jamf

WHITE PAPER

Conditional Access: Going Beyond Perimeter-Based Security

The Modern Workplace and the Next Generation of Security

For decades, organizations built “walls” around their company and leveraged network perimeters as the first line of defense. But as workspaces have become more fluid, the security perimeter has changed. The concept of creating a network and protecting it by firewall may not be enough. It’s time to rethink a traditional, perimeter-based security model.

The days of all office workers clocking in at 9:00 a.m. and clocking out at 5:00 p.m. are a thing of the past. People don't simply work from the office Monday through Friday. They work at home, coffee shops, hotel lobbies or job sites at flexible times that work for them. And when they do, they not only require access to company resources, they need access outside of "traditional" business hours. The new "workspace" is fluid and people now need the ability to use tools and consume data across devices, apps and locations.

This is where the cloud comes in.

Cloud services beyond the firewall are the building blocks of this new worker-centric flexible environment. And these services provide greater access to information by allowing users to log into any webpage or app from any machine and access information. And modern cloud services enable organizations to automate their operations at a fraction of what many of those services used to cost.

This workplace transition and growing reliance on the cloud is more than a passing fad, as cited by Vladimir Petrosyan, senior product manager at Microsoft, during his Jamf Nation User Conference 2017 presentation:

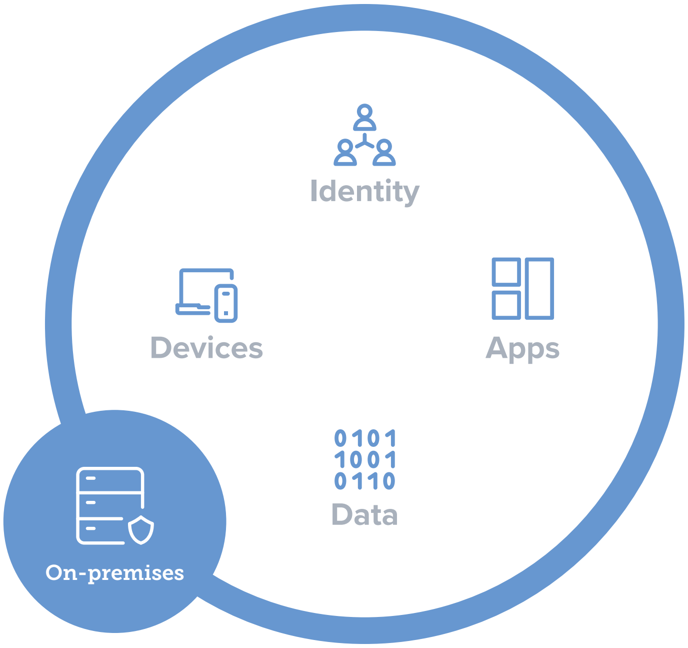
- **85 percent** of organizations keep sensitive information in the cloud
- **80 percent** of employees use non-approved SaaS apps for work
- **41 percent** of employees say mobile business apps change how they work

As more businesses look to evolve with the changing landscape previously driven by shadow IT, security parameters and how they protect users, devices and apps must also progress. While on-premises infrastructure and servers are still used for many critical apps and services, the growth in cloud-based tool use across organizations is being driven by content and collaboration platforms, cloud office suites and the use of mobile devices that store data off-device. The reality is that not only are employees working outside the firewall, but most of the applications and data they access is in the cloud. Not to mention, many are attempting to access organizational resources from their personal devices. More companies have also begun moving their infrastructure to the cloud, calling for strengthened security to access corporate services. Thus, companies are searching for new and better ways to remain compliant and secure.

The key is striking the right balance of empowering users to be their most productive and keeping valuable company data protected.

THE SECURITY SHIFT IN TODAY'S ENTERPRISE

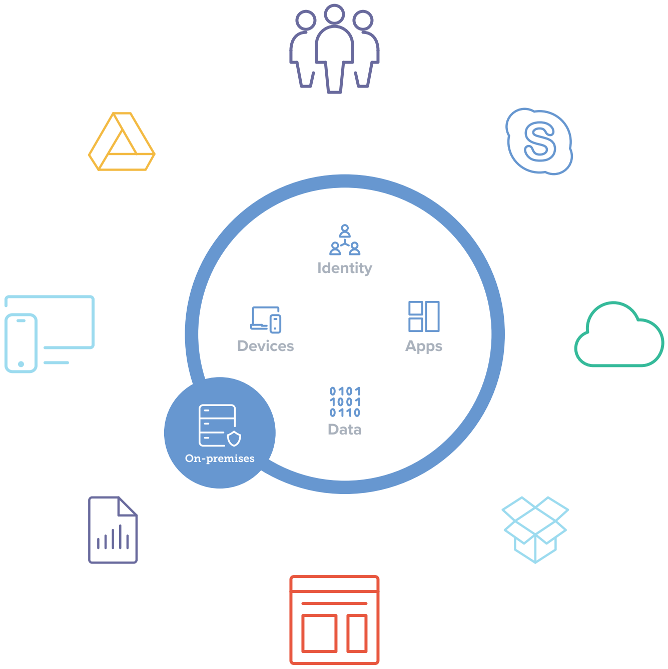
The security perimeter has changed. The concept of creating a network and protecting it by firewall doesn't fully apply anymore because devices and data are no longer hosted on-premises. Devices are used worldwide and can directly access cloud services, email applications and other potentially sensitive corporate resources anywhere, anytime.



Traditional Security Model

Above is an example of a traditional security model with protection perimeters behind the firewall.

But this represents just a small portion of what our coworkers and their devices now access. Cloud storage, productivity apps, across multiple devices outside the firewall is the new norm. Given the pervasive nature of what we now rely on, it's easy to see how vulnerable organizations are if they continue to leverage a perimeter-based security model.



Modern Security Model

Organizations can no longer use traditional on-premises identity management to provide access to services, since the majority of devices and the resources users require are moving to the cloud. To alleviate potential security vulnerabilities and keep users productive — no matter where they are — it's time to rethink a traditional, perimeter-based security model where the identity is as globally accessible and elastic as the cloud services we are accessing.

DEVICE AND ACCESS: SECURITY LAYERS

There are three common factors to security and authentication, none without its flaws:

- Device-based security
- User-based security
- Multi-factor authentication

Device-based security

This security method can apply to managed corporate devices or managed devices that are not compliant with an organization's security policies. This security model fails to protect the device if credentials are obtained through phishing or a "lucky" guess. Additionally, if a device isn't managed — which many are not — they are not secure and compliant with an organization's standards.

User-based security

This security layer can apply to devices that use a user's username and passcode to access. But, if an unmanaged device or computer that has access to corporate services and resources is lost or stolen, or a user's credentials are maliciously obtained, the entire network is at risk.

Multi-factor authentication

Multi-factor authentication is a security layer where a user is granted access to their device and company resources only after successfully presenting several separate pieces of validation. Examples of personally identifiable credentials include:

- Something you know (a password)
- Something you have (a security token)
- Something you are (a thumbprint)

While requiring a username or passcode, as well as a secondary physical authentication method (such as an RSA token) may seem like a foolproof way to validate the user, organizations still lack tools that allow them to tap into the rich tapestry of context devices can provide, as well as methods to secure the broad set of use-cases, users, and locations that come along with them.

The moral of the story is that a secure user or physical authentication may not be enough. Organizations must require both and then some, without compromising the end user experience.

IDENTITY IS THE NEW PERIMETER

There are a number of vendors who have emerged to help manage identity and access to services, including Centrify, Duo Security, Microsoft, Ping Identity, Okta, Sailpoint and Salesforce. Many of these tools can work with existing authentication infrastructure, such as Active Directory, and extend those identities to cloud services using protocols such as Oauth, SAML and OpenID.

Identity is the one commonality across all of a user's devices, and can transcend simple user, device or token-based security. Factoring identity management into your security management process is key to creating a secure environment in a mobile, cloud-computing world.

"Security breaches and attacks have reached a sophistication level and spread rate where human minds and human hands just can't do it on their own," according to Brad Anderson, corporate vice president of Microsoft.

Organizations require a set of capabilities that help understand identity risk, device risk and application risk — and ultimately a guarantee that only trusted users, on trusted devices, using trusted applications get access to data.

> Microsoft Enterprise Mobility + Security is a management framework for securing identity, devices, and data. Read more about EMS at https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security

Through identity-driven security, Microsoft authenticates user credentials against Azure Active Directory (AD) when a user goes to access Microsoft Office 365. This identity authentication is done 15 billion times a day, according to Anderson.

More than 90 percent of the world uses Active Directory as the authoritative source for enterprise identities on-premises. For many of them, Azure AD is the authoritative source for enterprise identities in the cloud. Everything built at Microsoft is built on top of Azure AD in Microsoft's cloud.

A SOLUTION TO THE SECURITY GAP

During the 2017 Jamf Nation User Conference, Anderson offered a new solution to the gap in modern security. "Jamf Pro is using Microsoft Workplace Join functionality, within Azure Active Directory, to join Jamf-enrolled Macs with all the rest of the enterprise's corporate-owned or personally owned devices. Once Workplace Join is complete, Intune can report on it in the same way it reports on Intune-enrolled devices." He continued by saying, "It means enterprises can provide access to their corporate resources not only based on the user's credentials, but also on the compliance of the Mac. It's something we call conditional access."

Jamf Pro, the standard in Apple device management, can enforce policies on devices in order for them to be able to access Office 365, leveraging EMS conditional access. Jamf managed Mac computers now get Workplace Joined in Microsoft's cloud provided they meet the Intune device compliance policies required to do so, which can be custom-tailored to each organization's needs. Once the computer's data is in the cloud, Microsoft Intune and Enterprise Mobility + Security (EMS) can now fully integrate with Jamf to manage those devices.

If an unmanaged Mac requests access to email or other cloud services, IT can enable a user-initiated enrollment process from Jamf Pro and ensure that unsecure or unmanaged devices get under management before being granted access.

Mac policies, such as password requirements, can be defined with Intune and allow IT to apply them systemwide. The Jamf and Microsoft collaboration is unique in its ability to go above and beyond what Apple's mobile device management (MDM) framework allows for, accessing local tools. For example, an administrator can create a configuration profile that enforces and validates the strength of passwords. This bridges the gap between organizational policies and what is available out-of-the-box through traditional MDM options for the Mac.

When user credentials are verified by Microsoft and device credentials by Jamf, in real time, an analysis of the user risk, the device risk (is it compliant or not with an organization's policy) and the application risk (what app is being used) is run to determine whether to grant access or block access from cloud resources.

Where multi-factor authentication falls short in focusing mainly on the user, this new method extends trust to how the user is interacting with information, so that the trusted identity is an authenticated user on a compliant device.

Now organizations get an extension of multi-factor authentication through verified compliance: 1) username and password, 2) code and token, and 3) device compliance — and now organizations can contextually and dynamically provide the right access based on a user, device and the context of that use-case, effectively delivering the adaptive and flexible perimeter demanded by today's multi-device, multi-location worker.

PROXY-FREE CONDITIONAL ACCESS

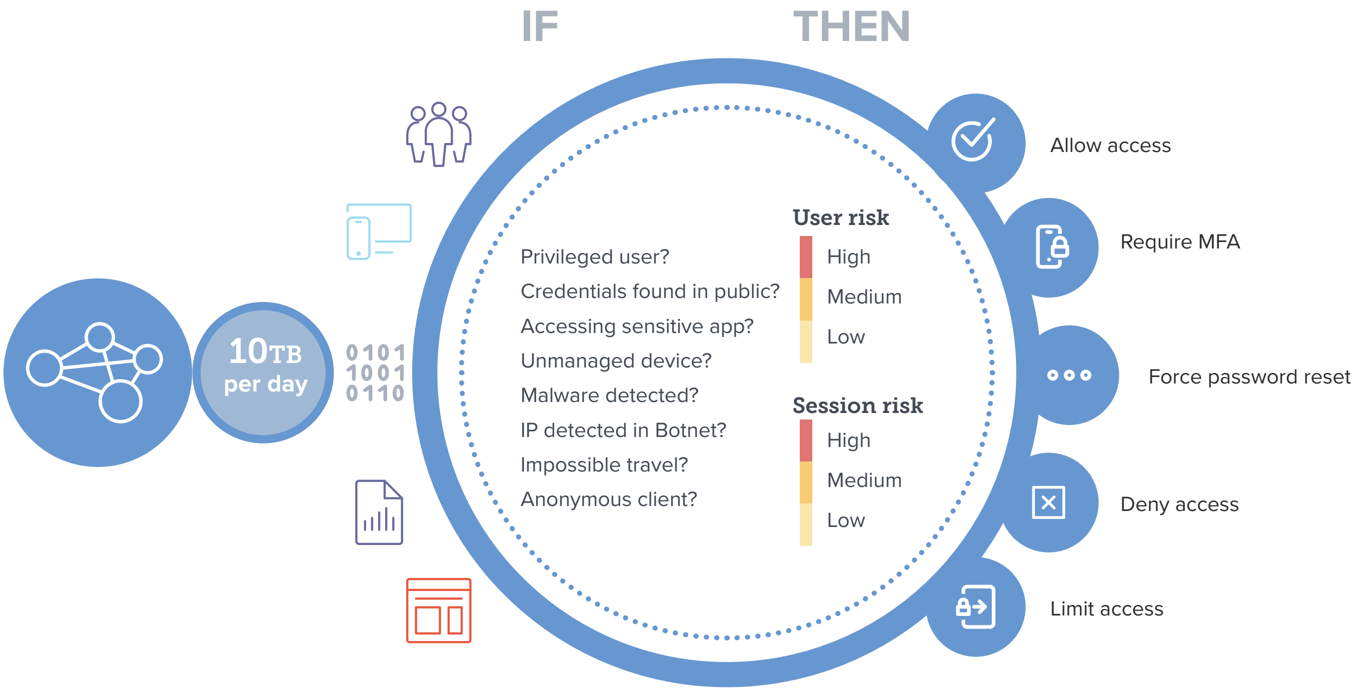
EMS Conditional Access is the key to making this level of security a reality and what provides the ability to automatically verify any risk associated with the identity, the device and the application.

This gives IT the control to define under what conditions users can access your resources.

Many enterprise mobility management (EMM) providers have solutions that support conditional access through a proxy server in order to qualify remote devices to authenticate to resources that live within the network perimeter of an organization. A proxy server is a server that acts as an intermediary for requests from users seeking resources from other servers. This can be for traffic coming into a network or leaving a network. Proxies are not necessary with the unique Jamf and Microsoft collaboration. With the partnership, everything directly integrates with Azure Active Directory as a single source of truth, with compliance of a device being an attribute that can be used as a prerequisite to gain access to various services. This means there is nothing in the middle, such as a proxy server, that requires network configuration to determine access or act as an additional piece of network infrastructure to be maintained. This offers a richer authentication experience built directly into Azure Active Directory and Intune while also allowing for one less point of failure.

Enterprise organizations have accepted and acknowledged the rapid adoption of Macs. That's why they require a solution that goes beyond perimeter-based security, just as they do with their other devices. In layman's terms, before trusting a user, the device that the user authenticates from must first be approved.

Microsoft and Jamf collaborated to create a purpose-built solution that fully integrates with their foundational Azure Active Directory and Intune technology stack, keeping the native experience for users intact and leveraging the strengths of both Jamf and Intune to build a solution for customers that is far and above what each organization can provide on its own.



EMS Conditional Access

MICROSOFT AND JAMF PARTNERSHIP

The Jamf and Microsoft EMS partnership provides an automated compliance management solution for Mac computers accessing applications set up with Azure AD authentication. This collaboration leverages conditional access to ensure only trusted users from compliant devices, using approved apps, can access company data.

Together, Jamf and EMS prevent an unauthorized user from using a device to access specified resources provided by the organization. These devices could be a personal device, an unmanaged device or a managed corporate device that is not compliant with security policies and therefore more vulnerable to security threats attempting to access corporate data. This is accomplished by requiring that the user register devices they want to access Microsoft Office 365 and other applications validated by Azure AD.

What makes this process unique from other vendors claiming conditional access is that devices are not required to pass through a proxy. By avoiding the proxy, organizations enjoy a more streamlined approach to device protection.

And the end user experience? Informative and easy. If a device isn't compliant and a user attempts to authenticate and receive access, the user receives a message on their device saying they do not meet certain requirements. The user can then click on this message and walk through the steps to resolve the compliance issue.

The message lets the user know what's happening and why the device isn't compliant. If it's a password issue, the user simply clicks on "Resolve Issues" and can update their password to become compliant and therefore gain access.

The info that Jamf feeds in to Microsoft makes security stronger and more intelligent, resulting in a better management solution that enables a streamlined end user experience.

AS ANDERSON SAYS, "LOVED BY USERS; TRUSTED BY IT"

To deliver a modern, empowering and secure experience, management workflows need to align with how and where people work, and the tools they use. IT needs to integrate their protection protocols in a natural way and set guidelines so that, if a user is out of compliance, there is a seamless way to bring them back into compliance without risking company data.

Together, Jamf and Microsoft empower IT to do this through identity-based security. This unlocks the world to users and does so without the need to pass through a proxy.

For decades, organizations built "walls" around their company and leveraged network perimeters as the first line of defense, leaving internal security as a bit of an afterthought. Data has moved and the world has changed and these modern solutions are addressing those changes.

Discover how to evolve your security practices so that IT has the tools they need and users remain secure and productive on their device of choice.

Better Security Starts Here

jamf

www.jamf.com

To learn more about how Jamf Pro can make an impact on your Mac and iOS management, visit **jamf.com/products/Jamf-Pro**.