



ENDPOINT MANAGEMENT:

Centralized Management for Patching and Securing Endpoints

"To labor and not to seek reward." - Seamus Heaney

Challenges

- All tooled up but no centralized integration
- Time consuming & endless process
- Security gaps
- Disparates system compliance
- Remote users & BYOD
- Blame game/responsibility
- End user neglect

Solutions

- Patching of software & operating systems
- Server and system protection
- Deploying and reporting on corporate policy
- Firmware updates
- Remote troubleshooting support

Benefits

- Actionable reporting
- Visibility into user endpoint ecosystem
- Close vulnerability gaps
- Improve productivity
- Free up IT for critical projects
- Enhanced security
- Streamlined configuration
- Dramatically improved system compliance

Endpoint management is the strong, silent type - thanklessly laboring in the background to protect valuable systems, networks, and assets from cybercriminals. Although IT teams constantly respond to threats and thwart attacks, the truth is, they spend their time holding the fire line. As the business expands, so does the digital attack surface across the enterprise, further impacting risk. Executives can help shore up their IT teams and protect critical business assets with a trusted Managed Service Provider like TBC Consulting. Let TBC toil for you - from implementation to maintenance - with a comprehensive endpoint management solution that delivers. Every. Time.

Challenges

The top endpoint management tools may promise to update and patch servers, systems, and applications. Still, without a centralized integration plan and continuous feedback, multiple tools increase complexity and the likelihood of failure. When there is a lack of visibility into endpoints and an uptick in remote workers using personal devices, corporate controls easily implemented in an office setting are often too difficult to enforce remotely across the enterprise.

It is no surprise that 70% of breaches come through security gaps in endpoints. Unfortunately, companies respond to breaches by playing the blame game instead of understanding how the underlying condition of their infrastructure and the lack of endpoint oversight contribute to an attack.

Solutions

With constraints on resources, many organizations turn to MSPs for IT advice, expertise, and ultimately, to engage a high trust partner to share the burden of responsible digital asset protection. At TBC, endpoint management is an active and iterative solution, very different from the 'set it and forget it' philosophy of many IT providers.

Endpoint management identifies, updates, patches, and continuously monitors endpoint devices and systems to prioritize protection and increase stability. Corporate security policy and compliance controls are pushed out from a centralized hub, either on-prem or in the cloud, to manage the computing experience for employees regardless of location. TBC also regularly tests those controls to verify unified tool integration and confirm that firmware, operating systems, and software are patched and updated correctly in accordance with corporate compliance standards.

Benefits

Companies are better positioned to grow securely with more powerful risk management, increased visibility into endpoints, and actionable reporting on vulnerabilities. Let TBC manage the daily grind of patching, updating, defending, controlling access, and ensuring corporate standards are distributed across the enterprise.

With TBC experts supporting in-house teams, the daily burden of endpoint protection is relieved, and IT teams can focus on mission critical projects. TBC's comprehensive endpoint management solution is reliable, scalable, and secure.

