riverbed

SOLUTION BRIEF

5 Essential Device & Application Security Mitigations

Strong cybersecurity strategies have become mission critical because interrupted business leads to financial loss, employee, and customer dissatisfaction, as well as damage to your integrity and reputation. So, the question remains: How can IT reduce and mitigate cybersecurity risk?

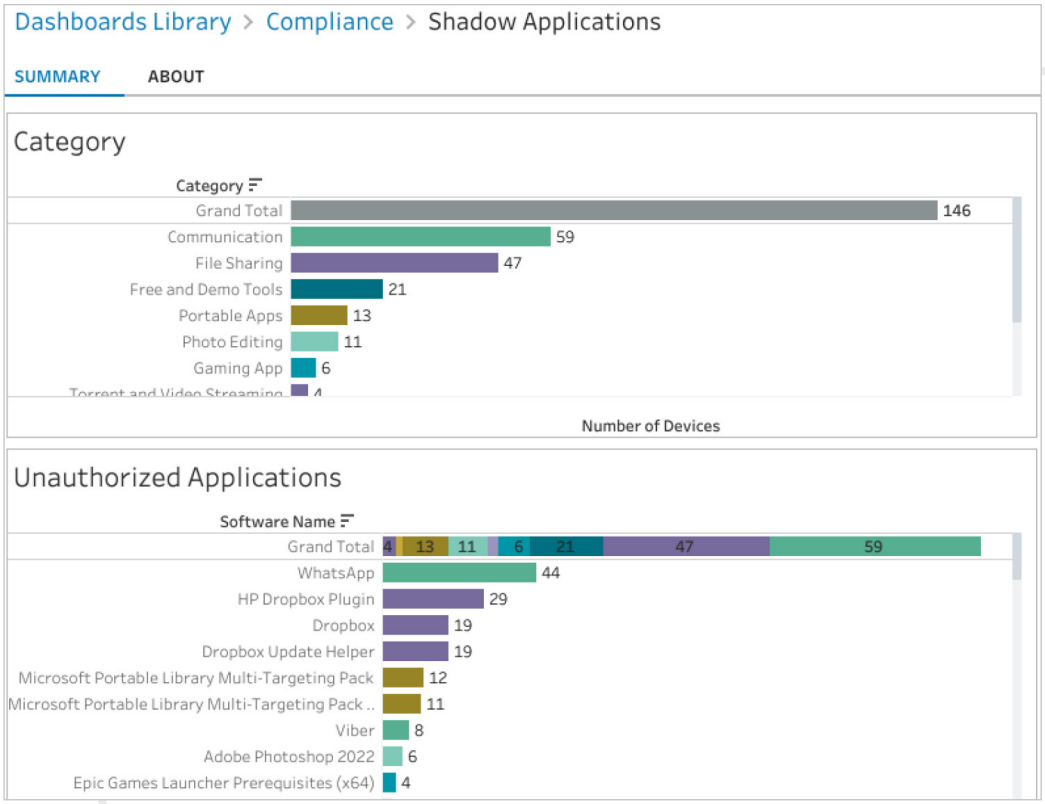
In this piece, we list countermeasures that all enterprises and government agencies should move toward for securing end user devices.

Mitigation 1: Application Control

With so many users working remotely – some using their own devices – how can you know exactly what applications are installed and running on their devices?

Then there's 'Shadow IT' – applications or technology tools not approved by IT. Shadow IT is deployed when business units or small groups of employees are trying to be more productive. But, as we are discovering, these apps can be far from secure.

What you need to protect your systems and data is a monitoring tool that offers clear visibility into what applications are running on which user devices across your enterprise. Knowing this offers you greater control, and therefore security.



Alluvio Aternity provides an overview of any unauthorized apps, such as WhatsApp, DropBox, uTorrent, or Google Docs. It then allows you to drill down by country, department, and individual device name – providing the information the Service Desk needs to identify and remove commonly exploited consumer applications.

Mitigation 2: Patching Applications

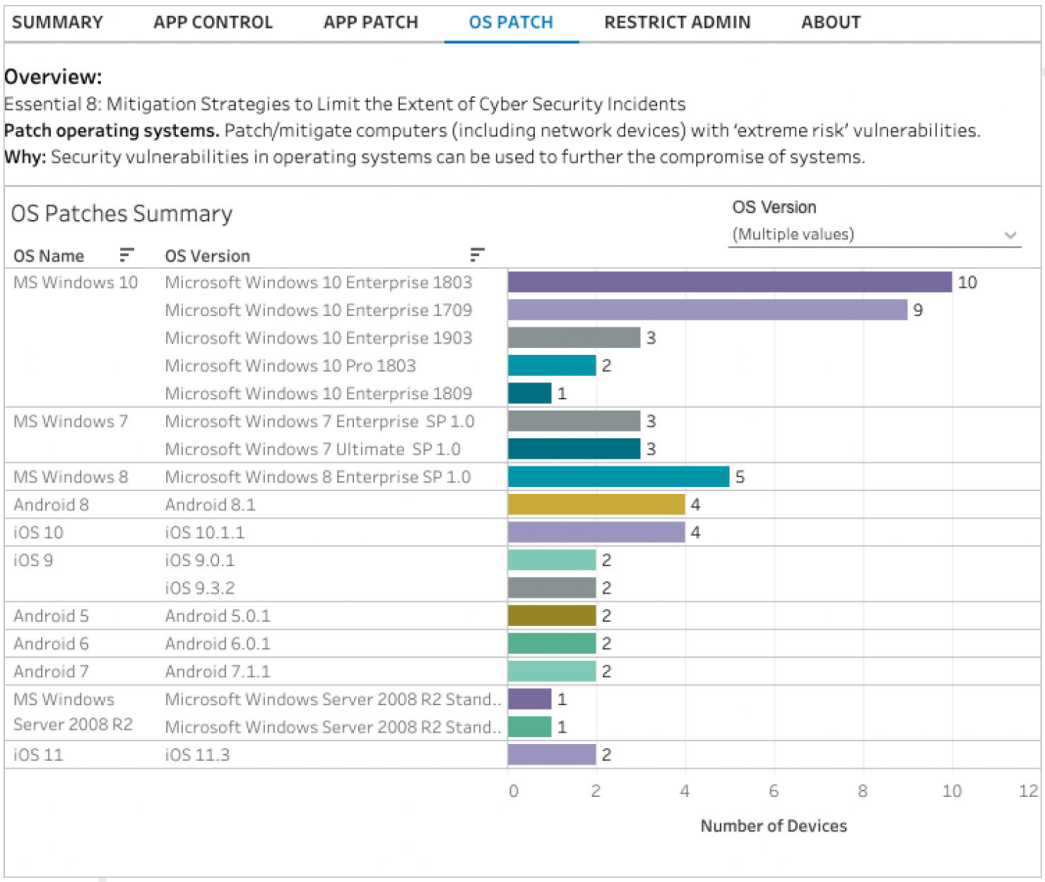
Out-of-date application versions on devices are a significant source of vulnerabilities. Patches and updates often contain bug fixes to security vulnerabilities that eliminate potential back doors, and often improve user experience with new application features.

Alluvio Aternity™ identifies all versions of corporate applications such as Microsoft 365, Citrix and Acrobat Reader used by your workforce. As an example, many organizations find that their users are running 30 or more versions of Citrix Receiver or AutoCAD – even outdated versions of Zoom or Microsoft Teams.

Knowing this information allows IT administrators to pinpoint exactly how many versions of apps are being used, who among your users have outdated versions, then take action to apply relevant patches or updates.

Mitigation 3: Patch Operating Systems

Most environments utilize a range of operating systems across user devices. Microsoft provides regular operating system (OS) security updates, but once this support service ends (i.e., Windows 7), the operating system will no longer receive security updates. This leaving user devices unprotected against hacks and other cyber exploits.



Alluvio Aternity displays the full range of operating systems across your environment.

Mitigation 4: User Application Hardening

IT should remove all Java or Flash. Both executable services are acknowledged sources of cyber exploits such as malware downloads.

The Adobe Flash Player is no longer supported as of January 2021. Although it's blocked in all modern browsers and it's not uncommon to still see it on devices. If you still have a local copy of Flash, you should uninstall it. This will keep you safe from any future security issues since Adobe isn't updating it anymore. Meanwhile, Java is vulnerable to log injection attacks and trust exploits that follow access-control vulnerabilities. It also should be removed from all devices.

Alluvio Aternity enables IT teams to identify precisely which apps and devices are running Flash and Java. It also enables IT to see the implications on applications and users before blocking Flash and Java, so they can perform necessary actions first.

Mitigation 5: Restrict Administrative Privileges

Remove retired or unused administrative accounts to prevent access of sensitive data.

According to breach reporting, malicious or accidental misuse of administrative privileges remains a major vulnerability. Administrative accounts are the 'keys to the kingdom'. Malicious insiders or external attackers can use these accounts to gain unauthorized access to information and systems from within or outside the organization and use that for malicious purposes.

Aternity prescribes a range of processes for strictly controlling privileged access. These include validation on establishment, limitations on external access and – at higher levels of maturity – the automatic revocation of privileges after a time of inactivity and disablement after 12 months – unless revalidated.

Because historical administrative accounts holding the 'keys to the kingdom' can lay dormant if forgotten, Alluvio Aternity offers complete visibility over current holders by username, device name, department, and IP address. This enables IT to review and validate admin privileges – closing loopholes that could potentially be exploited by past contractors or employees.

Visibility Strengthens Security

The ability to progress through these 5 mitigation strategies has much to do with visibility. Without a clear picture of potential security vulnerabilities on all devices, applications, and more, IT has little chance of limiting them.

Given that the user devices are often 'wild cards' in your cyber defense, especially remote devices, the first step is to gain the visibility you need to act. Alluvio Aternity offers valuable visibility to implement and maintain proven mitigation strategies that reduce compromises.

riverbed

Riverbed – Empower the Experience

Riverbed is the only company with the collective richness of telemetry from network to app to end user that illuminates and then accelerates every interaction so that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed offers two industry-leading solution areas – Alluvio by Riverbed, an innovative and differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users, whether mobile, remote, or on-prem. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com/unified-observability.