

Lead the way.

With Responsible IT Infrastructure That Empowers Your Business

Integris.

Why Responsible IT Architecture Is at the Root of Everything We Do—and How That Can Benefit Your Business

Responsible IT Architecture is our own term. But the idea behind it is simple. We believe that every client we serve should have a baseline of products that keeps their cybersecurity covered, and their productivity assured. Integris can deliver on that promise, whether you're buying a full suite of tools from us, or we are supplementing tools you already have.

The bottom line, however, is this—we won't work with clients unless we're working on a solid IT foundation. **With our Responsible IT Architecture program, we strive to:**

- ✓ Protect your networks with firewalls and hack-proof authentication
- ✓ Create a bulletproof platform that protects you against outages, disasters, and data loss
- ✓ Continuously patch, monitor, and remediate vulnerabilities in your system
- ✓ Filter out bad actors and code trying to interact with your systems



*"We have improved our security and flexibility, begun our cloud migration, and switched to remote working due to the COVID crisis. Again, with the guidance of Integris not missing a single step. Our future is planning for better efficiencies and reducing costs – all while preparing for the next unexpected turn. As Integris has proven repeatedly, **Integris will be a trusted partner on this journey forward.**"*

Bryan LeBlanc, CIO Pace Claims

Business Benefits

What could your business accomplish if your systems were built on the right foundations? Plenty. When you work with Integris, we take on all your daily IT headaches, so you can focus on getting down to business.

When you have a fully developed, Responsible IT Architecture, you can:

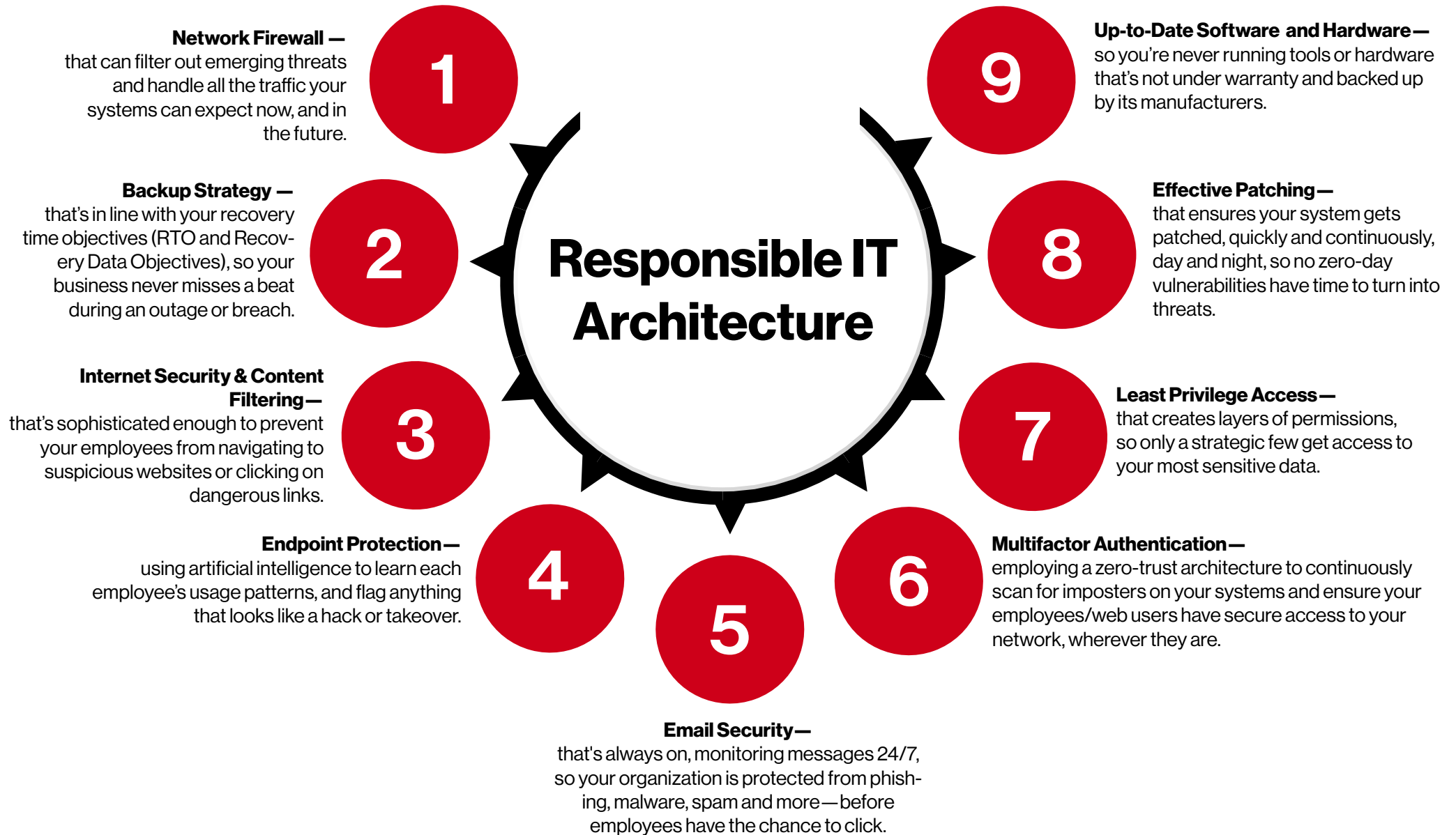
- ✓ Let Integris manage your IT vendors, so you'll never have to juggle multiple accounts, data sets and dashboards again
- ✓ Stay one step ahead of your compliance requirements for regulators and cyber insurers
- ✓ Ensure that your systems are up to your usage requirements, eliminating traffic-based outages and bottlenecks
- ✓ Never lose data, with cloud backup that never runs out or goes dark
- ✓ Prove to customers and clients that their data is safe when it's in your hands, with cybersecurity documentation that wins you business

And that's just the beginning. Contact us for a free consultation, so we can show you what Responsible IT Architecture can do for you.

integrisit.com

Responsible IT Architecture

Whether you've signed up for a managed service plan with Integris or you're coming to us for a la carte services, we'll ensure your company has the industry gold standard for:



How Responsible is My IT Architecture? *Try this Self-Assessment*

On a scale of 1-5, with 5 being highly responsible, please rate your organization.

1 Network Firewall

- 1 Does your firewall cover all your assets, or are you relying on your cloud providers to cover you? Can your firewall handle the level of internal and external traffic on your systems? Are employees covered by your firewalls, even when they're working remotely?
- 2
- 3
- 4
- 5

2 Backups that Cover Your Needs

- 1 In the event of an outage, breach or disaster, how long could your system be down before you experience negative revenue consequences? How much data could you lose in the event of a breach before you reached mission critical status? The answer will determine how much you should invest in your cloud backup systems.
- 2
- 3
- 4
- 5

3 Internet Security & Content Filtering

- 1 What happens when an employee clicks on a link that goes to a site on the dark web, or one without a current security license? Will they be able to reach it anyway? Is there a safe, quarantined spot in your system where suspicious links can be sent and dealt with?
- 2
- 3
- 4
- 5

4 Endpoint Protection

- 1 Are all the endpoints that operate on your systems covered? For instance, are there protections when an employee uses a personal phone, tablet or computer to log onto your systems? Are your anti-virus systems intelligent enough to know when an employee is likely to log on, and what they request to do in your systems? Would they recognize if there were spikes in unusual behavior?
- 2
- 3
- 4
- 5

5 Email Security

- 1 Is your email monitored around the clock? Do you have the ability to quarantine questionable email for analysis? Do your employees have an easy tool for reporting suspicious emails?
- 2
- 3
- 4
- 5

6 Multifactor Authentication

- 1 Are your employees asked to use a token system, like Duo, or a passwordless fingerprint, as a secondary verification to log onto your systems? Do these systems work for all endpoints?
- 2
- 3
- 4
- 5

7 Least Privilege Access

- 1 How many users in your system have broad, all-inclusive admin rights? Who has secondary admin rights, over just a portion of your site? And what can an employee with general log in credentials see? If any of these credentials fell into a hacker's hands, what could they see and how much damage could they do?
- 2
- 3
- 4
- 5

8 Patching Protocols

- 1 When your vendors announce a patch, who handles patching on your systems? What if a custom patch needs to be done after a hack? Are your patches installed as soon as they are announced, or do you have a wait period? Can you produce a report on their patching activities if an insurer or regulator asks to see them? If your patching is done internally, do you feel your team is adequately resourced to deal with the patching workload?
- 2
- 3
- 4
- 5

9 Your Software and Hardware

- 1 Is your hardware so old that you're having trouble running the latest programs on it? Are you still able to service your software and hardware through the manufacturer? Do you have a strategic plan for your software and hardware purchases, and a budget line item to support it?
- 2
- 3
- 4
- 5

Build a Roadmap for Your Future with Our Paid Assessment

What's next for your IT systems?

Integris can tell you. Our paid assessment will help take you there.

The first step in creating a Responsible IT Architecture is finding the gaps in your systems. Our comprehensive assessment starts with a visit from our engineers, who come onsite to look over your entire network, governance system and documentation. We check your hardware, your licenses, and your protocols, comparing them against best practices for your size and industry. We also look at the security and usage needs you'll have in the future, based on current threats and traffic patterns.

When we're done, we'll provide you with a gap analysis, a plan for next steps, and a budget covering your comprehensive needs. We'll show you exactly how to achieve a responsible IT architecture for your company, while keeping your costs scalable for your growing company.

Our assessments cover your entire IT enterprise, including:

- ✓ Cybersecurity protocols
- ✓ Hardware/software recommendations
- ✓ Regulatory compliance
- ✓ System traffic analysis
- ✓ System vulnerability
- ✓ Backup and disaster recovery
- ✓ KPI and data collection

Contact us today.

We'd love to show you what Responsible IT Architecture can do for you.

integrisit.com/contact

