BetterCloud | BeyondID Cloud Service Management WHITEPAPER

A Guide to Effective SaaS Management Using a Zero Trust Security Model

About the Author

This whitepaper was written by Arun Shrestha, CEO and co-founder of BeyondID, in partnership with BetterCloud. At BeyondID, Arun is committed to building a world class organization whose mission is to help customers build secure, agile, and future-proof business. BeyondID is a cloud service management company helping customers acquire, deploy, and manage cloud services as simply, securely, efficiently, and cost-effectively as possible. Arun is fortunate to have spent time with many Fortune 1000 and fast-growing enterprise companies to advise and assist them on strategy, planning, deployment, and management of cloud security and operations.

Prior to co-founding BeyondID, Arun held executive positions over a span of 20 years at Oracle, Sun Microsystems, SeeBeyond and most recently Okta, which went public in 2017. Arun served as vice president of global customer success and services at Okta, senior director of advanced customer services in North America at Oracle, and senior director of professional services in global emerging markets at Sun Microsystems.

Today, the new reality is that network-based security is no longer adequate.

With an increasingly mobile workforce and the spread of shadow IT, plus the rapid rise of cybercrime, companies must find new ways to effectively manage their sprawling SaaS portfolio. They also must seek the ability to offer their core businesses as microservices – securely and seamlessly.

Now, that's a mouthful. Let me elaborate.

Right now, SaaS is creating dozens of challenges (and opportunities) for IT

Cloud and SaaS sprawl

The rise of cloud and SaaS has given companies access to an unprecedented volume of IT resources never before possible. This can boost corporate productivity tremendously, but it also introduces **new IT security challenges** beyond the corporate firewalls. Enterprise companies use over 1,000 cloud applications on average and that number is growing.

Shadow (stealth) IT

Corporate IT can no longer control their IT environment. Business functions are choosing to procure and use many SaaS applications without the knowledge or permission of IT. This phenomenon, also known as shadow (or stealth) IT, is significantly increasing the risk of data breaches and security incidents. Corporate IT has no choice but to get ahead of this by **becoming a business enabler**, not an inhibitor.

The rapid obsolescence of network-based security architecture

The current network-based security architecture is no longer adequate due to the rise of the mobile workforce and the rapidly growing number of applications in the cloud. Once the security perimeter is breached through various forms of cyberattacks (like phishing, malware, or compromised passwords), a threat actor can move freely across other security layers and systems, where data can be compromised.

Cybercrime is on the rise

Cybercrime damage costs will hit **$6 trillion annually by 2021**, which is expected to be the greatest transfer of economic wealth ever. Cybercriminals are targeting more people too: An estimated 6 billion people will be internet users by 2022, up from 3.8 billion people in 2017. Hackers continue to use every mean possible to hack into systems and data, including critical SaaS applications such as HRIS, ERP, CRM, productivity suites, and data repositories.

The popularity of microservices

Microservices have gained immense popularity in the last few years. With demonstrable success from Netflix and AWS, more companies are starting to offer their core businesses as microservices to expand their customer and revenue base. That means old and new companies must find a secure and seamless way to expose these services to their customers and partners. Many of these microservices are available as SaaS offerings through publicly supported APIs. Companies can simply subscribe to these services instead of building them from ground up. (For example, see: **Uber's use of Twilio's** communications services to send and receive messages, or **MGM's use of Okta's** identity and access management (IAM) services to manage a seamless customer access and experience across various MGM properties.)

So how does IT address all of this?

You might ask how companies are addressing the amalgamation of challenges and opportunities presented by all of this. Though we are still in the early phases of innovation, there are proven methods to achieving a higher degree of maturity for managing sprawling applications in the cloud.

A proactive cyber defense posture is a must. Companies must proactively strategize, plan, and execute cyber defense. They must continue to invest in cybersecurity tools and technologies, subscribe to cybersecurity expertise, and retain cybersecurity talent who can stand up impenetrable cyber defense. That means revisiting your cyber defense strategy and standing up new security architecture.

Companies need to invest in a new security architecture. The new security architecture must be flexible in accommodating a global mobile workforce that accesses a growing number of applications in the cloud or on-premise using many types of devices, from anywhere, at any time. Various factors such as users, devices, data, applications, and networks are included in the scope for the new security architecture.

The solution must be secure and seamless. Despite security threats, companies must find a secure and seamless solution that will enhance their customers' experience, improve their employees' productivity and ease of use, and simplify collaboration with their partners.

Hello, Zero Trust

The world is rapidly changing. Apps have moved to the cloud and users are accessing them from anywhere, any time on multiple devices. Despite that, the way enterprises secure access to applications has largely remained unchanged – they are still dependent on the corporate network perimeter.

The new reality, however, is that *people* are the perimeter.

Companies must ensure that as they embark on the cloud transformation journey, their applications remain secure. To do this, they should readdress security and consider a Zero Trust security model.

The best way to architect and implement a new security framework is start with "no trust but verify" model. In other words, every service request made by any user or machine is properly authenticated, authorized, and encrypted end to end. The model has been promoted by Forrester as "Zero Trust" since as early as 2010 and has also been adopted by Google as BeyondCorp.

Inspired by this, companies have started exploring this model and many are already on their way to implementing it. Adopting the model is a journey of its own that requires careful strategic, tactical, and operational planning.

Enter: the Zero Trust security model. In other words, every service request made by any user or machine is properly authenticated, authorized, and encrypted end to end. Here are some considerations to keep in mind.

Key factors to consider when rolling out Zero Trust

The goal: The main goal of a Zero Trust security model is to prevent data breaches.

It's a new version of corporate identity. Zero Trust redefines corporate identity. To prevent data breaches, every service request must be properly authenticated, authorized, and encrypted end to end. The model has to take into account a user's corporate identity, which is a combination of the user plus the device used to request the service at a point in time.

Authentication and Authorization as a Service must be based on many dynamic factors. For example, you should create your access policy framework based on behavioral patterns, which will vary across companies (more on this below). Elements to factor in providing authentication and authorization as a service are group membership, role, device state, geolocation and time-based controls, rules granularity, time for granting/denying access, and configurable policies enabling flexible controls. The agile architecture requires decoupling authentication and authorization service logic (including identity governance) from the core application, which can then support dynamic and evolving security requirements. This trend is here to stay.

Use a centralized access control model for more visibility into user activity. With a central gateway, you can use it to monitor, track, and address any issues.

Enforce security measures that promote a better user security posture. The **best security measures** are those that become everyday habits.

Remove trust from your network. This approach eliminates static credentials, which are the most common source of breaches. Imagine a world without passwords.

Enforce least privilege access. Every module, be it a process, user, or program, must be able to access only the information and resources that are necessary for its legitimate purpose.

Every company is becoming a technology company to compete effectively. Software must be delivered faster and most efficiently to run the core business. This requires companies to adopt a DevOps mindset and use automated systems and streamlined processes to make the most out of cloud computing.

Take inventory of all users' devices and credentials. Authenticating devices is equally as important as authenticating users.

Prepare and understand your current security architecture. Look for gaps and source of vulnerabilities.

Perform data analyses. You must be able to make sense of all the data collected (e.g., devices, credentials, and the current state of your security architecture).

Understand and document behavioral patterns: Every company operates differently; therefore, their processes may vary, as will their user behaviors (both internally and externally). A big part of the solution is to understand and implement security and access policies that take these behavioral patterns into account.

Lay the foundation for your policy framework. Think about **which elements will form the foundation for your policy framework**, and how granular your policies need to be. What can and can't your users do? The rules that make up your policies should be easy to understand, and policies must be configurable to enable custom controls.

Let's get tactical now. What are the critical processes and tools required to implement Zero Trust and achieve effective SaaS management?

Eight steps to implement effective SaaS management and Zero Trust

1. **Use a centralized access control model.** This relies on the core principles of role-based access control with role definitions and governance using identity and access management (IAM) and privilege access management (PAM) products.

2. **Apply strict access controls** to sensitive data, systems, and applications. Only allow access to assets that users need to do their jobs.

3. **Use context-based authentication also known as Adaptive Access** with the ability to step up factors that are required to verify the rightful user who is requesting a service. Factors can be a combination of devices, certificates, keys, login time, geolocation, etc.

4. **Document and understand the current security architecture.** Discover holes and gaps, and develop your future security architecture to plug these holes and gaps.

5. **Leverage user and entity behavior analytics (UEBA)** to look for and alert on abnormal behaviors for a specific user, system, or device, and require step up authentication measures.

6. Establish a policy framework for your org **and write the rules for it.** This should include steps like activation, investigation, remediation, and enforcement of these rules and policies.

7. **Monitor the network.** Inspect and log traffic, and continue to update rules based on your UEBA.

8. **Remediate and enforce in real time.** Get visibility into user activity, apply rule-based dynamic access controls, remediate issues in real time, and enforce these policies either through one-off or bulk actions.

Ten key technologies required to implement effective SaaS management and Zero Trust

1. **IDaaS** for managing workforce and customer user identity, authentication, and adaptive/contextual access management.

2. SaaSOps for securing user interactions **through**:
   - User activity event monitoring and data protection
   - Configuration, entitlements, and settings change management
   - Granular controls with policies and orchestration

3. **IGA** for managing identity governance and administration from access requests, access recertification, Segregation of Duties (SoD), and automation of user lifecycle management including compliance controls required by SOX, HIPAA, PCI-DSS, GDPR, FedRAMP, etc.

4. **PAM** to establish a least privilege access model for protecting sensitive data and applications in the cloud or on-premise including operating systems and workloads.

5. **CASB** to establish a gateway and roll out policy orchestrators for using SaaS apps.

6. **HRIS** as the source of truth to implement joiner, mover, and leaver use cases, and to enable real-time provisioning and deprovisioning for users to access authorized applications, data, and systems. This is critical to reducing the attack surface since most data breaches occur because of compromised inside actors.

7. **SIEM or UEBA** solutions to look for and alert on abnormal behaviors.

8. **ITSM** for incident management, release management, people management, and change management.

9. **Secure Web Gateway** to protect remote offices connected directly to the internet and apply next generation firewalls that can protect both cloud and on-premise systems and applications.

10. **Web and mobile security** to protect web and mobile applications in real time from imitation (fraud) attacks. This technology proactively alerts companies when users' credentials have been compromised.

In conclusion, effective SaaS management leveraging a Zero Trust security model is a journey that requires a thoughtful and comprehensive strategy and architecture. Best implemented in phases with surgical tactics backed by best-in-class technologies and best practices, it should be fully operationalized over a period of time, and constantly optimized on an ongoing basis.