opentext™

SERVICE OVERVIEW

OpenText Security Health Check Service

Cost effective review targeting high-impact, strategic cybersecurity controls

Visibility into current capabilities for 6 foundational security control areas

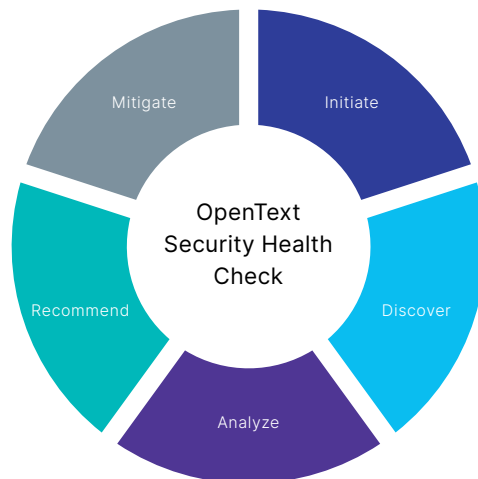**Actionable recommendations** to address gaps and drive security posture

Reduced risk through improved procedures

Organizations must be proactive and resilient when mitigating cyber and regulatory risks. Many have implemented new tools and processes to combat increasing risks, but they may have lost track of core resilience elements in the process. In order to properly prevent and respond to cyber-attacks, it's critical that they maintain a complete picture of their foundational security controls and capabilities.

Businesses must assess risks regularly to ensure that security controls required for compliance are in place and operating effectively. A Cybersecurity Health Check is a great way to achieve these objectives.

Security Health Check workflow

opentext™

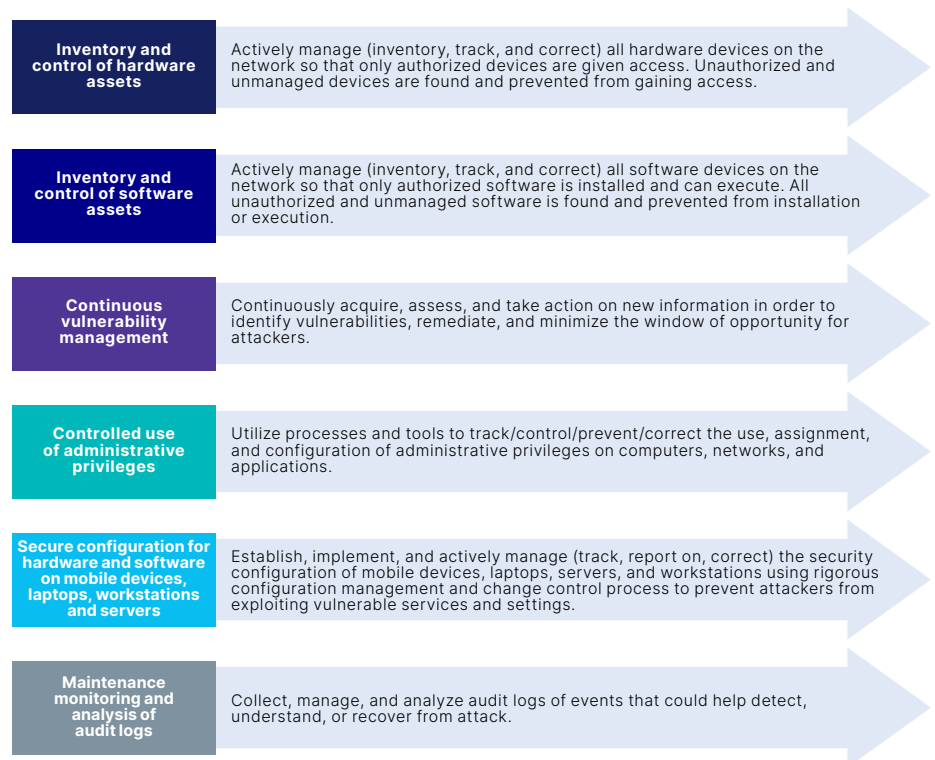## Additional Security Services:

Threat Hunting Service

Cybersecurity Tabletop Exercise

Visibility—Having a clear line of sight to control activity maturity provides valuable information to support informed decision-making. OpenText Professional Services provides an independent assessment of foundational controls that ensures you have your bases covered.

Actionable recommendations—The key deliverable is a security health check report featuring an executive summary, identified risks, and recommendations for improvement. Recommendations are prioritized by the associated risk impact and ease of implementation.

Reduced risk—Recommended action plans are designed to reduce the risk of a cyber incident or regulatory fines.

Inventory and control of hardware assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access. Unauthorized and unmanaged devices are found and prevented from gaining access.
Inventory and control of software assets	Actively manage (inventory, track, and correct) all software devices on the network so that only authorized software is installed and can execute. All unauthorized and unmanaged software is found and prevented from installation or execution.
Continuous vulnerability management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
Controlled use of administrative privileges	Utilize processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
Secure configuration for hardware and software on mobile devices, laptops, workstations and servers	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.
Maintenance monitoring and analysis of audit logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from attack.

Security Health Check controls

To talk to a Security Services expert, please contact **securityservices@opentext.com**

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: **opentext.com**.

Connect with us:

- **OpenText CEO Mark Barrenechea's blog**
- **X (formerly Twitter)** │ **LinkedIn**

opentext.com/contact