

Service Introduction

IRONBYTE SOLUTIONS



Service Overview

Our service protects your business computers from phishing, scams, and ransomware, and keeps their software up to date to fix security flaws and bugs.

Email security

IronScales

Blocks phishing and scam emails

Endpoint protection

Huntress

Catches hidden attackers, watched around the clock

DNS filtering

Control D

Blocks dangerous websites before they load

Device management

NinjaOne

Monitors and manages every computer

OS and software updates

Action1

Keeps operating systems and apps up to date

Email account management

Included service

Creation and deletion for new hires and departures

**Requires access to 365 or Google Workspace admin profile*

Email configuration

Included service

Set up correctly and securely

24 hour SLA support on services

Included service

For the services we provide, up to 24 hour response

Quarterly review

Included service

A regular check-in on your security

\$50 per device per month Optional add-ons: Backup (CrashPlan) \$25/month, Password manager (Bitwarden) \$6/user/month

Email Security

Ironscales - Stops scam and phishing emails before they cause harm.

WHAT IS INCLUDED

- Scans incoming email for phishing, impersonation, lookalike senders, and fake invoices
- Adds a clear warning inside the inbox when a message looks suspicious
- Removes a confirmed threat from every mailbox, not just the one that received it
- Works with Microsoft 365 and Google Workspace email (Other email types may not be eligible)

REAL-LIFE EXAMPLE

What happens

A fake invoice arrives from a lookalike of a trusted vendor email address, asking to update payment details.

How it is stopped

IronScales flags the mismatch, warns the employee, and pulls the message from every inbox before anyone clicks or pays.

What you do: Report anything unusual to us. Otherwise, nothing day to day.

Note: IronScales works only with email accounts that have a proper Microsoft 365 or Google Workspace license.

Endpoint Protection

Huntress EDR - Finds attackers who hide on a computer, even when antivirus sees nothing.

WHAT IS INCLUDED

- Watches every computer for hidden attacker activity, not just known viruses
- Security experts review suspicious activity around the clock
- Can isolate an infected computer to stop an attack from spreading
- We act on alerts and clean up the problem at its root

REAL-LIFE EXAMPLE

What happens

A stolen password lets an attacker quietly install a hidden remote-access tool on an office PC. Antivirus sees nothing wrong.

How it is stopped

Huntress spots the hidden foothold, isolates the computer, and we clean it up before any data is taken.

What you do: Nothing day to day. We act on alerts for you.

DNS Filtering

Control D - Blocks dangerous websites before they open.

WHAT IS INCLUDED

- Blocks known malware, phishing, and scam websites before they load
- Protects devices in the office, at home, and on customer Wi-Fi
- Runs quietly in the background with nothing for staff to do

REAL-LIFE EXAMPLE

What happens

An employee searches for a free PDF converter and clicks a lookalike site that hides malware.

How it is stopped

Control D recognizes the bad site and blocks the page before anything downloads.

What you do: Nothing. If a legitimate site is blocked, tell us and we will review it.

Device Management + OS/Software Patching

NinjaOne & Action1 - Keeps every computer healthy and up to date, with no effort from you.

WHAT IS INCLUDED

- NinjaOne monitors device health and lets us manage computers remotely
- Action1 manages operating system and software updates on every device
- We decide which updates are needed and which to hold back, so a buggy update never disrupts your work
- Flags out-of-date software so weak spots get fixed early

REAL-LIFE EXAMPLE

What happens

A serious flaw is found in a popular browser, and criminals start exploiting it within days.

How it is stopped

Action1 rolls out the fix to every computer, and NinjaOne flags the one laptop that missed it so we fix it right away.

What you do: Nothing. Updates are handled for you.

Email Management

We handle the setup so your email stays organized and secure.

WHAT IS INCLUDED

- Email account creation and deletion: new hires get a properly set up account, and departures lose access promptly
- Email configuration: settings, forwarding, and security options set up correctly
- Basic support for the services we provide (24 hour SLA)
- A quarterly review of your security

REAL-LIFE EXAMPLE

What happens

An installer leaves the company on a Friday, and his phone and laptop still receive company email.

How it is stopped

We remove his account promptly, redirect his mail to a manager, and make sure no former employee keeps access. A new hire gets a properly set up account on day one.

What you do: Send us a request when someone joins or leaves.

Not included in this plan: real-time tech support and any work outside the scope of the services listed.

Essential Add-On Services

Two extras that work with your plan. Available with the base plan.

Backup: CrashPlan

\$25/month

WHAT IS INCLUDED

- Continuous backup of important folders on each computer
- Easy to browse and restore files, including earlier versions

REAL-LIFE EXAMPLE

What happens

A laptop is lost, or ransomware locks the Documents folder.

How it is stopped

We restore the files from the last good backup, so work continues.

Password Manager: Bitwarden

\$6/user/month

WHAT IS INCLUDED

- A strong, unique password for every site
- Shared logins kept safe instead of in emails or notes

REAL-LIFE EXAMPLE

What happens

A password reused on many sites leaks in an unrelated breach.

How it is stopped

Every login is different, so the leak cannot unlock payroll, banking, or email.

Sync is not backup: OneDrive and Google Workspace

- Sync mirrors changes, so a deleted, overwritten or ransomware-encrypted file is copied to the cloud too. Recycle bins and version history expire, and someone has to notice in time. Only files in the synced folders are covered.

Why an active folder backup is necessary

- It keeps a separate copy that attacks and mistakes can't overwrite. It keeps earlier versions of each file, so you can go back in time. It also runs automatically and covers the folders you choose.

How does IronByte compare to Traditional Managed Service Provider (MSP)?

	Traditional MSP	IronByte Solutions
Typical price	Around \$160 per device per month for mid-tier support	\$50 per device per month
Main focus	Day-to-day IT support and a helpdesk for your team	Preventing problems: phishing, ransomware, scams, out-of-date computers, and email that stops working
Tech support	Frequent, on-demand help	24-hour basic support for the services we provide (not full IT support)
Best for	Businesses that need frequent tech support	Businesses that do not need IT support but want to stay protected

Need frequent tech support? A traditional MSP is the better fit. Worried about phishing, ransomware, scams, computers that fall behind on updates, or email that is not working properly? IronByte Solutions is the best choice.

