivity and helps lower costs, it also makes your data more vulnerable to attack. Proactively managing all endpoints and ensuring that they are up to date and supported is of paramount importance to your IT infrastructure.

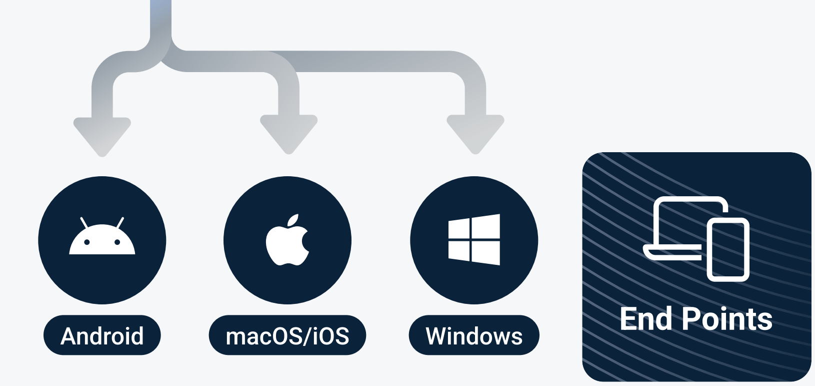
Hosted Exchange



What is Hosted Exchange?

Hosted Exchange is a service provided by Microsoft or another 3rd party vendor whereby email mailboxes are provisioned on servers in the cloud. The servers provide the service & storage, while being maintained, backed up, and protected by the provider. Customers can access the mailboxes and work collaboratively using a variety of applications across a multitude of platforms.





Why is this Important?

Rich in efficiency and effectiveness, email has become the number one communication tool in the business world. With so much riding on the ability to communicate with employees, customers, and vendors, it is extremely important that email remain highly available at all times. Moving the email server(s) from inside the office or away from older POP3 accounts to a cloud-hosted platform such as **Hosted Exchange** or **Exchange Online** not only improves reliability but it greatly increases security. Using cloud Hosted Exchange will ensure you can access email from any device with an internet connection.

Did You Know?

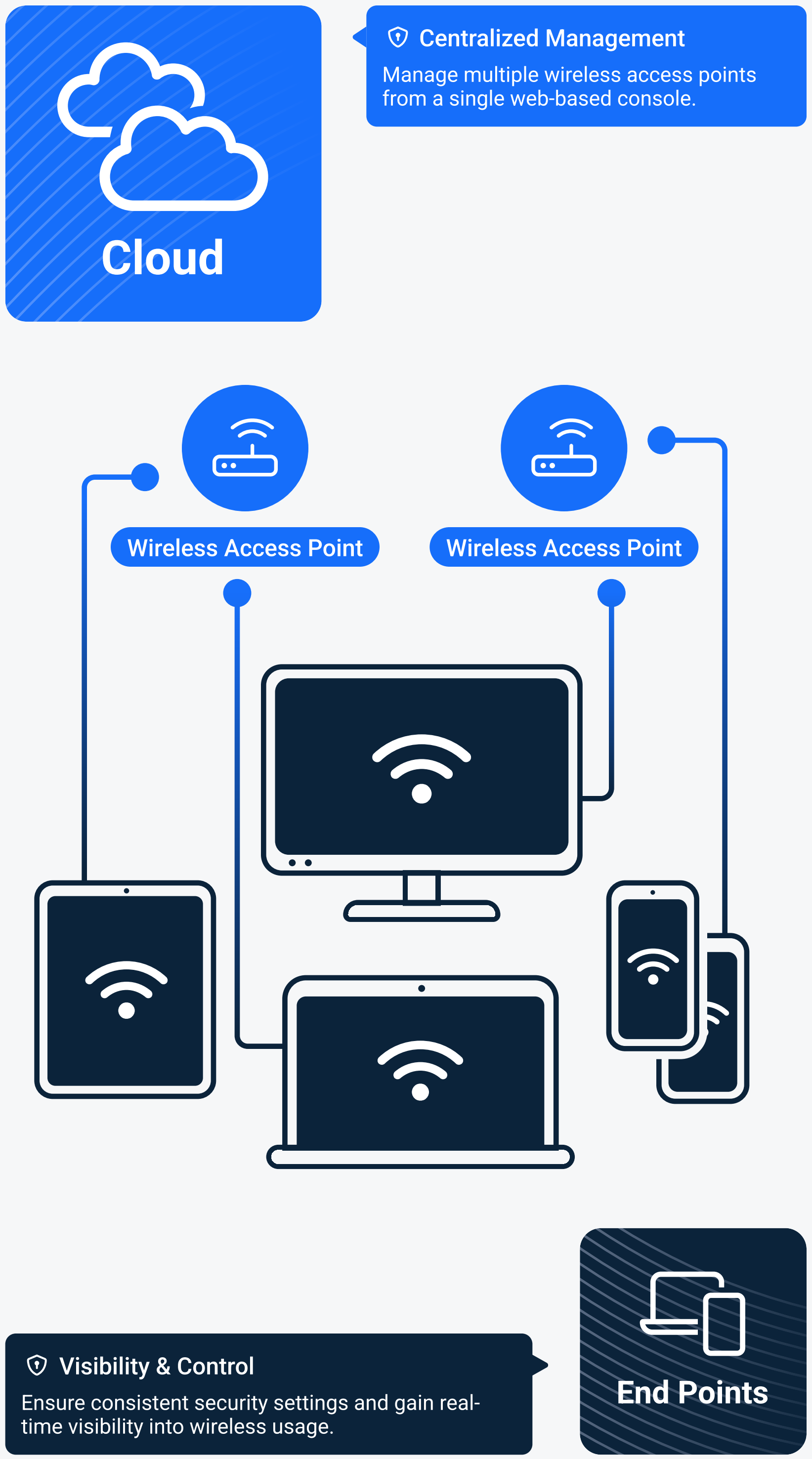
84%

of a company's intellectual property **passes through their email platform**

112

emails sent and received **per day** by the average corporate employee

Managed Wireless



Centralized Management

Manage multiple wireless access points from a single web-based console.

Visibility & Control

Ensure consistent security settings and gain real-time visibility into wireless usage.

Why is this Important?

Wi-fi has quickly become a necessity for most businesses. As more and more smartphones and tablets are brought into the office, it's now an expectation that wireless access be available. To improve security, many businesses provide a separate wireless guest network for their partners and visitors. Nonetheless, wireless is inherently less secure because it doesn't require a physical connection. Special security considerations need to be made when configuring and providing Wi-fi and the devices being utilized should be managed and monitored for threats and bandwidth consumption.

E&O Insurance

Essential Coverage

Client Data Loss
Covers the costs of recovering or restoring lost data in the event of a disaster or deletion.

Network Security Liability
Covers the inadvertent transmission of a virus or the failure to prevent unauthorized access to computer systems by a third party or unauthorized employee.

Breach of Contract
Covers the costs related to your IT provider's failure to fulfill their contractual obligations.

Independent Contractors
Covers any independent contractors that your IT provider may utilize while performing their duties and services.

Additional Cyber Liability Coverage

Privacy Liability
Covers the disclosure or misuse of Protected Health Information and Personal Identifying Information.

Privacy Breach Notification Costs
Covers the costs to provide notification to the individuals who are required to be notified by the applicable Breach Notification Law.

Forensic Expense Coverage
Covers the costs to hire a computer security expert to determine the existence and cause of any electronic data breach.

Crisis Management Expense
Covers the costs of a public relations consultancy for the purpose of averting or mitigating material damage.

Regulatory Defense/Penalties Coverage
Covers the claims expenses and penalties which you are legally obligated to pay because of any claim in the form of a regulatory proceeding resulting from a violation of a Privacy Law.

You should consider your own Cyber Liability policy to protect yourself from a rogue employee, staff errors, and lost or stolen unencrypted laptops and mobile devices.

Why is this Important?

Unlike other regulated industries, there's nothing that requires your IT provider to purchase coverage for **Errors & Omissions (E&O)** or other forms of cyber liability insurance. You should make sure that your IT provider has adequate coverage for the services that they provide or your business could be exposed to serious risk without any ability to seek reasonable financial restitution. Without E&O insurance containing the proper coverages. most IT providers lack the financial resources to absorb heavy losses from lawsuits and the costs to defend them. If you're unsure if you're protected, ask your IT provider for a Certificate of Insurance for their Cyber Liability E&O policy.

Did You Know...?

Errors & Omissions insurance, otherwise known as Professional Liability Insurance, is often overlooked by IT providers. Although there is no standard form, E&O insurance protects your IT provider from claims of professional negligence or failure to perform their professional duties. These could include loss of your data, software or system failure, claims of non-performance or the negligent oversell of products or services. It's important to note that these types of claims are NOT covered by General Liability insurance.

Employee Productivity Monitoring

Employee Monitoring Software gives small business owners and managers insight into how employees spend their time at work. The best software can monitor the following:

Internet Monitoring
These tools track employees' browsing history and bookmarks, including time spent on social media.

Email Monitoring
Corporate email addresses gives employers access to their employees' emails, both sent and received.

Keyword Tracking
Bossware tools that let employers define and then track specific keywords being typed on company devices.

Screenshots of Computer Screens
Tools that automatically take screenshots of whatever is on employees' screens every five or ten minutes.

Live Video Feeds and Playback
Bossware gives employers to access and watch a live stream of their employees' screens or watch recorded playbacks.

Remote Desktop Control
Often used by IT departments to help with tech issues, these tools allow employers to take remote control of any employees' desktop.

Webcams and Microphones
Software that allows employers to secretly activate inbuilt webcams and microphones on employee devices.

Keystroke Logging
Tools that track everything employees type in web browsers, emails and documents, and can be used to monitor conversations.

Activity Trackers
Company-provided activity trackers, like smart watches & wristbands, that monitor sleep, exercising routines, and more.

Smart ID Badges
Smart ID badges equipped with tiny microphones that record what employees say in meetings and how often they're away from their desks.

Why is this Important?

When the pandemic forced companies to close their offices, the result was an increase in remote work & work-from-home. To protect company data, and to ensure employees remained engaged and productive while working from home, many employers resorted to using **Employee Monitoring Software**. Employee productivity is a concern of organizations today, especially in the form of lost productivity in the workplace. Employees will misuse their privileges causing lost productivity for the company and deadlines not being met. Now it is necessary for businesses to take advantage of employee monitoring software.

Did You Know...?

1 in 5

businesses are now using apps and programs on employees' devices to **track their online activities** or have plan to do so in the future.

Businessnewsdaily.com - 2020

62%

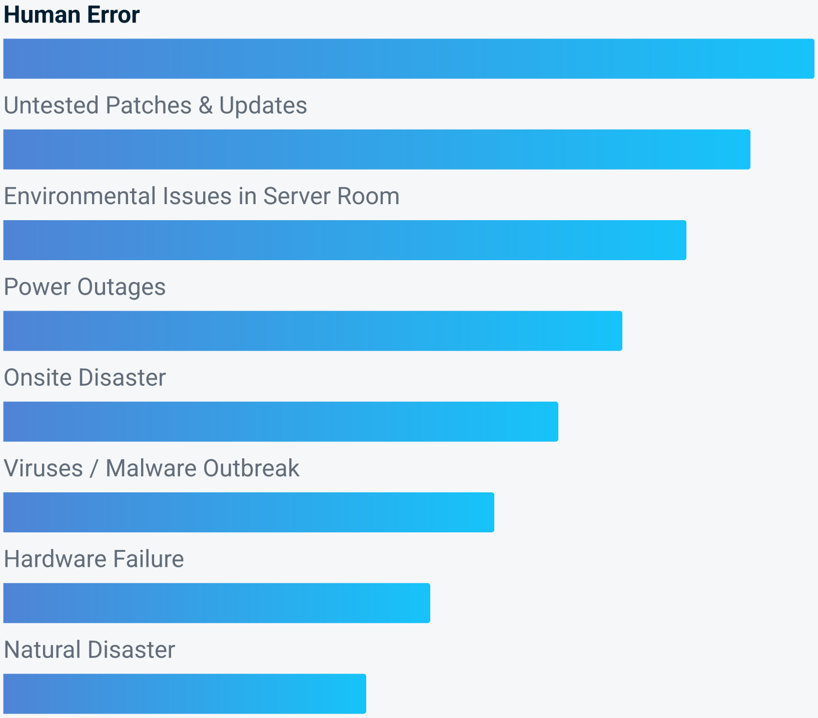
of executives said their companies use software to collect data on their people for insights into productivity, innovation, and business agility.

hbr.com - 2020

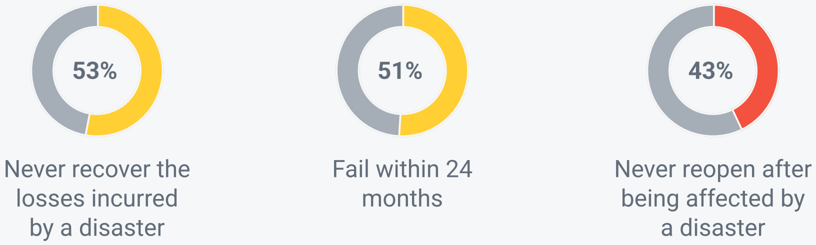
Business Continuity

Without a proper plan, any disruption to critical systems, physical locations or other key resources can impact customers & harm the financials of an organization. It's essential for organizations to discuss how an unplanned outage would impact their business and to plan how they need to respond effectively.

Most Common Causes of System Downtime



Businesses WITHOUT a Business Continuity Plan



Why is this Important?

There is a big difference between **Business Continuity** and Backup & Disaster Recovery. Business Continuity plans help ensure that a business can continue its operation in the event of a natural or man-made disaster. Don't do what 83% of other businesses do and begin planning during a disaster. Be prepared and remember that the best plan is one that works in a variety of scenarios and requires a minimum of change during and after a disaster. With ever-increasing cloud computing options, business continuity has become more affordable and easier to implement.

Backup Disaster & Recovery is **reactive**, while Business Continuity is **preventative**.

Did You Know...?

48%

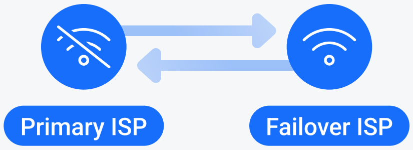
of business owners have **no business continuity plan in place**.

84%

of companies experienced one or more instances of **system downtime** in the previous 12 months.

Square - 2020

Internet Security Appliance

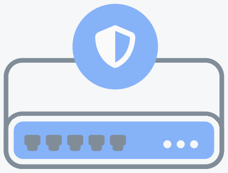


ISP Load Balancing is a method of monitoring several internet circuits and switching between them in the case of a failure. This increases uptime and provides better availability of cloud services.

A **Virtual Private Network (VPN)** allows for the secure transmission of data from the internal network to endpoints, such as **laptops, remote locations, and cloud storage**.

Features of a Strong Internet Security Appliance

- Gateway Anti-Virus & Anti-Spyware
- Content Filtering
- Intrusion Prevention & Detection System
- Application Layer Filtering
- Reporting



A network firewall is a **hardware-based device** that acts as a physical layer between the internet-based cloud and protects the internal network from unwanted traffic. It actively blocks traffic that matches predetermined security rules but doesn't inspect anything inside the packets.

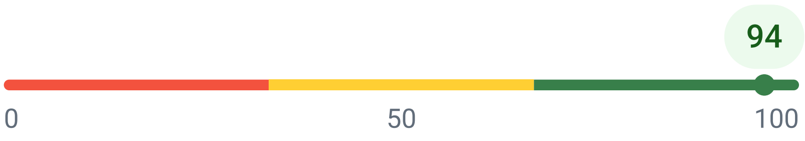
Why is this Important?

An network firewall, or **Internet Security Appliance**, is the first line of defense when protecting your network and data from internet-borne threats and outside attackers. The hardware provided by an Internet Service Provider (ISP) or a residential-grade router is not enough to effectively protect a business. Implementing a monitored appliance with Unified Threat Management security services activated and up to date is a great start towards ensuring that critical data is protected. If you don't have an Internet Security Appliance, **your business is exposed to a myriad of risks**.

Did You Know?

Many Internet Security Appliances are enhanced with Unified Threat Management and combine other security features with those of the firewall. This provides for a simple solution which is easier to manage and may help meet complex regulatory compliance requirements.

Audit Score



Infrastructure

🟩🟩🟩
🟩🟩🟩
🟩🟨🟩

Security

🟩🟩🟩
🟩🟩🟩
🟩🟩🟩

Managed Support & Services

🟨🟩🟩
🟩🟩🟨
🟩🟨🟨

Telecommunications

🟩🟩🟩
🟩🟩🟩
🟩🟩🟩

PCI Compliance

🟩🟩🟩
🟩🟩🟩
🟩🟩🟩

Cyberattack Risk

🟩🟩🟩
🟩🟩🟥
🟩🟩🟩

Microsoft Cloud

🟩🟨🟨
🟩🟩🟩
🟩🟩🟩

🟥 Requires Immediate Attention 🟨 Needs Improvement 🟩 Satisfactory

Proposed Plan Summary

The results of each category of your base plan audit is summarized here using color-coded boxes. Utilizing a weighted scoring system, the results were combined and averaged into an overall audit score. Individual category scores and details for each audit item are shown in subsequent pages. Your base monthly IT expense is shown as a range and has been converted into effective IT monthly expense based upon your audit score. This helps to level the playing field when comparing plans.

Financial Summary

Monthly IT Expense

$3,300 - $3,300

$0 $15,000

Effective Monthly IT Expense

$3,510 - $3,510

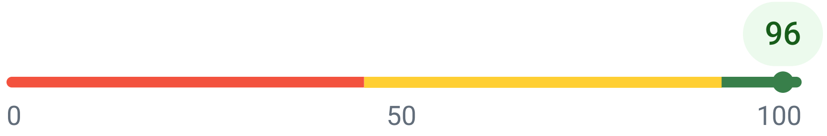
$0 $15,000

One-time Cost

$5,000

$0 $15,000

Infrastructure



Infrastructure is the foundation upon which all of your technology rests. Just like with a house, it's extremely important to verify its integrity before you begin to build on top of it. Poor initial design decisions can lead to downtime, lost sales and ultimately drive up your total cost of ownership. This detailed analysis page represents an overview of the state of your Base Plan Infrastructure. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Infrastructure audit score. easy identification and the results for this section are reflected in the Infrastructure audit score.

Business Continuity

Business Continuity is always on and business can be conducted from remote, alternate locations.

Server

There are no servers onsite.

Backup & Disaster Recovery

There is no data located locally so there is no need for local backups with replication.

Remote Accessibility

Key employees have cloud access to critical files and applications and can work remotely with minimal disruption.

Cloud to Cloud Backup

All critical SAAS applications are currently being backed up.

Disaster Recovery Plan

There is a structured Disaster Recovery plan in place with periodic updates and a full annual test.

High Availability

There is a redundant platform implemented to provide high-availability access to a hosted site in the event of a local outage

Data Compliance

The office has met some of the Regulatory Compliance requirements from HIPAA or FINRA.

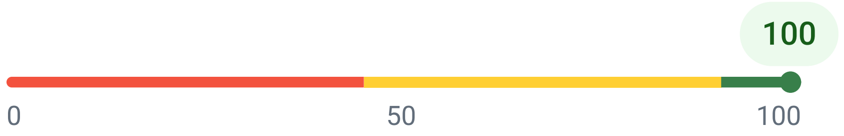
Workstations

The workstations are within 3 years old, under warranty and running a supported operating system.

Baseline Plan

Category Details

Security



Security is arguably the most important section of your audit report. With so much riding on the security of your infrastructure, you can't afford to have any deficiencies. Fortunately, there's an abundance of security solutions available to help mitigate the risks and protect your data. This detailed analysis page represents an overview of the state of your Base Plan Security. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Security audit score.

Security Awareness Training

Solution has been implemented and deployed to all customers with reporting automation included.

Endpoint Encryption

Endpoint Encryption has been added on all local devices.

Managed SOC

Managed SOC solution has been implemented to all endpoints and actively being monitored by outsourced team.

Dark Web Monitoring

A Dark Web Monitoring solution has been implemented to the entire customer base.

Managed DNS

There is managed DNS with a 3rd party provider and security and content filtering are in place..

Next Generation Endpoint Protection

Replaces legacy anti virus and anti spam filtering.

Application Whitelisting

Only permitted applications may run on the environment.

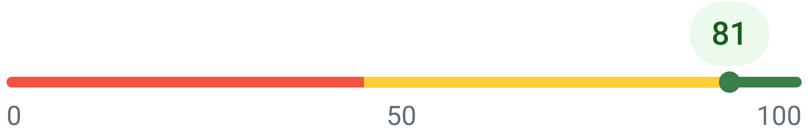
Anti-Phishing

Anti-phishing solution has been installed and implemented across the entire customer base.

Content Filtering

Content filtering has been enabled across all users and devices to mitigate the risk of infection from suspicious websites.

Managed Support & Services



Managed Support & Services is the customized/user defined category as per business need.

Onsite Support

Onsite Support is billed against blocks of hours at a discounted rate.

Help Desk Support

Remote Help Desk Support is included for all supported endpoints and services.

Monitoring

Monitoring of server(s) and workstations is automated with scripted remediation and included in the plan.

Inventory & Asset Management

Inventory & Asset Management is automated, included at no additional cost and reviewed quarterly.

Windows & Application Updates

Windows updates on server(s) and workstations are automated and up to date.

Virtual CIO Services

vCIO services such as budgeting and IT planning are provided at an hourly rate.

Proactive Maintenance

Proactive maintenance of server(s) and workstations is automated and included in the plan.

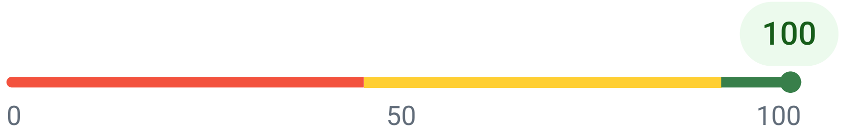
Mobile Device Management

Mobile device management (MDM) is in place for some but not all smartphones with email accounts configured.

Vendor Management

Vendor Management is billed hourly for all vendors with a valid support contract.

Telecommunications



Telecommunications is one of the fastest evolving areas of technology. Traditionally viewed as a separate cost center, the proliferation of voice over IP (VoIP) solutions has helped many businesses save more money while greatly improving upon their business continuity. This detailed analysis page represents an overview of the state of your Base Plan Telecommunications. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Telecommunications audit score.

Unified Communications

Application needed to integrate phones with (Salesforce, Teams, etc.) is present.

Enterprise Feature Set

Although there are only physical phones on premise, the VoIP platform contains the same features as an enterprise phone system.

Transcription

Voicemail can be sent via email with transcription.

Telephony Continuity

The VoIP phone service will continue to route calls to other unified communication devices even if the internet is down or the power is out.

Multi-Site Coordination

The VoIP phone system can be easily expanded by placing additional phones in alternate locations where internet access is available.

Future Proof Scalability

Satisfactory

Portability

The current phone system and phone numbers can be relocated anywhere there is internet service.

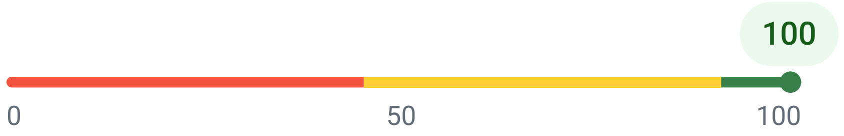
Ongoing Maintenance Fees

There are no ongoing maintenance fees associated with the current phone system.

Fixed Fee Billing

The phone bill is driven by fixed fee billing and unlimited calling.

PCI Compliance



Payment Card Industry (PCI) compliance is a set of regulations developed to ensure that the credit card industry is properly managing and securing customer data. Before it was formed in 2006, there was no clear industry standard that all credit card companies had to follow, and that's a problem for any company that deals with big data. This detailed analysis page represents an overview of the state of your PCI Compliance. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the PCI Compliance audit score.
has context menu

Annual PCI SAQ

The Annual PCI SAQ has been completed with the assistance of IT provider.

Credit Card Fee Recoupment

The customer is now passing along fees to recoup additional charges to increase revenue.

Credit Card Fees

The processing fees are now in line with industry standards or below industry standards.

EMV Chip Acceptance

PCI compliant devices have been installed with the latest security standards.

Payment Software Integration

The business has their current line of business applications integrated with their payment software.

PCI DSS Compliance

The customer is now compliant in accordance to the PCI Standards Council.

Point to Point Encryption

P2PE is utilized to ensure secure transfer of cardholder information.

Secure Payment Gateway

The customer has implemented a new secure payment gateway.

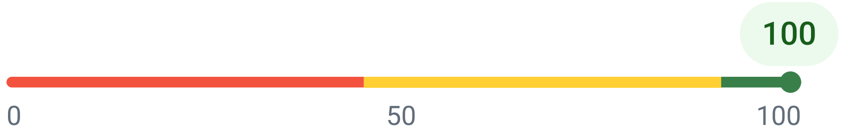
Tokenization

Tokenization is being utilized when transactions occur.

Baseline Plan

Category Details

Cyberattack Risk



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc vulputate libero et velit interdum, ac aliquet odio mattis. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur tempus urna at turpis condimentum lobortis.

Password Policy

Password policy enforces regular password rotation every 90 days to protect accounts and data.

Password Management

Password management software is in place, ensuring secure and efficient handling of user credentials and enhancing overall security.

Dark Web Monitoring

Dark web monitoring is actively used to protect against threats, ensuring early detection of compromised data and enhanced security.

Endpoint Encryption

BitLocker encryption is enabled, ensuring protection for data by securely encrypting drives and preventing unauthorized access.

Anti-Virus

Anti-Virus is corporately managed by a cloud based subscription and all endpoints are up to date.

Data Encryption Policy

Sensitive data was detected, requiring immediate action to secure and protect the information from potential exposure.

Data Compliance

Data encryption policy is active, ensuring sensitive information remains secure and protected across all platforms.

Vulnerability Management

Proactive vulnerability management enhances security posture by identifying and addressing risks, ensuring a safer environment.

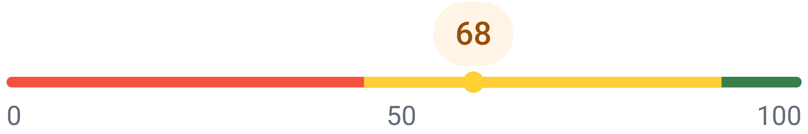
Content Filtering

Content filtering is enabled to ensure a safe and secure environment by blocking harmful or inappropriate content.

Baseline Plan

Category Details

Microsoft Cloud



The Microsoft Cloud is an open cloud platform made up of products and solutions that empower organizations to thrive in a changing world. It offers a variety of tools to help businesses manage challenges and meet their goals, drive value faster, and build for the future. It also helps protect and defend your business with security, compliance, identity, and management solutions that work across all your platforms, clouds, and apps.

Cloud Storage

Microsoft Cloud offers flexible storage solutions, empowering users with secure, scalable options to efficiently manage and protect their data.

Admin Role Overlap

Admin Role Overlap in Microsoft Cloud leads to excessive access permissions, increasing security risks and complicating role management.

Third Party Applications

Blocking Chrome from allowing third-party cookies disrupts user experience, causing issues with website functionality and personalized content.

Azure Site Recovery (ASR)

Azure Site Recovery rules are effectively configured, ensuring robust protection against malware and enhancing overall system security.

Microsoft Defender

Defender Antivirus is enabled, ensuring robust protection against threats and enhancing the overall security of our systems.

Data Loss Prevention

DLP policies are enabled, ensuring sensitive data is protected against leaks and unauthorized access for enhanced security.

Endpoint Detection & Response (EDR)

EDR Block Mode is enabled, enhancing security by proactively preventing threats from executing, ensuring robust protection for our systems.

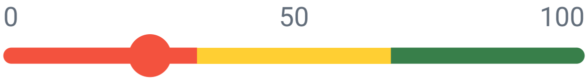
Virtual Meeting Software

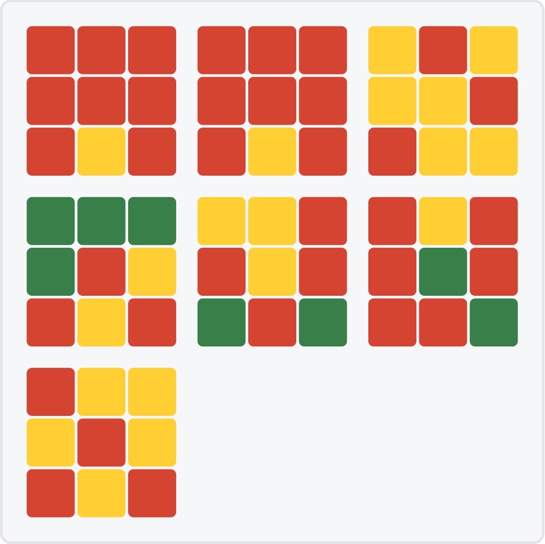
Lobbies for Meetings in Microsoft Teams has been enabled, ensuring participants are verified before joining, fostering a safe environment.

Transport Layer Security (TLS)

TLS versions are up to date strengthening security, ensuring encrypted communications are protecting sensitive data effectively.

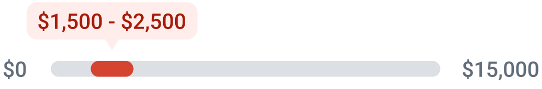
Baseline Plan 22



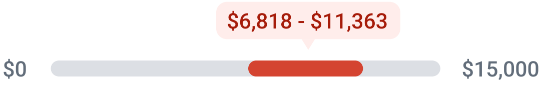


Financial Summary

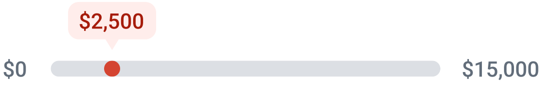
Monthly IT Expense



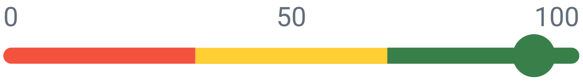
Effective Monthly IT Expense

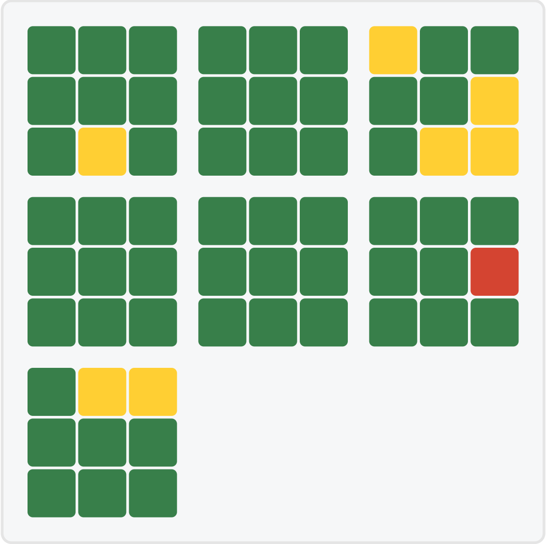


One-time Cost



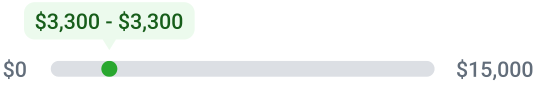
Proposed Plan 94



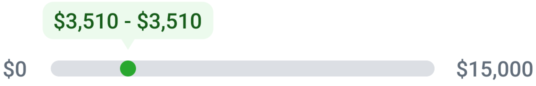


Financial Summary

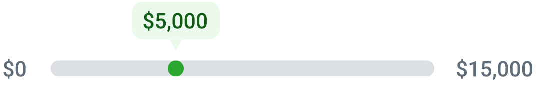
Monthly IT Expense



Effective Monthly IT Expense



One-time Cost


$5,000
$0
$15,000