totalsolutions
MAKING I.T. EASY

Managed Service Agreement

Total Solutions Way 2027
City of Oneida

Start Date: January 1, 2027

TS Managed Services	Foundation
Unlimited Remote & On-site Support	✓
Account Manager/Technical Alignment	✓
Proactive Monitoring	✓
OS Patch Management	✓
Third-Party Vendor Liaison	✓
M365 Tenant Management & Support	✓
Remote Access & Work from Home – *Ninja Remote*	✓
Endpoint Detection & Response (EDR/MDR) with 24/7 Managed SOC - *Huntress*	✓
Identity Threat Detection & Response – M365 (ITDR) - *Huntress*	✓
Managed Backup (Servers) – *Cove Data Protection*	✓
Managed Backup (Critical Workstations) – *Cove Data Protection*	✓
3 Year ($65 per seat for 107 seats): ***Adjusted Quarterl** **Cybersecurity Awareness Training:**	**$6,955.00/mo.*** ~~**$1,200.00/mo.**~~ **Complimentary**

Table of Contents

TS Managed Services 2
Table of Contents 3
Managed Services Requirements 4
Agreement 5
Terms and Conditions 7
Managed Services 13

Managed Services Requirements

1. Client's PCs (laptops/desktops/Macs), servers and network equipment including routers, switches, backup devices and media must be less than 5 years old or turning 5 years old in the first 11 months of the agreement. Servers must be replaced by clients upon reaching the age of 5 years. Equipment may be retained beyond 5 years with TS approval. Labor to replace PCs is included in service agreement. Labor to replace server(s) will be processed as a project and costs billed outside the monthly service amount at TS' then hourly rate or flat-rate. Servers must be covered by an active hardware warranty. TS will coordinate warranty diagnostics, repairs and return to service.
2. PCs in excess of 5 years in age that fail will need to be replaced by the client with a new machine or one that is less than 5 years in age.
3. All servers and PCs with Microsoft Windows or Apple operating systems must be running an operating system supported by Microsoft or Apple with support expected to continue 12 months or more with the latest service packs and critical updates installed. As Microsoft or Apple stops supporting an operating system, client must update their operating system or remove it from any access to the network.
4. Client will maintain service/support contracts for hardware such as servers, routers, firewalls, switches, and specialty software applications.
5. If a client has software particular to its business which is installed on its network, the client is responsible for installation, training and continuing technical support from the software provider. TS technicians will assist with network support, but they are not experts in all software applications and rely on the software manufacturer to provide software support at client's expense.
6. All server and desktop software must be genuine, licensed, and vendor supported.
7. The network must have a currently licensed, vendor-supported hardware firewall between the internal network and the Internet.
8. Client will NOT allow third-party vendors access to the environment without approval and/or monitoring by TS.
9. All wireless data traffic in the environment must be securely encrypted.
10. The client shall make available to TS all information, facilities and services reasonably required by TS to enable it to perform the Managed Services and cooperate with TS's personnel in the diagnosis, investigation and correction of any fault in the software and/or equipment provided by TS.
11. The client must designate which employee(s) are authorized to make changes to the account, request password modifications for themselves or other users.

Agreement

Client and TS agree to the following:

- TS will provide the Managed Services set forth above. The term of this Agreement is 12 months and is based upon the assets the Client has in place at the time this MSA is executed. This Agreement will automatically renew monthly unless at least 30 days prior to the expiration of each such term, either party notifies the other party in writing of non-renewal. TS or Client may terminate this contract at any time, after an initial 12-month period with at least 30 days prior written notice.

- Client agrees to all requirements as set forth above.

- Client will pay TS monthly on or before the 1st day of each month the amount of **$6,955.00.** TS does not have a site visit charge. If the client is in a jurisdiction which charges sales tax on services, the stated price does not include tax.

- TS' current hourly rate for additional services is **$150/hour**; this may be subject to change. TS will provide client with notice of any change in hourly rate 30 days prior to rates becoming effective.

- The addition of locations, IT assets, services, or service hours not set out in this agreement or requested services which are not part of the Managed Services will be billed as "Additional Services" and billed at the standard hourly rate, as a Project and will be billed pursuant to a separate agreement between the parties or through an adjustment to the Client's monthly charges.

- Client may elect for TS to provide Hardware as a Service (HaaS) whereby TS provides a particular device for the Client's use. Should the Client elect HaaS, it will be subject to the execution of an addendum to this MSA and billed as an Additional Service on the Client's monthly invoice.

- The cost of any equipment necessary to perform the Additional Services or Project will be paid by the Client prior to installation. The estimated charges for Projects and Additional Services will be paid in full prior to the commencement of the applicable work. Client agrees to make payment in full within 30 days of billing for Additional Services not anticipated in the initial estimated charges, plus incurred expenses.

- Client acknowledges and agrees that this Agreement grants Client no title or right of ownership in or to the Managed Services, or any component thereof, or to any associated materials including, but not limited to any documentation, including, but not limited to, all user manuals and other documentation supplied by TS to Client whether provided in electronic form or otherwise, including training manuals, program listings, data models, flow charts, logic diagrams, functional specifications, instructions, etc., or intellectual property. Client shall not, at any time, take or cause any action, which would be inconsistent with or tend to impair the rights of TS or its licensors.

- Ownership of material data for the Managed Services shall remain with the Client. Such data includes Client's corporate data, including, but not limited to, registration data, supplied and input by or on behalf of Client ("Client Data"). TS agrees not to use any Client Data for any purpose

other than to perform the Managed Services and fulfill its obligations under this Agreement. TS further agrees not to make Client Data available to any third party without Client's prior written consent, unless required to do so to perform the Managed Services set forth herein. However, in performance of the Managed Services, it is possible that data files on magnetic media may be destroyed. TS will take commercially reasonable precautions to avoid destruction of data, but will not be held responsible in the event that such destruction occurs except in the case of gross negligence on the part of TS.

- TS will begin and maintain network documentation: on-going documentation of hardware, software, network settings, IP addresses, firewall settings and related network information.

- Client will comply with the Terms and Conditions and the Managed Services Requirements.

This Agreement includes the Managed Services Components, Managed Services Requirements and also the Terms and Conditions; these documents are incorporated herein by reference.

TS and the Client have executed or caused this Agreement to be duly executed by their authorized representative as of the date set forth below.

City of Oneida

Print: Kyle Lovell

Sign: _____ Date: _____

Address: 109 N. Main St, Oneida, NY 13421

Total Solutions I.T., Inc.

Print: Michael Morrill

Sign: _____ Date: _____

Address: 9085 Old River Rd, Marcy, NY 13403

Terms and Conditions

1. Confidentiality during the term of this Agreement, and thereafter in perpetuity, neither party shall, without the prior written consent of the other, disclose to anyone any Confidential Information of the other. "Confidential Information" for the purposes of this Agreement shall include each party's proprietary and confidential information such as, but not limited to, customer lists, business plans, marketing plans, financial information, designs, drawing, specifications, models, software, source codes, and object codes. Confidential Information shall not include any information that Client makes publicly available or information which becomes publicly available through no act of TS or Client or is rightfully received by either party from a third party provided as part of these requests.

2. Client and TS both agree that they will not solicit for hire and will not hire or otherwise engage any of each other's employees or contractors, either directly or indirectly during the period that Managed Services are being provided under this agreement or in the 24-month period immediately following termination of this Agreement.

3. Force Majeure: Neither party shall be liable for any failure of or delay in performance of its obligations under this Agreement to the extent such failure or delay is due to circumstances beyond its reasonable control, including, without limitation, acts of God, acts of a public enemy, pandemics, fires, floods, wars, civil disturbances, sabotage, accidents, insurrections, terrorism, blockades, tariffs, embargoes, storms, explosions, labor disputes (whether or not the employees' demands are reasonable and within the party's power to satisfy), acts of any governmental body, failure or delay of third parties or governmental bodies from whom approvals, authorizations, licenses, franchises or permits must be obtained, or inability to obtain labor, materials, equipment, or transportation or illness of TS' technical staff (collectively referred to herein as "Force Majeure"). Each party shall use reasonable efforts to minimize the duration and consequences of any failure of or delay in performance resulting from a Force Majeure event. Notwithstanding the foregoing, a Force Majeure event shall not delay the Client's payment obligations set forth in the Agreement.

4. If the Client work is substantially changed due to a Force Majeure, TS will evaluate the need for change to IT services to Client and related change of managed service fees, as well as any other services provided to the Client including Hardware as a Service (HAAS), including any necessary fee increase(s). Recognizing there are ongoing expenses to TS for maintaining backups, remote monitoring, other vendor support software/licensing and availability of technicians to service on going needs, TS will review with Client the need for a modification of fees if any. Late fees will not be charged under an agreed scenario below:
    a. A flat fee charge per month. If the change is a flat fee per month, then billing will resume upon Client's resumption of services as mutually agreed between TS and Client. This may be an evaluation between the parties of a gradual resumption of workers and network activity or an immediate resumption of workers and network activity.
    b. Deferred billing by 50% over 3 months. Then beginning after 3 months the deferred amount to be added back in subsequent months by 25% of deferred amount or as mutually agreed.

5. TS shall not be liable to Client or any of its affiliates for any damages, whether incidental, direct, indirect, special, consequential or punitive damages arising out of or related to the Managed

Services or equipment provided hereunder, including but not limited to loss of profits or revenue, loss of use of equipment, lost data, or loss to person or property, costs of substitute equipment or other costs even if TS has been advised of the possibility of such damages. Regardless of the form of action, TS' cumulative liability shall be only for loss or damage directly attributable to negligence of a TS employee or contractor, for the cost of restoring the network to its condition prior to the negligence, but in no event shall such liability exceed thirty thousand dollars ($30,000.00). If a collection action is initiated by either party or if TS has to defend any action by Client, TS shall be entitled to its reasonable attorney fees and expenses to be paid by Client.

6. EXCEPT AS STATED HEREIN, ALL GUARANTEES, WARRANTIES, CONDITIONS AND REPRESENTATIONS, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMTED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSLY EXCLUDED. A TS contractor is a technician or contractor who is authorized by and operates on behalf of TS, is paid by TS and has access to TS' service ticket management system for making time entries and charges for their work. TS is not responsible for the acts of other technicians, contractors or consultants providing service to Client not under its control and direction. If Client purchases equipment from TS, it understands and agrees that it will look to the manufacturer for all remedies and warranties and agrees that TS is not responsible for functioning of the equipment and has not made any express or implied warranties regarding the equipment. TS shall not be liable for any claim or demand against the Client by any third party on account of any errors or omissions of TS related to the services performed hereunder.

7. Remote access to personal computers and/or networks. If, or when, Client transitions to home or alternative networks, TS will use its best effort to make connections and serviceability. However, home or alternative networks may not have adequate internet connectivity and equipment to effectively work. TS is not responsible for inadequacies in those home or alternative networks or to secure those connections. Client acknowledges that home equipment will not be as secure and may not have TS' software and security features. TS is not responsible for the security of the home or alternative networks. Work on a home or alternative network unless otherwise included is outside the scope of this Agreement shall be charged as Additional Services. Client will also be responsible for any additional software installed at home or alternative networks.

8. In the event of a Force Majeure TS is not required to have technicians work during periods or at places where their safety or health could be in jeopardy and in any event will not require technicians to go on site.

9. Client agrees to carry cyber security, liability insurance and property insurance covering any damage to its network as well as to any clients of the Client adversely affected by Client's network functioning or transmissions from its network.

10. TS may apply changes or additional terms, conditions, and provisions to this Agreement upon 30 days advance written notice to Client containing the proposed addition or change. If the additions or changes are not objected to then they shall take effect at the end of said 30-day period. Within the 30 days Client may submit changes or objections to the proposed changes or additional terms. If the parties do not agree on the change or addition, then it shall not become part of the Agreement. All the terms, conditions and provisions of this Agreement will continue to apply during any renewal term. Both parties agree to negotiate in good faith rates to be mutually agreed under any renewed contractual service term to be effective at the end of the initial term.

11. Failure to pay: If payment is not received by the first of the month for that month of service TS reserves the right to suspend all on-site and remote services until the monthly fee has been paid, provided TS gives the Client five (5) business day notice of intent to suspend the Managed Services due to late payment.

12. It is understood that any Federal, State or Local Taxes applicable shall be added to each invoice for services or materials provided by TS. Client shall pay any such taxes unless a valid exemption certificate is furnished to TS for the jurisdiction of use, except in cases when TS procures or sources the incorrect equipment and/or software and/or support services any incorrect items or software shall be returned to TS.

13. If Client fails to make payment for any services or items purchased, and such failure continues for fifteen days, interest shall accrue on any amount due at the rate of 12% per annum until paid. In the event collection processes are instituted to collect any amounts due from Client, Client shall pay all costs of collection plus reasonable attorney fees.

14. Indemnification:
    a. The Client agrees to indemnify, defend, and hold harmless TS, and its officers, directors, principals, members, managers, employees, subcontractors, agents, representatives, successors and assigns from and against any damage, claim, loss, expense (including reasonable attorneys' fees and damage to any person or property), occurring as a result of (i) the Client's use of TS's Managed Services, or use by those authorized by the Client of TS's Managed Services; (ii) the Client's handling, storage, transmission or possession of information, data, messages or other content or assets on TS's systems or network, on Client systems or network that are installed, managed or otherwise serviced by TS, or on third party systems and networks that TS uses to provide its services, including but not limited to, claims: (A) for libel, slander, invasion of privacy, identity theft, infringement of copyright, and invasion or alteration of private records or data; (B) for infringement of patents; (C) for security breaches of any kind; or (D) based on handling, storage, transmission or possession of information that contains viruses, malware or other destructive code, media, or any unlawful content; (iii) the Client's breach of any software licensing requirements of third parties; (iv) the Client's failure to comply with any provision of the Agreement; or, (v) the Client's failure to obtain permits, licenses, or consents that Client may be required to obtain to enable TS to provide its Managed Services (e.g., landlord permissions, wiring permits, etc.).
    b. TS agrees to indemnify and defend the Client, its directors, officers, principals, members, managers, employees, agents and successors against third party claims alleging that TS's Managed Services as provided infringe any third party patent or copyright or contain misappropriated third party trade secrets. TS's obligations under this section will not apply to the extent that the infringement or violation is caused by (i) functional or other specifications that were provided or requested by the Client, or (ii) Client's continued use of infringing services after TS provides reasonable notice to the Client of the infringement. For any third party claim that TS receives, or to minimize the potential for a claim, TS may, at its option and expense, either: (i) procure the right for the Client to continue using the services in question; (ii) replace or modify the services with comparable services; or (iii) terminate the services. The provisions of this Section state the entire liability and obligations of the indemnifying party, and the exclusive remedy of the indemnified party, with respect to any of the claims identified herein.

15. This Agreement is fully assignable by TS. Immediately upon assignment the assignee's name, address and contact information shall be provided to the other party. This Agreement shall be fully binding and enforceable as against all permitted assignees and successors in interest.

16. Termination:
    a. Termination by Client: Client may terminate this Agreement with or without cause within the first 6 months of the initial 12-month term of the Agreement with payment of a Termination Fee equal to the amount of the monthly Managed Services fee agreed to in this Agreement $**6,955.00,** payment of all past and currently due amounts together with late fees and costs and payment for the remaining term of any software subscriptions which cannot be terminated at the time Client terminates this Agreement, i.e., Microsoft NCE. Provided TS was notified in a service ticket within 10 days of the original occurrence of any incomplete tasks, work orders and/or faulty equipment which it itemized with sufficient detail to identify the problem, Client may withhold payment related to such incomplete tasks, work orders or faulty equipment until same are completed or resolved. Upon completion of all tasks and work orders, or resolution of faulty equipment, Client shall release all money previously withheld. Under all other circumstances, TS shall be given a reasonable opportunity to complete any open tasks, work orders or resolve any open issues for which the Client has withheld payment. Any such election shall be made in writing by Notice of Termination and is to be accompanied by the Termination Fee and all other amounts due.
    b. Termination by TS: TS may terminate this Agreement:
        i. Upon giving notice to Client of default of its obligation in this Agreement and should the default not be cured within five (5) business days of receipt of written notice from TS.
        ii. Should Client fail to pay for Managed Service or products at the time of ordering or within 30 days of billing. TS's failure to enforce any payment requirement set forth in this Agreement shall not be construed as a waiver of the right to do so.
    c. Should Client file for protection under the federal bankruptcy laws, or any bankruptcy petition or petition for receiver is commenced by a third party against Client.
    d. Backups. In the event of default or early termination or in the event the parties do not renew at the end of the term of this Agreement, Client shall be responsible for transferring backups to a system administered by Client or others on its behalf and for paying all costs associated with transferring and/or setting up backups off of the system maintained by TS. If Client does not provide for any transfer of backups, they shall be terminated within 30 days of the Notice of Termination or Notice of Default. Client assumes all responsibility for its backups and TS has no responsibility to retain backups. In the event prior to the end of the 30 days, client places its own backups on site or obtains its own cloud backups then it shall notify TS so its backups can be terminated.
    e. In the event of default or termination under any circumstances, Client agrees it will provide access to TS technicians to remove licenses and tools. Should Client fail to provide such access it shall continue to be responsible for 50% of the amount of the monthly Managed Services fee until access is provided and the licenses and tools removed.
    f. In the event of default or termination under any circumstances, Spam filtering will be terminated. Client understands that it is entirely responsible to redirect all of Client's MX records away from the spam filter or email system and redirect email to its server or

provide TS access to its network information and equipment to take those steps. Upon termination of spam filtering services email will "bounce" if Client has not taken these steps or requested and allowed TS to take the necessary measures. Client understands the above and accepts this responsibility and the consequences if it fails to cooperate or act; Client acknowledges, that upon termination of the spam filtering if these steps are not allowed or taken email will not be available and there is no recourse whatsoever as against TS.

g. In the event of termination by either party, Client is responsible for the full amount of all payments for services provided and products ordered, including, but not limited to all costs associated with the remaining term of any subscription for software which cannot be terminated at the time this Agreement is terminated, i.e., Microsoft NCE Software.
h. If either party terminates the Agreement, or if Client defaults, then the parties agree to work cooperatively to transfer the Client's data and network information as directed by the Client to another service provider or to the Client. The Client shall be responsible for all costs related to the transfer which will include hourly charges of technicians to accomplish the transfer and any services maintained by TS containing Client data. Client must designate a vendor to handle its email, backups and any other services provided by TS. Client must establish an account for transfer of the backups and any other services within 30 days of notice of termination or default, or within 30 days of termination of this SLA. TS has no responsibility for backups, email or other services beyond 30 days following termination or default under this Agreement.
i. In the event of termination of services for any reason by either party, upon written request by Client, TS will provide up to 60 days support to allow Client to make a transition provided Client pays all amounts then due and pays the Managed Services Fee for the additional 60 days in advance.

17. Dispute Resolution: All claims and disputes arising under or relating to this Agreement are to be settled by binding arbitration. The parties agree they waive the right to bring a lawsuit based on such claims or disputes. Before commencing any arbitration proceedings, the aggrieved party must first present the claim or dispute in writing to the other party. The parties shall have 30 days to resolve the claim or dispute. If not resolved, then the aggrieved party may commence arbitration proceedings. The arbitration shall be conducted by Arbitration Resolution Services, Inc. (ARS) or other mutually agreed upon dispute resolution service and the parties shall be bound by any and all rules of the American Arbitration Associations United States Commercial Resolution Dispute Resolution Procedures for Consumer–Related Disputes. Any decision or award as a result of any such arbitration proceeding shall be in writing and shall provide an explanation for all decisions. Arbitration shall be conducted by an arbitrator experienced in Information Technology services and experience required for arbitrator and shall include a written record of the arbitration hearing. An award of arbitration may be converted to judgment in a Court of competent jurisdiction. The location of arbitration shall be in Oneida County, New York. The fees and expenses of the arbitrator and proceedings shall be paid by the substantially non-prevailing party.

18. This Agreement and any amendments and its validity, construction and performance shall be governed by the laws of New York. Exclusive jurisdiction and venue for all matters relating to this Agreement shall be in Oneida County, New York, and the parties agree and consent to such jurisdiction and venue.

19. Nothing in this Agreement, express or implied is intended to or shall confer upon any other person any right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

20. Whenever possible, each provision of this Agreement shall be interpreted in such a manner as to be effective and valid under applicable law. If any provision of this Agreement becomes or is declared by a court of competent jurisdiction to be illegal, unenforceable, or void this Agreement shall continue in full force and effect without such provision and this Agreement shall be construed to the fullest extent possible as to give effect to the intentions of the provision found to be unenforceable or invalid. With respect to any such term or other provision deemed invalid, illegal, or unenforceable, the Parties hereto shall negotiate in good faith to modify this Agreement so as to affect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

21. Each party acknowledges and represents that it has been advised to seek, and has sought, the advice of independent counsel with respect to the subject matter hereof. The parties acknowledge, understand, represent and agree that the terms and conditions of Agreement are the result of their mutual negotiation and, as such, no provision shall be more strictly construed against a party on the basis that such party was responsible for drafting such provision.

22. Any notices required or permitted hereunder will be given to the appropriate party at the address set forth in this Agreement or at such other address as the party will specify in writing. Such notice will be deemed given upon email, upon personal delivery to the appropriate address, or if sent by overnight mail, one (1) day after the date of mailing.

23. Client shall not modify, create any derivative work of, or incorporate any other software into the computer software programs or any portion thereof with the exception of allowing automatic updates to commence or confirming the installation of an automatically scheduled update or fully supported software for which client has purchased technical support and has scheduled such installation with TS. Programs must be installed by a TS technician or software technical support with a TS technician assisting. TS will not be responsible for maintenance of or for repair of errors or malfunctions occasioned by any installation, modification or enhancement to the Programs made by Client or by anyone other than TS unless TS has agreed.

Managed Services

Remote and On-site Support

Total Solutions I.T., Inc. (hereafter referred to as "TS") will provide support for the client's existing hardware and software, including installed third-party software and line of business applications, network equipment, workstations, laptops, servers, printers, copiers, etc. TS will also provide support and troubleshooting for how-to and general operation items. TS will provide a Tray Icon for users to easily make support requests that include screenshots. TS will use its best efforts to resolve issues remotely and will come on-site in the event remote resolution is not possible. Items falling outside the scope of this agreement will be identified as "Projects" and subject to a separate agreement between the client and TS based upon time & materials rate or a flat-rate fee as agreed by the Parties. Examples of "Projects" include, but are not limited to, server or major software upgrades and new expansion or acquisition of facilities or services.

Direct-to-Service Service Desk

TS will provide phone and email access to our "Direct-to-Service" Service Desk ("Service Desk"). The Service Desk is available Monday through Friday (9am to 5pm) and for after-hours support by paging our on-call technician. Should TS be unable to resolve the issue at the time of the call, the Service Desk will advise the client of the timing for service delivery so that the client can resume work in the most efficient way possible.

Ticketing System & Documentation

TS uses a professional ticketing system to track issues, resolutions, authorizations, etc. Client Portal access to the ticketing system is available to the client upon request. TS maintains documentation of the client's environment, including IP addresses of devices, network and server configurations, printer/copier configurations, configuration backups of network devices, and instructional guides for software installation and troubleshooting procedures. Client access to up-to-date web-based documentation platform secured by 2-factor authentication is available upon request.

User Moves, Adds & Changes

TS will complete user Moves, Adds, and Changes (MAC) as required to move users between existing equipment, set up new users, deploy new user equipment/workstations, terminate users, and other associated user changes.

Monitoring, Maintenance & Patching

TS will monitor workstations, laptops, servers, firewalls, routers, switches, and wireless access points for concerns to include where appropriate and possible: connectivity, disk space, CPU usage, memory usage, service health, hardware health (including drives & RAID), update/patch status, and more. Tickets will be generated for any discovered issues and TS will assign a resource to troubleshoot. TS will perform routine maintenance and patching to include Windows updates and 3rd party patch management.

Managed Endpoint Protection / Antivirus

TS will deploy, monitor, and maintain managed anti-virus/anti-malware software, including all licensing, for all Windows-based workstations, laptops, and servers. Anti-virus/anti-malware software is monitored

and immediately notifies TS should a virus or other malware be detected but is unable to be automatically removed or disinfected by the anti-virus software. Definition updates will be automatically installed as available and anti-virus software will notify TS in the event of an update failure.

Managed Backup

TS provides, maintains, and monitors managed backup software, including all licensing, to protect servers and critical workstations where required and possible *Appropriate backup storage hardware may be required and is not included as part of the costs associated with this agreement.*

Disaster Recovery Foundation

TS Managed Backup is image based, allowing us to restore your server from the cloud in the event of a facility compromise. TS also maintains a rental server on-hand for certain disaster recovery situations and potential migration support.

Remote Access & Work from Home

If authorized by the client, TS will provide corporate licensed TeamViewer-based access for users to remotely access their computer from outside the office. Where VPN-based access is appropriate and in place, TS will create and configure VPN accounts and software to support work from home from company owned devices.

Office 365 Configuration & Support

TS provides best practice configuration and support for Microsoft Office 365 including license additions and changes, account creations and terminations, installation and setup of software, troubleshooting of email delivery, and DNS hosting and maintenance of required records.

Third Party Vendor Liaison

TS will act as a liaison with client's third-party vendors, including reaching out for support, managing open support cases, and working with vendor to perform technical troubleshooting of issues. TS will also vet any access or changes requested by vendor to ensure compatibility and protect the client's environment from unintended consequences.

Project Development & Planning

TS will provide access to Professional Services department for identification of projects, development, and planning. Services falling outside the scope of this agreement will be identified as "Projects" and subject to a separate agreement between the client and TS' time & materials rate or a flat-rate fee as agreed to by the Parties. Examples of "Projects" include, but are not limited to, server or major software upgrades and new expansion or acquisition of facilities or services.

Virtual CIO / Technology Alignment

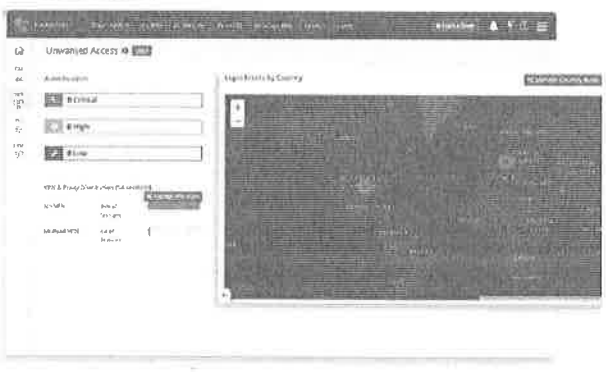
TS will provide quarterly technology alignment and meetings with client to review ongoing issues, go over upcoming Project work, discuss changes in vendors, advise on industry best practices, create budgets, and plan the technology roadmap for the next period.

Huntress Managed Identity Threat Detection & Response (ITDR)

Huntress Managed ITDR finds and stops identity-based threats in Microsoft 365.

Identity is the new endpoint.

Huntress Managed ITDR is built to address the evolving threat landscape of credential theft, session hijacking, VPN and location-based anomalies, credential-stealing malware and Adversary-in-the-middle (AiTM) attacks. Our fully managed solution provides continuous monitoring for identity-based threats, rapid detection of unauthorized access, and swift response to suspicious activities like rogue applications and shadow workflows. By focusing on the protection of credentials and session tokens, Huntress ensures your organization's digital identities remain secure, even as attackers develop more sophisticated methods.



Key Outcomes

Always-on Identity Protection

Sleep easier knowing our team of relentless identity experts monitors your Microsoft 365 environment 24/7, identifying and mitigating threats.

Block Unwanted Access

Detection and response to combat credential theft, session hijacking, and AiTM attacks to protect your most critical assets.

Uncover Rogue Apps

Proactively detect and remediate potentially malicious OAuth applications installed in your Microsoft 365 environments.

Combat Shadow Workflows

Neutralize malicious inbox and forwarding rules to protect your business from pervasive business email compromise (BEC) attempts.

No Noise. Just Results.

Every alert we send is actionable, human-verified, and built to keep you two steps ahead of the attackers. Our low false positive rate puts us ahead of others in the industry.

HUNTRESS

98% of users say that Huntress Managed ITDR has helped them reduce the time it takes to detect and respond to identity threats.[1]

Threats Detected

Location-based and VPN Anomalies
Expose unusual login locations and VPNs to ensure only authorized users have access to your data.

Malicious Inbox & Forwarding Rules
Spot shady activity, protect your inbox, and keep your emails secure and private.

Session Hijacking
Stop hackers from exploiting your systems and bypassing your 2FA/MFA.

Credential Theft
Keep cybercriminals out by locking down and monitoring your identity assets.

Rogue Apps
Hunt and stop malicious OAuth apps lurking in your Microsoft 365 environment.



Huntress by the Numbers

4.9/5
G2 customer rating

100%
Of customers would recommend[2]

3-minute
MTTR (mean-time-to-respond)

1.7M+
Identities protected

> Huntress flagged a suspicious login attempt, and I was able to immediately block the account before the bad actor could do any damage. I'm super pleased with how quickly we were able to remediate this. Before Huntress, it could have been days or even weeks before we knew an account was hacked, and likely only after malicious emails were sent out.

Joshua Ross
Founder | JXE Tech[3]

[1]https://uevi.co/6267FIBN
[2]https://uevi.co/1546QIJX
[3]https://uevi.co/3794INKV

Contact us to learn more.

Michael Morrill
BIGMIKE@TOTALSOLUTIONS.COM
totalsolutions.com

totalsolutions MAKING I.T. EASY

In partnership with HUNTRESS

Huntress Managed Endpoint Detection and Response

Huntress Managed EDR brings the tech *and* the experts to ensure endpoint security does precisely what it should: stop attackers in their tracks.

Top-tier endpoint security shouldn't be a luxury only for the big players with deep pockets. When basic defenses aren't enough, Huntress Managed EDR levels the playing field with a solution tailored for organizations like yours.

We blend cutting-edge tech with expert oversight, offering 24/7 monitoring by seasoned hunters who find, stop, and evict hackers hiding in your environment. We're laser-focused on cutting through the noise and filtering out false positives to surface the real dangers. And when hackers break through? We're on it day and night—isolating and eliminating them before they can mess with your business.

Key Outcomes

Catch What Slips Through the Cracks

Attackers will always find a way in—but when they do, you'll be ready. Our technology surfaces potential threats, leaving hackers nowhere to hide.

Act Only On Validated Threats

No more wild goose chases. We filter out false positives with human validation. So when you get an alert, you can act fast and with confidence.

Enjoy 24/7 Peace of Mind

Relax and enjoy your day off knowing your endpoints are covered. Our 24/7 SOC team has your back, ready to respond to threats around the clock.

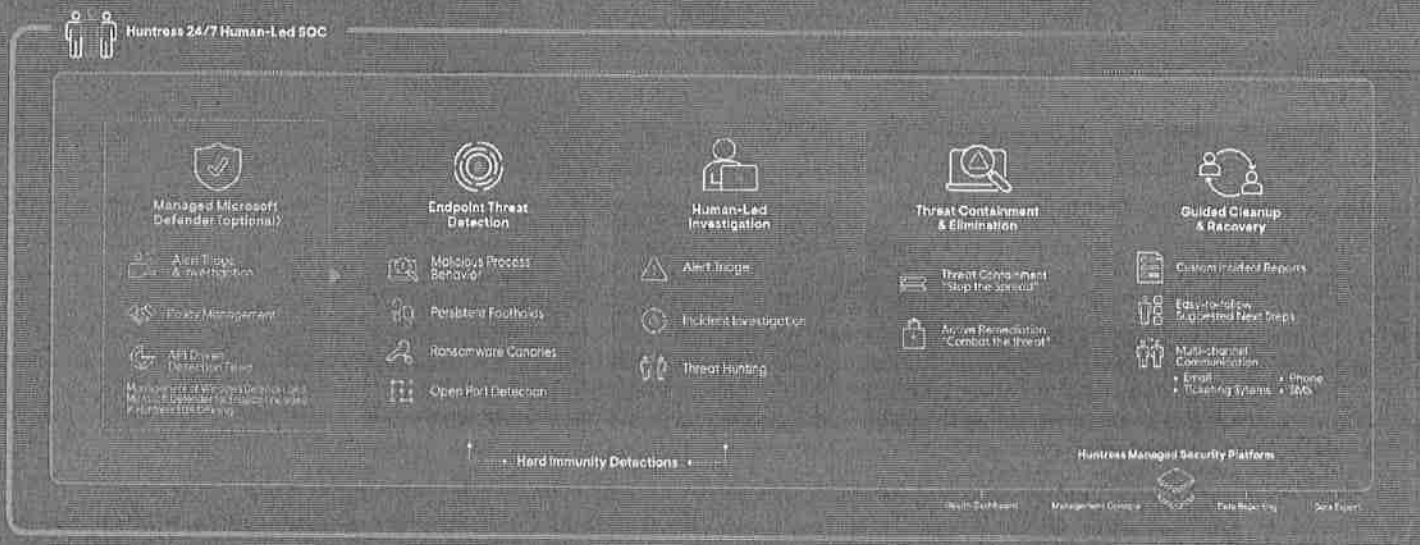
Fight Hackers With Hunters

Don't just find hackers, beat them at their own game. Our expert threat hunters track down their every move, removing their footholds and kicking them out for good.

Break Hackers, Not Your Bank

Protect your budget while protecting your endpoints. Our straightforward pricing keeps things predictable—no surprises.

Created By Hackers to Beat Attackers



HUNTRESS

Full Coverage, No Catch:

Huntress Delivers What You Need to Beat Hackers

Many EDR solutions hook you with big promises but hide key features behind confusing subscriptions that stretch your budget and leave you vulnerable. At Huntress, we keep it simple—everything you need is included. Need proof it works? With over 3 million endpoints protected, our 98.8% customer satisfaction and 500+ five-star reviews show we don't just make claims, we deliver results.

	Tech & Human Expertise	24/7 Coverage	False-positive Reduction	Containment & Response	Pricing & Packaging
Huntress	✓ Combines top-notch endpoint tech with our team of experts—handling everything from management to hunting. Hackers don't rest, but neither do we.	✓ Watches your back 24/7 with our global SOC staffed by expert threat hunters who use their sharp insights to slice through the noise and focus on the threats that matter.	✓ Highlights the most pressing threats with strict quality assurance processes that filter out the noise, ensuring you only respond to validated threats.	✓ Quickly isolates hackers and proactively responds before they can disrupt your business, while supporting your team in eliminating their presence and ensuring they never return.	✓ Adopts a single, straightforward package that provides maximum value for your investments and ensures you have everything you need when you need it most.
Other Managed Solutions	✗ Delivers endpoint tech but skimps on the human touch, leaning on automation to save bucks and boost profits—leaving you to staff in-house experts to fill the gaps.	✗ Charges hefty fees beyond their standard packages only to partially monitor your systems with subpar coverage, while disguising simple alert forwarding as "threat hunting."	✗ Drowns you in a sea of alerts with little context, diverting focus from other priorities and, crucially, from the threats that truly demand attention.	✗ Gives hackers extra time to meet their objectives, placing the burden on your team to track down and stop threats that operate with extreme speed and precision.	✗ Sells you low-value services, packages and then slaps on pricey add-ons—only to have you realize what's missing when it's already too late.

Huntress By the Numbers

4.8/5
G2 Customer Rating

98.8%
Client Satisfaction

<1%
False Positive Rate

Leader WINTER 2025 · Best Results WINTER 2025 · Best Relationship WINTER 2025 · Best Usability WINTER 2025 · Best Est. ROI Enterprise WINTER 2025 · Easiest Setup WINTER 2025

Contact us to learn more.

Michael Morrill
bigmike@totalsolutions.com
totalsolutions.com

totalsolutions MAKING I.T. EASY

In partnership with HUNTRESS

City of Oneida

Business Review Audit Report

Prepared by

totalsolutions

August 7, 2026

totalsolutions
MAKING I.T. EASY

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.

totalsolutions
MAKING IT... EASY

Audit Score

83

0 50 100

Infrastructure



Security



Managed Support & Services



Compliance



Requires Immediate Attention Needs Improvement Satisfactory

Base 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 an effective IT monthly expense based upon your audit score. This helps to level the playing field when comparing plans.

Financial Summary

Monthly IT Expense

$0 - $0

$0 $10

Effective Monthly IT Expense

$0 - $0

$0 $10

One Off Cost

$0

$0 $10

totalsolutions
MAKING IT EASY

Infrastructure

74

0 50 100

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.

Server	Workstations	Backup & Disaster Recovery
The server(s) is within 5 years old, under warranty and running a supported operating system.	Significant number of Windows 10 computers; also significant number of computers 5-12 years old.	TS Managed Backup - Server (direct to cloud) is deployed. TS M365 Cloud Backup is deployed to back up Microsoft 365
Internet Security Appliance	**Controller-based Wireless**	**Switching**
SonicWall firewall is supported by manufacturer. May need to change to move away from insecure SonicWall SSL VPN.	UniFi Cloud Key wireless controller is in place	Throughout all locations, switches are a mixture of managed and unmanaged. Critical switches are managed. Overall, switching is acceptable.
Cameras & Security System	**Cabling**	**Power Management (UPS)**
Satisfactory	Cabling needs to be cleaned up	Satisfactory

totalsolutions
MAKING IT EASY

Security

87

0 50 100

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.

Anti-Virus	Anti-SPAM and Virus Filter	Endpoint Encryption
TS Endpoint Management with EDR and MDR is deployed.	Proofpoint Essentials Professional (email filtering, encryption, and archiving) is deployed	Around 1/3rd of computers do not have Bitlocker enabled (primarily because they are too old to have a TPM chip to support the encryption).
Physical Security	**Managed DNS**	**Managed Wireless**
No obvious physical security issues	DNS is managed and monitored by Total Solutions, domain registrar information is documented.	Wireless configuration includes main corporate wireless network and separate VLAN isolated guest network.
Two Factor Authentication	**Remote Accessibility**	
MFA is configured and enforced for Microsoft 365 via Security Defaults method.	SonicWall SSL VPN with MFA is in use. SSL VPN has become a security risk and we are actively discussing replacement to mitigate the risk.	

totalsolutions
MAKING I.T. EASY

Managed Support & Services

74

0 50 100

Managed Support & Services is the most efficient way to minimize reactive support and proactively manage your infrastructure. In exchange for a fixed monthly fee, outsourcing support helps improve operations while reducing your overall expense. This detailed analysis page represents an overview of the state of your Base Plan Manages Support & Services. Each audit item is summarized and color coded for easy identification and the results for this section are reflected in the Managed Support & Services audit score.

Network Configuration	Configuration Policies	Monitoring
Satisfactory	Most computers are joined to server domain and Group Policies are enforcing configurations. Some computers are Windows Home and cannot be joined.	Satisfactory
Inventory & Asset Management	**Windows & Application Updates**	**Email Platform**
Satisfactory	Significant number of Windows 10 computers still in use, which Microsoft no longer releases updates for.	Email is through Microsoft 365
Proactive Maintenance	**Mobile Device Management**	**Vendor Support**
Proactive management is in place with TS Managed Services - Foundation	No MDM solution in place, may not have company owned devices	Satisfactory

totalsolutions
MAKING I.T. EASY

Compliance



Email Archiving	Email Encryption	Content Filtering
Proofpoint Essentials Professional (email filtering, encryption, and archiving) is deployed	Proofpoint Essentials Advanced (email filtering and encryption) is deployed	SonicWall content filtering is in place
Cyber Liability Insurance	**Dark Web Monitoring**	**Security Awareness Training**
Satisfactory	TS Cybersecurity Awareness Training is in place, which includes Dark Web monitoring	TS Cybersecurity Awareness Training is in place
Microsoft Licensing Compliance	**Acceptable Use Policy**	**Unsupported Software**
Office is licensed through M365 licensing	Policy status unknown	Satisfactory

Cabling

Problem State: Cabling needs to be cleaned up

Impact: Network cables should be proper length and not tangled in order to trace ports for troubleshooting and for ease of replacing equipment. Building cabling should terminate to a patch panel and be identified with port numbers that match wall jacks on the other end.

Workstations

Problem State: Significant number of Windows 10 computers; also significant number of computers 5-12 years old.

Impact: Microsoft ended support for Windows 10 in October 2025, meaning they no longer release updates to patch critical security issues.

totalsolutions
MAKING I.T. EASY

Configuration Policies

Problem State: Most computers are joined to server domain and Group Policies are enforcing configurations. Some computers are Windows Home and cannot be joined.

Impact: Policies should be set to enforce computer passwords and complexity, security settings, folder redirection (to protect locally stored files in Desktop and Documents folders), and other settings.

Windows & Application Updates

Problem State: Significant number of Windows 10 computers still in use, which Microsoft no longer releases updates for.

Impact: Microsoft ended support for Windows 10 in October 2025, meaning they no longer release updates to patch critical security issues.

totalsolutions
MAKING IT EASY

Endpoint Encryption

Problem State: Around 1/3rd of computers do not have Bitlocker enabled (primarily because they are too old to have a TPM chip to support the encryption).

Impact: BitLocker encrypts a computer's hard drive so that if the computer is lost or stolen, someone can not take out the hard drive and extract the data.

Workstations

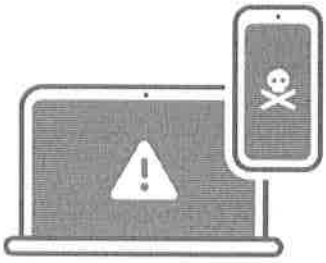
Modern Workstations

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**.

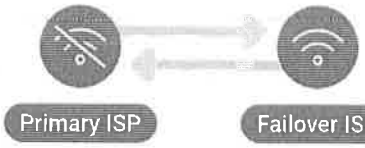
17%

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

TechAdvisor - 2021

Internet Security Appliance



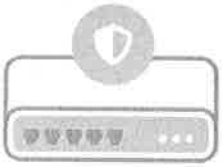


ISP Load Balancing is a method of monitoring several internet circuits and switching between them in the case of a failure. This increases uptime and provides better availability of cloud services.

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.

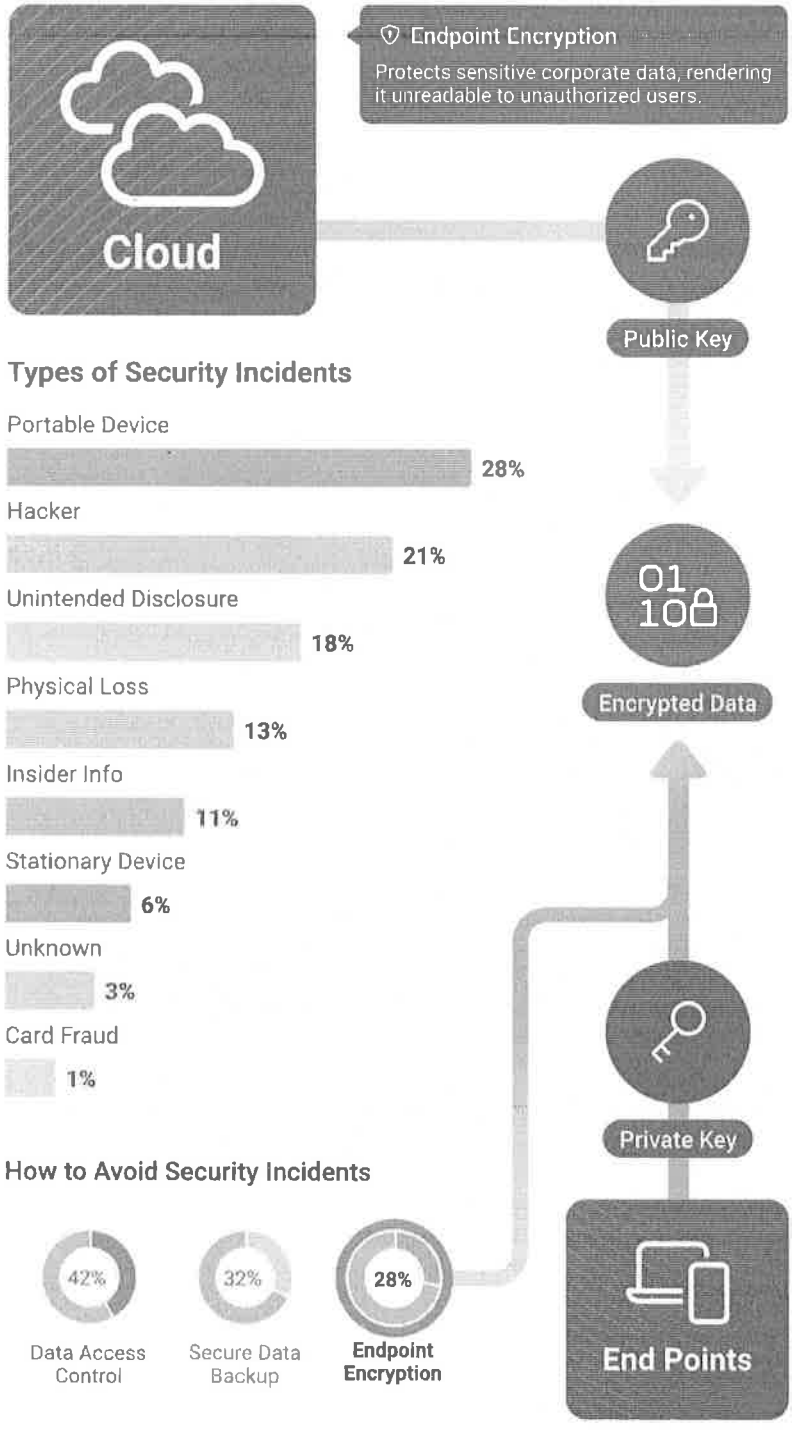
Why is this Important?

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.

Endpoint Encryption



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%

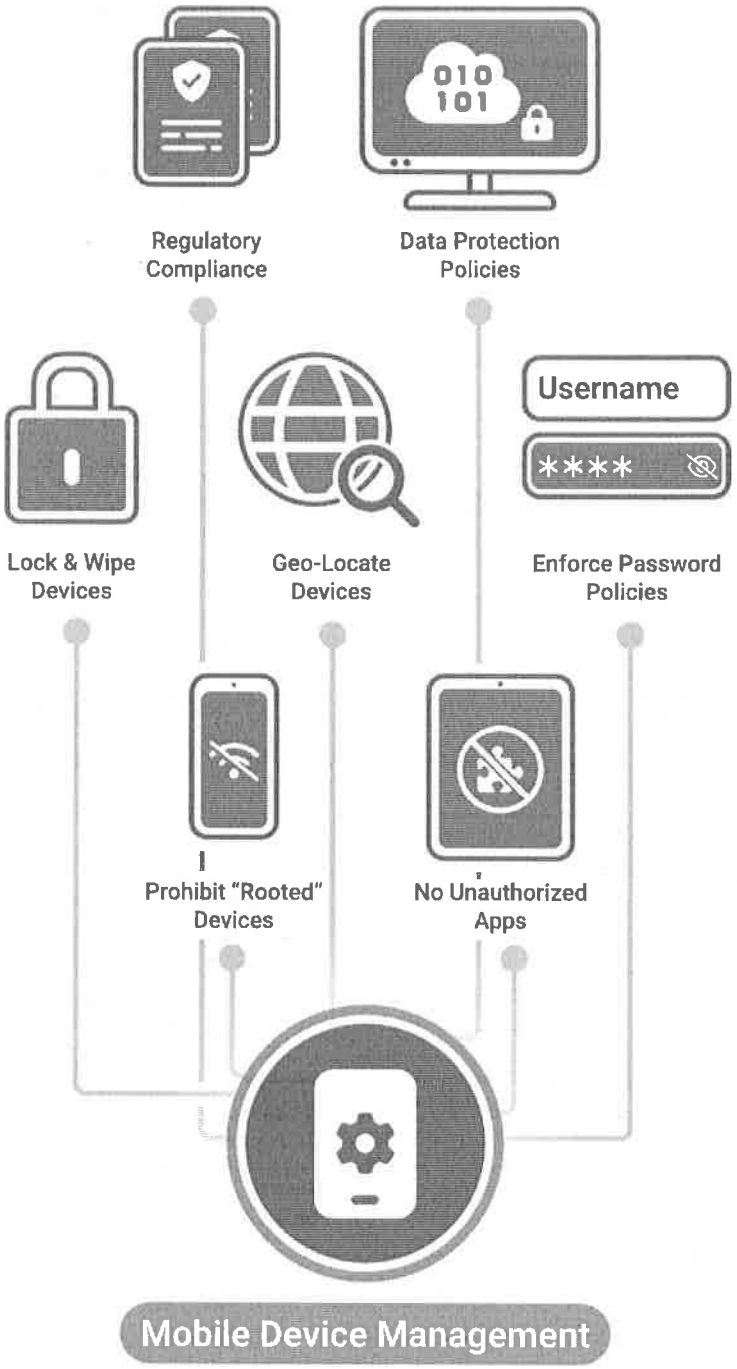
of security incidents is a result of **insider information** or **unintended disclosure**.

FTC Consumer Sentinel Network 2021 Report

7%

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

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**