TBConsulting
Technical and Business Consulting, LLC

SOLUTION BRIEF

SECURITY MONITORING:

Fortify your defenses and protect your digital assets with 24/7/365 monitoring, threat detection, and improved response times.

You underestimate the power of the Dark Side. If you will not fight, you will meet your destiny. – Darth Vader

Challenges

- Rogue downloads
- Vulnerable edges
- IT talent shortage
- Heavy firewall reliance
- Slow incident management
- Underutilized tools
- Lack of strategy
- Communication breakdowns
- Technical debt

Solutions

- Security Posture Assessment
- Security Monitoring
- Vulnerability Management
- PEN testing
- Risk management program
- Cybersecurity Defense Matrix
- 24/7/365 monitoring

Benefits

- Achieve security maturity
- Reduce risk
- Mitigate the loss of productivity
- Proactive alerting and incident response
- Increase resiliency
- Improve security posture
- Mitigate cyber incidents and exploits
- IT team can focus on strategic initiatives
- Protection of digital assets
- Enhanced infrastructure performance
- Develop strong security posture

Imagine your business falling victim to a cyberattack. A single ransomware attack can topple the pillars of your business like dominoes. Your IT solutions have all been lined up to run the business, but a cyberattack can trigger the unstoppable collapse of your data security, operations, revenue streams, reputation, and financial stability.

Even if you are willing to pay the ransom, and you are able to recover all of your data (unlike 92% of victims, *Sophos, 2021*), your business will still experience costly downtime, unstable or interrupted operations, loss of customer trust, and sales may suffer. Say goodbye to putting your head in the sand. Determine your tolerance and find your roadmap to digital maturity by implementing best practice securing monitoring.

Challenges

Growth can be both a blessing and a curse. As your business expands, and revenue skyrockets, the additional demands placed on your IT resources can backfire if they don't receive additional support. Many executives think that 'tooling up' the IT department is enough support – but with the influx of devices, software, data, and increasing the capacity of servers and networks, IT teams can fall into a tailspin of troubleshooting and firefighting. Vulnerabilities are exposed, patches aren't installed, and alert fatigue is blamed for missing legitimate attacks.

With the vast increase in hybrid workplaces, security controls once standard across the office environment are difficult to implement across the 'work from anywhere landscape'—which includes mobile devices, personal devices used for work, and the use of unsecured connections. Employees may download unapproved software to get their work done faster, unknowingly putting your network at risk.

Recent cyberattacks have cause large-scale damage to supply chains and infrastructure. Cyberattacks are no longer merely ransom attempts—but rather they are carried out by criminal enterprises leaving no organization safe. Recovery from a cyber crisis is long, and often expensive; the hidden costs associated with the loss of contract revenue, intellectual property, and consumer confidence can be present for years.

Solutions

In the scramble to support remote and hybrid workforces, many organizations have come to rely too heavily on firewalls and other security tools, without first integrating those efforts into a cybersecurity strategy. Companies now face technical debt that is mounting due to the difficulty of hiring and retaining IT talent, further jeopardizing their ability to reach cybersecurity maturity.

Cybersecurity is not a single tool approach, but a multi-layered strategy that includes security awareness training, multifactor authentication compliance, 24/7/365 monitoring, agile responses, and the support of cybersecurity experts with the foresight to anticipate issues.

TBConsulting offers deep technical and business expertise to erase that technical debt and elevate the security posture and digital functionality of your enterprise. Protecting your edges is of critical importance, and the ability to evaluate, respond to, and remediate a threat is a sign of security maturity.

So how do you achieve security maturity? By first evaluating your risk tolerance, then defining your tools and processes, and finally implementing a roadmap to reach your desired state of security maturity. Opting in for a Security Posture Assessment will help determine your current position on the cybersecurity defense matrix and will help you develop an actionable plan to protect your organization.

Benefits

Preparation and a robust response program are harbingers of a mature security solution. To preserve the functionality of your enterprise and enhance the performance of your infrastructure, you may need the support of an experienced Managed Security Service Provider. With the daily grind of IT and security tasks taken off their plate, your IT teams can focus on strategic initiatives that will drive revenue growth.

TBConsulting is an MSSP with 25 years of technical and business experience in implementing right-sized security solutions and structured processes for clients. We work to deliver a trust-based and supportive IT partnership—one with open communication and security engineers and architects who are forward thinkers. We use industry leading tools and proven processes to protect complex environments and host an always-on, human powered, IT Operations Center. With the consistency of 24/7/365 security monitoring and white glove service, you will be prepared to respond to the constant barrage of security threats.