BANDWIDTH WANTS TO KEEP YOU IN THE KNOW

Security Controls Overview

Security at Bandwidth is a high priority for our network and business. 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 achieved ISO 27001:2013 certification 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, and traffic monitoring deployed.

VULNERABILITY MANAGEMENT

Vulnerability and policy scans are performed on Bandwidth's environments and assets weekly internal and external.

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. Entrances and exits to all sites/offices are under video surveillance.

Data Centers hosting Bandwidth's equipment are certified SOC II or ISO 27001:2013 compliant. Each 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 security posture of each vendor for ongoing compliance.

LOG/EVENT MANAGEMENT

All 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 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 behavioral analytics and anomaly detection. Bandwidth requires 2-factor authentication for all remote access to Bandwidth networks and systems.

GOVERNANCE, RISK, & COMPLIANCE (GRC)

Bandwidth holds the international recognized ISO 27001:2013 Certification for our product and services. Bandwidth's information security program, information security policies, standards, and guidelines, are managed and monitored through centralized GRC platform .The Bandwidth security team performs ongoing audits and risk assessments across the organization as part of Bandwidth's information security management system (ISMS).

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.