Security Controls Overview

Bandwidth has a dedicated information security team that oversees Bandwidth's security program. Bandwidth recognizes information must be managed, controlled and protected as it has a significant impact on our products and customers. Bandwidth's Information Security program centers on ISO 27001 and 27002 to protect assets against unauthorized use, disclosure, alteration, and destruction.

Network security

Bandwidth's network environment is monitored 24x7 by a team of Network Operations Technicians. All site locations have firewalls.

Vulnerability management

Vulnerability scans are performed on Bandwidth's environments and assets daily.

Application security (BW AppSec)

Bandwidth's application security program proactively performs static and dynamic scanning of systems and software code. Continuing education for developers is based on OWASP Top 10 with continuous educational feedback loops in the development lifecycle to bring additional awareness to our secure software delivery.

Change management

All changes to production environments must be reviewed and approved by Bandwidth's Change Review Board. Approval requires risk analysis, test, and back-out plan before any changes can be made. Changes are scheduled during off-peak times to minimize disruptions.

Endpoint security

Bandwidth desktops, laptops and mobile devices are centrally managed and are fully encrypted. All end-user computers have anti-virus and anti-malware protection.

Physical security

Access to all Bandwidth offices is restricted and controlled by assigned proximity badges. Visitors must sign in, display a visitor badge, and be escorted by the sponsoring employee.

Bandwidth hosted data centers are SOC 2 Type II or ISO 27001:2013 certified. Each data center site location provides layers of security, including biometrics, security guards, cameras and equipment secured in isolated rack/cages.

Third-party penetration testing

Bandwidth uses third-party partners to perform external penetration testing against applications and networks at a minimum on an annual basis.

Vendor risk management

The Bandwidth VRM (vendor risk management) program enables Bandwidth to appropriately identify and protect its business data and intellectual property hosted/stored by third-party vendors. Bandwidth evaluates all third-party vendors for data security. Continuous third-party evaluations are done to reevaluate the security posture of vendors for ongoing compliance.

Log/event management

Bandwidth security logs are collected and stored for one year in a centralized logging infrastructure that is analyzed real-time by the Bandwidth Security Incident Event Monitoring (SIEM) system. In addition to real-time threat analysis and alerting, Bandwidth has established a SOC for 24x7 monitoring of events and alerts.

Identity and access management

Access to Bandwidths production systems and services by employees is on a need-to-know model with least privileges. Bandwidth continuously monitors user accounts using security analytics and anomaly detection. Bandwidth requires two-factor authentication for all remote access to Bandwidth networks and systems.

Governance, risk, & compliance (GRC)

Bandwidth's information security program, information security policies, standards, and guidelines, are built on the ISO/IEC 27002 code of best practices for information security. The Bandwidth security team performs ongoing audits and risk assessments across the organization as part of Bandwidth's information security management system.

Incident management

Bandwidth has a formal incident management program and has a dedicated incident response team to assemble and manage incident investigations.

People/HR security

Bandwidth performs background checks on all potential new employees before employment. All new-hires must complete security awareness training at the start of employment and ongoing for all employees.