druva

White Paper

The Essential Security Checklist for Enterprise Endpoint Backup

IT administrators face considerable challenges protecting and securing valuable corporate data for today's mobile workforce, with users accessing and creating data from a wide variety of locations and networks. Protect your company's critical information against breach and leakage by choosing an endpoint backup solution that features enterprise-grade security with the strongest encryption, access control, cloud and private cloud security features, and data loss prevention capabilities.

Endpoint backup solutions should encrypt data in transit and in store.

1. Encryption

Because endpoint devices frequently connect to unprotected networks, endpoint backup solutions should encrypt data in transit and in store to prevent unauthorized viewing of sensitive corporate data. Data in transit should be protected with encryption like 256-bit SSL, which allows users to securely access corporate data without the use of a VPN. Data in store should be protected with encryption like 256-bit AES, which has been established by the National Institute of Standards and Technology (NIST) and adopted by government, financial institutions, and other organizations that require the highest level of security.

2. Access control

Endpoint backup solutions should offer secure access that is easy for IT to manage. Web-based access to the administrative control panel and client should be over HTTPS, to provide authentication of the website and web server and encrypt communication between the client and the server.

To make managing user access easy, some endpoint backup solutions offer single sign-on capabilities through Security Assertion Markup Language (SAML), which permits users to securely log into the backup client using their credentials on external identity services such as Microsoft Active Directory. This allows organizations to use their existing identity management policies with the endpoint backup solution.

Less than half of users enable passwords for their mobile devices,[1] so choose a backup solution that allows administrators to mandate that employees use a PIN to access the backup mobile app. This regulates access to corporate data from the app, even if the device itself isn't password-protected.

1. http://kraasecurity.com/data-breach-problems-with-byod/

Choose a solution that is compliant with international standards such as SAS 70 and ISAE 3000 Type II.

3. Cloud security

With so many cloud solutions out there, you should be confident that the endpoint backup solution you choose sufficiently protects your corporate data. Ensure enterprise-grade protection by choosing a solution that is compliant with international standards such as SAS 70 and ISAE 3000 Type II. These external audits assess all aspects of cloud infrastructure, operations, and control, including facilities, physical security, storage and network infrastructure, firewalls, network configuration, account management, and more. Cloud backup solutions should segregate each customer's data from other customers' and use unique encryption keys for each customer. Each customer's unique encryption key should be further encrypted to prevent the key from being compromised. Avoid solutions that save the encryption key in plain text on the client device or server. Instead, look for solutions that feature a sophisticated digital envelope encryption model, where encryption and authentication keys are mutually shared between the customer and the cloud, so that the cloud service provider does not have any access to customer data.

4. Private cloud security

For private cloud deployment, select a solution with server architecture that protects your network from intrusion by allowing you to block your inbound firewall ports from unsecure inbound connections. This can be done by placing an edge server in a subnetwork with limited connectivity (demilitarized zone), while the cloud master and storage nodes remain behind the corporate firewall. Incoming backup and restore requests from outside the corporate network are forwarded by the edge server to the cloud master over a secure connection. Authentication and storage of data therefore occur behind the corporate firewall without opening any inbound ports.

34% of data breaches occur as the result of a lost or stolen device.

5. Data loss prevention

34% of data breaches occur as the result of a lost or stolen device.[2] Protect data on laptops, smartphones, and tablets from breach and leaks with an endpoint backup solution that includes data loss prevention capabilities. Endpoint backup solutions should encrypt files on devices by leveraging endpoint operating systems' built-in encryption technology, such as Microsoft Encrypting File System. Administrators should be able to easily configure which files and folders are backed up to ensure that sensitive corporate data is protected without requiring full-disk encryption.

Endpoint backup solutions should include geo-location and remote wipe capabilities. Administrators should be able to pinpoint the exact location of an endpoint device at any point in time and initiate a remote decommission on a lost or stolen device, as well as configure an auto-delete policy to wipe data if a device has not connected to the backup server for a specified number of days.

6. Audit Trails

With the proliferation of data on laptops and mobile devices, organizations need to maintain visibility and control of how regulated data is being accessed, shared, and distributed in order to ensure compliance. However, only 19% of IT professionals say their organizations actually know how much regulated data is on endpoint devices like laptops, smartphones, and tablets (Ponemon Institute).

If your organization deals with regulated data, audit trails are an essential feature for meeting compliance needs, as they allow stakeholders to see how, when and where data is being accessed, shared, stored and deleted. Audit trails provide IT with insights into data activity so that administrators can be on top of data risks. When audit trails are combined with global policies that let administrators set privileges around data access and sharing, regulated organizations can ensure compliance of endpoint data.

2. http://www.esecurityplanet.com/hackers/symantec-attacks-on-the-rise-but-spam-and-botnets-down.html

About Druva

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com

Q416-CON-10566