Enabling Zero Trust Remote Work

April 2020

Braxton-Grant TECHNOLOGIES

bitglass Next-Gen CASB

Overview

The pandemic of 2020 has driven a surge in the remote workforce as organizations attempt to enable business continuity. Such a paradigm forces IT teams to revisit their infrastructure to balance security with productivity. This guide identifies the essential components of a solution as follows:

1. **Identity and Multi Factor Authentication (MFA)**: Strong identity management via Single Sign-On combined with MFA is an essential component.
2. **Access Control and Data Loss Prevention (DLP):** Access to corporate data must be controlled with respect to the context of the access depending on the user, location, type of device, sensitivity of the data, compliance requirements etc. Furthermore, policies must be enforced on content flowing into and out of applications, based on the context of the flow.
3. **Zero-Day Threat Protection:** subject to greater risks from hacking and malware. Protection from threats is essential across devices, networks and apps.
4. **Visibility:** Regulated organizations must retain access logs for remote workers to satisfy compliance requirements.

Requirements

Remote workers need access to Public Cloud Apps, the Web, and Internal Applications, from both company managed devices and unmanaged personal devices used by employees, contractors and partners.

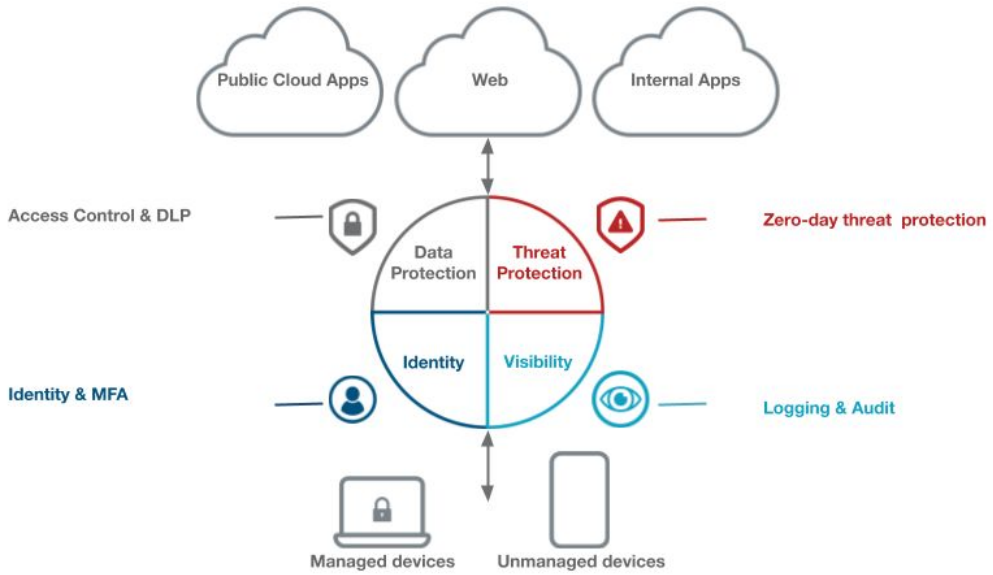

Fig 1. Security Requirements for Remote Work Enablement

At the same time, security considerations require

1. **Identity and MFA**: Strong identity management via Single-Sign-On and MFA is an essential component. Remote workers are subject to greater risks from phishing attacks, and MFA is a critical second line of defense.
2. **Access Control & DLP:** Access to corporate data must be controlled with respect to the context of the access depending on the user, location, type of device, sensitivity of the data, compliance requirements etc. Furthermore, DLP policies must be enforced on content flowing into and out of applications, based on the context of the flow.
3. **Zero-Day Threat Protection:** Remote workers operate off the corporate network and are subject to greater risks from hacking and malware. Protection from threats is essential across devices, networks and apps.
4. **Visibility:** Regulated organizations must acquire and maintain access logs for remote workers to satisfy compliance requirements.

In the following sections, we will examine the above requirements in the context of Public Saas Applications, Web browsing, and Internal Applications.

Public Cloud Applications

A typical enterprise may use dozens of public cloud applications such as Office 365, G Suite, Salesforce, Box, ServiceNow, Tableau etc. While these application providers secure their infrastructure, the applications themselves are freely accessible by any user, on any device, from anywhere in the world. As a result, it is the responsibility of the organization to secure their data as resident in their tenants on each application.

A common pitfall is a reliance on the application vendor to provide application controls. Because each vendor is most familiar with its own products and commercially optimizes the security for their own applications, this approach creates disjointed and heterogeneous security across applications; and unintentionally creates security gaps and becomes a management burden for security teams.

Recommendations

Tools required: SAML IdP with 2FA; CASB with real-time proxy for threat protection and DLP on any device across every application; End-point protection software.

1. **Identity and MFA**: SAML SSO with MFA must be enforced on every Public Cloud Application.
2. **Access Control & DLP:**
    a. Access to applications must be controlled by context, user, group, country of location, type of device etc.
    b. DLP policies should control the type of data that can be downloaded to the device. For example, files containing sensitive data such as PII, PCI and PHI must be blocked on unmanaged devices. Enabling controlled access from unmanaged devices is critical for remote workers, to cover the contingency that the user's managed device might fail.
    c. Conversely, some sensitive data must be blocked, masked or encrypted on upload to some applications, managed or unmanaged, e.g. PHI, PCI or PII may not be transmitted by email or posted to social media.
    d. Sessions must time-out when devices are left unattended
    e. An option must also be available to secure data at rest

3. **Zero-Day Threat Protection:**
    a. Reputable third-party End-point Protection software must be installed on all managed devices.
    b. All uploads into cloud applications from unmanaged devices must be scanned for malware prior to transmission to the application. This is particularly important for applications that are widely shared or deeply integrated into backend systems. For example, a file sharing application can spread malware very quickly to hundred or thousands of users. Likewise, HR applications are deeply integrated into payroll systems, and malware uploaded into such an application can cause major damage.
4. **Visibility:** Log all activity on all applications, whether from managed or unmanaged devices. Logs must be retained as required for ongoing compliance.

Web Browsing

Remote workers accessing the web from managed devices are exposed to threats and data leakage risks. The traditional approach that connects users to the corporate network via VPN fails when most users are remote. The load on the VPN firewall is too high, and performance bottlenecks affect usability. To overcome this, we recommend an approach that pushes processing to the edge and uses direct-to-cloud connectivity using an elastic direct-to-cloud Secure Web Gateway capable of handling shifting loads.

Recommendations

Tools required: Elastic Secure Web Gateway (SWG) in the cloud.

1. **Identity and MFA**: On managed devices, access to the SWG must require authentication via corporate SSO.
2. **Access Control and DLP:**
    a. Web browsing must be restricted to appropriate content.
    b. All uploads into the Web must be scanned for sensitive data and appropriate policies to block or log such data enforced.
3. **Zero-Day Threat Protection:**
    a. Block access to risky URLs entirely
    b. Reputable third-party Endpoint Protection software must be installed on all managed devices.
    c. All downloads from the Web must be scanned for malware and blocked as appropriate.

4. **Visibility:** Log all Web browsing activity, and retain as required for ongoing compliance.

Internal Applications

Remote workers also need access to applications within the corporate network. The traditional approach is to have these users connect to the corporate network via VPN for security. Such an approach is feasible when only a few users are remote, and access is restricted to managed devices. However, when most users are remote, the load on the VPN firewall is too high, and performance bottlenecks affect usability. Furthermore, VPN access from unmanaged devices is infeasible. To overcome these limitations, we recommend the Zero Trust Network Access (ZTNA) tools.

Recommendations

Tools required: ZTNA connectivity.

1. **Identity and MFA**: On managed or unmanaged devices, ZTNA must require authentication via corporate SSO and MFA.
2. **Access Control & DLP:**
    a. Access to resources must be contextual, based on user, group, application, location, type of device etc.
3. **Zero-Day Threat Protection:**
    a. Access must be restricted to devices with up-to-date and reputable third-party Endpoint Protection software.
4. **Visibility:** Log all activity, and retain as required for ongoing compliance.

Other Considerations

In this section, we examine other factors that are relevant to the solution architecture such as operating cost, complexity, scalability and uptime.

Recommendations

1. We recommend solutions that are entirely cloud delivered to reduce cost and complexity. Solutions that are deployed on public cloud infrastructure deliver better uptime and scalability.

2. Broadly speaking, solutions from independent security vendors offer greater security and flexibility than those from application vendors that are tailored to specific applications.
3. Endpoint security solutions integrated with the device limit cross platform flexibility and are prone to failure.