
When it comes to cybersecurity today, companies typically have three options:

1. **Do nothing or the bare minimum, and hope that cyber attackers don’t find you.**

2. **Keep your current cybersecurity posture as is, without consistent updating or monitoring (and hope cyber attackers don’t find you!).**

3. **Consider Cygilant’s hybrid security as a service to identify threats and vulnerabilities, mitigate risk, and achieve compliance.**

Let’s look at each one of these options in greater detail.

### 1) Doing Nothing or the Bare Minimum

You must realize cyber attacks will never stop and that every business is a target. Many organizations believe they’re “not worth a hacker’s time,” but if you have data (and every business does), you are worth hacking.

When that occurs (and it will), are you prepared to deal with the time, cost, and labor associated with:
• Investigating what happened and how to prevent it from happening in the future?
• Creating and sending customer breach notifications?
• Assuring your customers that their data is secure after a breach?
• Dealing with the bad press and media outreach/response?
• Paying additional attorneys and litigation fees?
• Taking a hard look at your IT environment and improving/hardening your defenses?

Chances are, you are not, which is why 60% of mid-market businesses fail after a data breach – they simply cannot afford it.

2) Keep Your Cybersecurity Posture As Is

If you have a basic security program and think you can “get by with the typical security measures in place,” you are mistaken. Just having a firewall and some endpoint security such as desktop anti-virus doesn’t cut it in today’s advanced cyber threat landscape. Consider:

• 50% of all messages on the Internet are spam, many of which contain links to malware and ransomware. It only takes one wrong or inadvertent click to have a cybersecurity nightmare in your hands.
• 70% of attacks target mid-market businesses. They’re easier targets than enterprises and they typically have less manpower and fewer technical resources to detect issues.

When companies like yours fall victim to malware, ransomware, hacking, or a data breach, your company will suffer from:

• Ongoing disruptions to continuity, productivity, and operations
• Increasing insurance premiums
• Losing customer loyalty and revenue from cancelled contracts
• Having to pay a ridiculous amount of money to unlock your data
• Devaluing of your company brand and degrading of your reputation

And let’s face it, you are likely to be fired if that happens. So it’s in your best interest and your organization’s best interest to do everything you can to stop these security incidents from happening in the first place. That’s where Cygilant comes in.

3) Consider Cygilant’s Hybrid Security as a Service Approach

If you’re struggling with your organization’s IT security and compliance posture because of lack of time, budget, or people, Cygilant is here to help. With Cygilant, you can implement a comprehensive proactive and reactive security monitoring program to protect against modern-day cyber threats while meeting regulatory mandates.
In fact, our customers experience significant benefits while protecting their assets. Here are just a few real-world examples of how we've helped:

**Save Time**

For every single security incident our customers address, we've already taken care of 50 incidents, saving them immeasurable time, money, and worry.

**Intercept Attacks**

Cygilant will give you visibility and control of your IT environment, catching attacks you might not have – like web attacks targeting passwords, UDP flood/DDoS attempts, and vulnerability exploits.

**Discover Anomalies**

Cygilant looks for unusual activity, behaviors, and configurations in your environment and will alert you to anomalies you wouldn't otherwise have been aware of – such as re-enabling of disabled accounts, evidence of weak firewall configurations, unpatched vulnerabilities, specific user behavior, etc.

**Reduce Vulnerabilities**

Our Vulnerability Management customers have seen a 47-72% reduction in vulnerabilities in just 60 days. Imagine what is floating around in your network that's unidentified and unpatched; wouldn't you want to do something about that?

**Reduce Complexity**

SOCVue Patch Management helps customers reduce the time and complexity associated with patching servers, desktops and laptops on or off their network. The service automatically scans Windows and Linux endpoints for missing patches for the OS, browser and 3rd-party applications like Java and Adobe.

Our customers love the peace of mind Cygilant delivers. Here are just a few quotes we've heard recently:

- “We have had nothing but great things to say about Cygilant. We love the extra set of eyes that are watching our network while we sleep. Thanks for letting us sleep better at night.”
- “SOCVue allows us to meet complex compliance mandates while Cygilant's highly trained analysts provide the expertise we don't have in-house.”
- “A vendor that is flexible, and has a great attitude, is a pleasure to work with. Thanks!”
- “Great company with customer service at the forefront.”
- **Read more customer testimonials**
How You Can Gain Peace of Mind

Cygilant provides three SOCVue hybrid security-as-a-service solutions that can help organizations of any size affordably and effectively improve their cybersecurity and compliance posture.

- **SOCVue Security Monitoring** gives you best-of-breed Log Management and SIEM that is managed around-the-clock for real-time threat detection, analysis and notification, proactive remediation guidance, and compliance auditing.
- **SOCVue Vulnerability Management** reduces your attack surface and mitigates risk with unlimited managed scans, analysis, risk prioritization, and remediation guidance.
- **SOCVue Patch Management** reduces the time and complexity associated with patching servers, desktops and laptops on or off your network.

Cygilant's SOCVue services combine the best people, process, and technology to build an enterprise-class IT security and compliance program. That's because SOCVue gives you the flexibility and cost savings of a security software-as-a-service offering, but also provides a world-class team of security and technology experts to manage the technology and help implement cybersecurity best practices.

With all the challenges you face today while trying to keep your organization safe, having the best IT security solutions in your corner should not be one of them. We know we can help you meet your organization's unique security and compliance goals. **Request a demo today** to see how quickly and affordably you can improve your security and compliance posture with Cygilant.

About Cygilant

Cygilant, a pioneer in **hybrid security as a service**, is transforming how mid-market organizations build enterprise-class security programs. Acting as an extension of our customers' IT teams, Cygilant provides continuous security operations based on best-of-breed technology at a fraction of the cost of alternate solutions. Cygilant is a trusted advisor to organizations that need to improve their IT security and compliance posture and protect against cyber threats and vulnerabilities.

For more information or to request a demo, visit: [https://www.cygilant.com](https://www.cygilant.com)