OneIT

CyberLock™

Infallible Cyber Security

from OneIT

In today's IT landscape, no single widget can create an infrastructure free from risk. Clients are demanding specialized expertise to protect their businesses from sophisticated cyber criminals, and many do not have in-house knowledge to address the threats, nor the time to stay up-to-date on the latest risks. ***CyberLock***™ from ***OneIT*** fills this void, delivering custom-designed cyber security solutions that protect the entire organization.

CyberLock services are organized into five levels or phases. Each phase was designed to build on the next, in a continual evolution of protection over customer assets. While the first phase of services will provide essential and baseline protection, later phases provide even greater levels of monitoring, reporting and intervention. These layers of protection insure every asset, from routers to workstations and everything in between, is monitored and protected 24/7/365.

Endpoint Security and Vulnerability Management	1	2	3	4	5
Vulnerability management (bi-weekly, monthly, or quarterly)	✓	✓	✓	✓	✓
Enterprise anti-virus	✓	✓	✓	✓	✓
Basic reporting			✓	✓	✓
Application whitelisting				✓	✓
Device control (USB device lockout)				✓	✓
Comp				✓	✓

Enterprise DNS Protection	1	2	3	4	5
Predictive security on all devices	✓	✓	✓	✓	✓
Prevent malware, phishing and C2 callbacks	✓	✓	✓	✓	✓
Enforces acceptable use policies	✓	✓	✓	✓	✓
Block malicious domain threats (DNS and IP layer)	✓	✓	✓	✓	✓
Identify targeted attacks	✓	✓	✓	✓	✓
Real-time, enterprise wide activity searches and reporting	✓	✓	✓	✓	✓

Managed Security Information and Event Management	1	2	3	4	5
Security, order network, and DMZ device logs		✓	✓	✓	✓
Threat intelligence		✓	✓	✓	✓
Monthly reporting		✓	✓	✓	✓

- Continued -

Server and service availability			✓	✓	✓
Network intrusion detection			✓	✓	✓
Database log collection			✓	✓	✓
Vulnerability reporting				✓	✓
Host IDS				✓	✓
Wireless IDS				✓	✓
Host configuration testing				✓	✓
File integrity monitoring				✓	✓
Security incidence response				✓	✓
Risk mitigation				✓	✓
Compliance reporting				✓	✓
Enterprise Managed DNS	**1**	**2**	**3**	**4**	**5**
DDOS attack protection	✓	✓	✓	✓	✓
DNS reporting	✓	✓	✓	✓	✓
Globally distributed DNS	✓	✓	✓	✓	✓
Charged by QPM	✓	✓	✓	✓	✓
Traffic reporting				✓	✓
Server Management	**1**	**2**	**3**	**4**	**5**
Downtime response	✓	✓	✓	✓	✓
OS patches and updates	✓	✓	✓	✓	✓
Health monitoring	✓	✓	✓	✓	✓
Service monitoring	✓	✓	✓	✓	✓
Security/vulnerability scanning			✓	✓	✓
Server optimization			✓	✓	✓
Exchange / email system monitoring			✓	✓	✓
SQL monitoring			✓	✓	✓
24/7 critical support				✓	✓
Storage management				✓	✓
OS hardening				✓	✓
Performance optimization				✓	✓
Blocklist monitoring and management				✓	✓
Website monitoring				✓	✓
Network Management	**1**	**2**	**3**	**4**	**5**
Network monitoring SNMP, Netflow* or sFlow*	✓	✓	✓	✓	✓
IOS and firmware patch management	✓	✓	✓	✓	✓
Connectivity troubleshooting and monitoring			✓	✓	✓
Troubleshooting and problem resolution			✓	✓	✓
Performance and availability management			✓	✓	✓
Network utilization capacity management				✓	✓
Preventive notification, trend and root cause analysis				✓	✓
Bandwidth utilization and QOS management				✓	✓
ISP circuit and outage management				✓	✓

- Continued -

Reporting	1	2	3	4	5
Enterprise ticketing portal	✓	✓	✓	✓	✓
Executive summary reports	✓	✓	✓	✓	✓
Performance summary reports			✓	✓	✓
Detailed performance reports				✓	✓
Utilization report for capacity planning				✓	✓
Uptime statistic reports				✓	✓
Compliance reporting					✓

Compliance Auditing and Monitoring	1	2	3	4	5
Configuration monitoring and management					✓
File integrity monitoring					✓
Activity monitoring and management					✓
Change monitoring and management					✓
Compliance auditing and reporting					✓

OneIT's **technology** solutions are a tapestry of services that work seamlessly together.

However, technology solutions are only one piece of the puzzle. The best protection against the most common threats, is educated and empowered employees. Your **people**. OneIT offers email security awareness training, including phishing simulations, to help organizations manage the security problems with social engineering and ransomware attacks. As an extra measure of protection, we also offer dark web scanning, to alert organizations if any of their users' credentials are for sale on the dark web, so they can take action before it's too late.

A thorough approach to cyber security is rounded out by solid **processes**. Without documented processes to follow, security audits can reveal undesirable results that then create reactive responses, which are often too late. Processes fill in the gaps between organizational expectations and employee behavior, minimizing security risk while improving morale and certainty among staff.