bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

bPlan for Your Company

Thank you for the opportunity to build this document.

Included is a summary of what we learned from our discovery process over the last few weeks. In it we detail:

1. The first major project everyone identified as their number one wishlist item.
2. A second major project that will deliver some quick wins while the first project is implemented
3. Cybersecurity, which we know has been a major source of pain recently and might be again if left as-is.
4. A proposal for BestMacs to provide these services
5. Our 27-point inspection results in more detail
6. Our evaluation of CIS Controls v8 IG1 in more detail

bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

The first project: *Example 1*.

The one we heard from literally everyone we talked with:

***In this example case, everyone was sick of their on premises server and VPN not working and had starting using personal cloud sharing services*. Note: this part is not copy/paste boilerplate. We will document the specifics for your company in detail.**

The goal here is to eliminate disparate single-use tools (like Evernote, Dropbox, Box, GoogleDrive), make all emails related to a project searchable in the program without needing to access each individual person's inbox, share data easily with other companies (without using email attachments).

There's not going to be a "quick fix" for this problem. It's going to start with evaluating some products designed to *solve this issue*, picking one of those products to evaluate in a pilot program (with a mock data, or a closed project), and then either repeating with the next product, or going all-in on that product with training and investment.

Generally my recommendation is to pick a start date and use the product moving forward for anything new. Attempting to take all the data you've ever worked on and integrate it into the new solution will be overwhelming.

Here at the three products I recommend we discuss and choose one to pilot:

1. *Product A: here's why I ranked it first, pros/cons*
2. *Product B: pros/cons*
3. *Product C: pros/cons*

I can judge the technical merits of these apps (like their integration with Outlook and your large file stores - see below) but I don't use them daily. So I lack the ability to judge them anymore than I can judge, for example, the tools a designer uses to make digital art. I can make sure they run, are technically sound, and your access to them is secure. Ultimately it will be up to you and your team to decide which one makes the most sense.

Here's a rough timeline. Events exclusively requiring you and your team are in bold. We would do the rest (we may still require your input):

- Start Date
    - **Choose a first product to test**
    - **Select demo data**
    - **Choose team members to use product on demo data as though it were real**
    - Develop mock calendar of activities (e.g. “an email received on Day 9 does X to demo data”)
    - Develop KPIs to judge the product’s fit for your company
- Day 2 - engage their sales team, establish a demo environment
- Day 3 - provide select members of your team with an orientation
- Day 4 - **your team starts loading demo data**
- Day 14 - **your team finishes loading demo data and begins daily workflow**
- Day 17 - checkpoint: is your team encountering challenges, or have a general feel about the KPIs for the product
- Day 22 - second checkpoint
- Day 28 - final checkpoint (assuming we did not dismiss the product on previous checkpoints
- Day 30 - decision time: choose this product or repeat process on second product

If you end up choosing this product, we will build a similar timeline for product implementation across all of your team, with optional stages of rollout to departments that need it the most.

bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

The second project:

server, network, and desktop infrastructure.

This is an example of a project that doesn't require quite as much in-depth planning and scope as these are tools we deploy frequently for many businesses.

At the office, we have an old paradigm of an on-premises Windows Server providing directory services. Looking at your server rack:

Can we talk about moving this rack and the cables runs out of the bathroom? (*No this isn't photoshopped - and thankfully, it's not from a real client we worked on.*)

The Internet comes through a Cisco ASA 5506-X firewall first. The device is end-of-life and hasn't had new security updates published since July 2022.

Not as glaring, but the Cisco Catalyst 3560G-48TS Switch is also EOL, since 2018.

bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

The ideal standard for Microsoft-based infrastructure for small businesses in 2024 is for devices to be running Windows 10 or 11 Pro, joined to an Entra ID directory, managed in Intune, and each user authenticating to devices with a Microsoft 365 Business Premium or E3 account.

All of your devices appear to be running Windows 11 Pro but talking to a local Active Directory server, also in the bathroom.

We would simply need to un-join each computer from the local AD, then join each computer to the company Entra ID (which is basically AD in the cloud, and included with the Premium licenses). This will also get each computer enrolled in Intune for management and compliance purposes (more on that later).

Then since each user's "profile" (account and files) are bound to the old local AD, we will need to log each user into the computer with their M365 account, and do a migration of the old profile to their new M365 profile. In doing so we would also enforce backup of the profiles using the users' OneDrive folder. When that's done, the profiles become portable - any user can log into any computer and have their data follow them.

I suspect there are challenges in having a desktop and a laptop for some people and this will make it moot as the data will be the same on both and sync to the cloud. Likewise anyone who stored anything locally on their desktop will be able to access said desktop from OneDrive on their iPad.

This also checks one of the boxes on our cybersecurity standard (CIS control 5.4, see below) in that the new profiles will not have administrator access on their devices. Each user being an admin (as they are today) affords no change management process. They can install - even unwittingly - malicious software or potentially unwanted software that inhibits business functions. We can discuss what revoking "admin" means for users, whether it be help desk requests for new installations/changes, or an "admin on demand" approval service. Patches should be centrally administered and deployed during off-peak times.

At BestMacs, we would want to do the above as part of onboarding our services, so this project would happen almost immediately.

With the workstations and local Active Directory out of the way, let's turn our attention to the EOL network gear.

---> Best For Your Mac-Powered Business

PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

My recommendation is to replace the Cisco Firewall and the fragile Dell with a UniFi Dream Machine Pro (UDMP) router. https://store.ui.com/us/en/pro/category/all-unifi-cloud-gateways/products/udm-se
This will provide modern Internet defenses while still fulfilling gigabit speeds of your Google Fiber account.

> *Interesting side note on the UDMP is that it also functions as camera feed storage and door lock management. You have a vendor providing you with these items. Depending on how you feel about that vendor and what other services they provide (like human response), we may be able to offer a cost savings there with the UDMP as the backbone for new camera, door lock equipment paid for by saving the monthly fees from cancelling that relationship. https://ui.com/us/en/camera-security and https://ui.com/us/en/door-access*

The UDMP only has 8 ports for local computers so we will also need a switch to replace the EOL Cisco switch. The old switch has 30 cables plugged in to its 48 ports, so a replacement 48-port still gives us room to grow before requiring new hardware: https://store.ui.com/us/en/pro/category/all-switching/products/usw-48-poe

NOTE: this plan has two projects. Your plan may contain as many as 4, depending on what we find in discovery.

bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

Let's talk cybersecurity

It's more than a standalone project, it's a property of everything.

In this case we didn't gain access to an employee who could take us on a deep dive of the IT infrastructure so there were a lot of unknowns.

BestMacs uses the CIS Controls (IG1) as our standard for clients' cyber hygiene. I often call it a 56-point checklist. I have attached yours below but you can see a summary to the right.

I was able to verify your EDR installation which I marked "yes" with a caveat that I have no way of knowing the processes that back that up (i.e. how it responds to threats it detects, if human judgement is involved and on what schedule, etc.).

Conversely, I was able to determine that some items are not in place. For example, none of the computers have BitLocker whole disk encryption. If one of the laptops were to be stolen, all of the data is available to the thief. We would enforce the encryption, and escrow the unlock codes, in Microsoft Intune.

The CIS checklist usually falls into one of three categories, ranked in order of difficulty:

1. Deployable items. Like 9.2, DNS filtering. At BestMacs, we deploy that shortly after onboarding is complete and can do so without any help.
2. Items that require tech and your people. Like 5.2, unique passwords. A password manager cannot be set up without interaction from each of your people, and it's useless without their ongoing proper use.
3. Policy items that require collaboration with your leadership. BestMacs can provide CIS templates for things like 2.1 - 2.3, Applications, but they are not always "one size fits all" and need your authority to get buy-in from your people.

My recommendation is to establish a cadence to consistently make progress on "greening up" this list. It's very much "eating an elephant" … one bite at a time. We would work on a measurable timeline together.

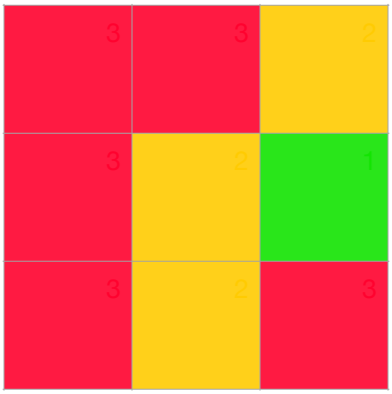
Client Status	Control
Unknown	1.1
Doubtful	1.2
Partial	2.1
Doubtful	2.2
Doubtful	2.3
Doubtful	3.1
Partial	3.2
Doubtful	3.3
Unknown	3.4
Doubtful	3.5
No	3.6
Doubtful	4.1
Doubtful	4.2
Unknown	4.3
Unknown	4.4
Yes	4.5
Yes	4.6
Unknown	4.7
Partial	5.1
Unknown	5.2
Unknown	5.3
No	5.4
Doubtful	6.1
Doubtful	6.2
Yes	6.3
Unknown	6.4
Unknown	6.5
Doubtful	7.1
Doubtful	7.2
Unknown	7.3
Unknown	7.4
Unknown	8.1
Unknown	8.2
Unknown	8.3
Likely	9.1
Unknown	9.2
Yes	10.1
Yes	10.2
Unknown	10.3
Unknown	11.1
Unknown	11.2
Unknown	11.3
Unknown	11.4
No	12.1
Partial	14.1
Partial	14.2
Partial	14.3
Partial	14.4
Partial	14.5
Partial	14.6
Partial	14.7
Partial	14.8
Partial	15.1
Unknown	17.1
Unknown	17.2
Unknown	17.3

---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

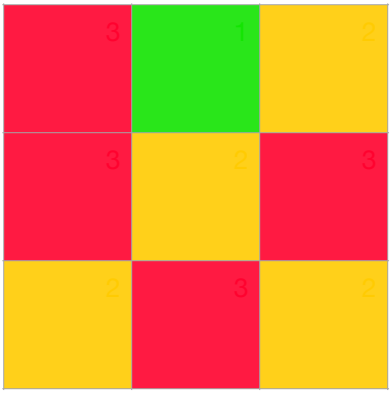
27-point audit summary

More detail on each box is attached below.

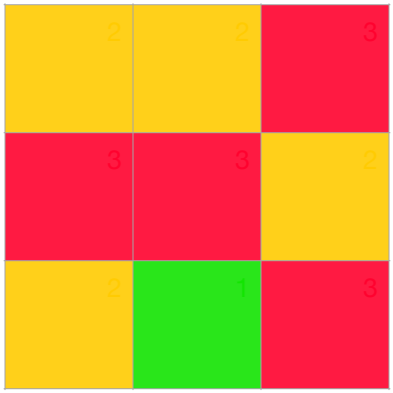
Infrastructure



Security



Support



Full detail on these boxes are attached below. We will attach three pages with detail on each box on your bPlan.

The items in red - which we will want to “green up” over time, some urgently - include:

Mobile Device Management
Business Continuity
Productivity Applications
Backup & Disaster Recovery
Server

Internet Security Appliance
Virtual Private Network (VPN)
Password Management
Managed DNS

Monitoring
OS & App Updates/Patching
Proactive Maintenance
Included Project Fees

bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

Final Thoughts and Proposal

Here I write a short one or two paragraph summary of the unique needs of your business and timelines for the above projects…

I hope you agree that implementing the major projects above and "greening up" both the 27-point audit and the 56-point CIS controls will be a huge improvement to your company, in terms of preventing another horrific cyber incident, and increasing your team's efficiency - and thus the financial bottom line to where our services are an investment with ROI, not simply another expense.

To that end, I'd like to propose our Best Practices service, which includes:

- Threat and failure monitoring on devices
- Log analysis and monitoring on workgroup services (Microsoft365 or Google Workspace)
- Administration of workgroup services
- Non-disruptive proactive maintenance
- bSmart productivity improving content
- Friendly, relatable people (no nerds)
- Bi-weekly, monthly, or quarterly touchbase
- Weekly reporting on key metrics
- Mail continuity, filtering, security services
- Network, VPN, router, firewall, and WiFi support for offices
- Cybersecurity awareness training that people will actually like
- Anti-hijack software (DNS filtering)
- Credential and MFA management implementation and training
- Next-gen behavioral anti-malware (EDR) with monitoring and remediation
- Scheduled patch verification and deployment
- Policy and procedure development, documentation
- Data protection with cloud-based immutable backup
- Vendor management and interaction with their tech support
- Device management and policy enforcement
- New employee onboarding and setup (and the opposite in offboarding)
- 24/7 support available as needed
- Unlimited nationwide remote help (8a-8p Eastern)

These bullet points alone will "green up" a lot of the reports. The labor for the proposed projects in this document is also included.

bestmacs
---> Best For Your Mac-Powered Business
PO Box 3483 Lawrence KS 66046 1-**(866) BESTMAC** http://www.bestmacs.com support@bestmacs.com

I bill for this service on an endpoint count, defined as a person and a single company-owned device. Additional company-owned devices are considered a half-endpoint (like people's second computer, your servers, routers). People without a device or operating off a shared or BYOD device are also a half-endpoint. BYOD devices are excluded since you don't own them. I adjust this count with each monthly invoice, up or down. If you grow, we grow with you, same if you were to unfortunately shrink.

I have you at:

- # people with primary computers
- # second computers (needs validation which we would do during onboarding)
- # network devices (assuming we plan to execute on the project 2 above)
- # servers (assuming we plan to execute on the project 2 above)

I'm pricing Best Practices for Your Company at $X per endpoint per month. At Y endpoints that's $Z/mo.

There will never be any other charges for additional labor. The only exception is a set-up fee for onboarding equal to the first month's service on the first invoice.

The EDR, DNS filtering, patch management, cloud backup and software is included (we will likely add new tools in the future at no additional cost).

The service is guaranteed for the first 90-days. At any point during that time you can terminate service and be refunded all of your monthly fees.

Lastly, a credit in the amount of $X that you paid for this report would be applied to the first invoice.

There's a lot of work to be done here, and some of it will take quite a long time to implement, but I know that Your Company will much better for doing it. I hope that you agree and that we have opportunity to work together.

Attached below this are greater detail on the 27-point boxes above, and the 56-point CIS checklist.