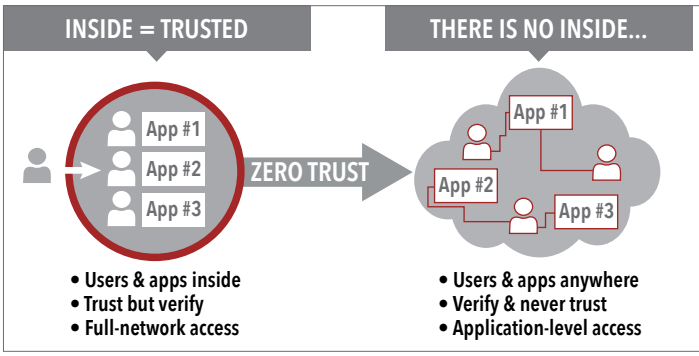
SAFEGUARD YOUR BUSINESS FOR DIGITAL TRANSFORMATION

5 STEPS TO START YOUR CLOUD SECURITY JOURNEY

Digital transformation is omnipresent for today's businesses. Adopting and mastering this transition is imperative, and neglecting to do so means certain loss of mindshare and market share — if not complete failure — in today's agile, ultra-competitive, and hyper-connected world.

Businesses that pursue digital transformation will be rewarded, but not without facing challenges with their ever-expanding attack surface as well as their existing network and security architectures. Successful transformation will require the evolution of traditional enterprise network, security, and application delivery architectures.



TODAY: *Inside = trusted — but users and applications are moving outside the traditional perimeter and threats are moving inside. The traditional perimeter-centric approach is no longer effective and increases risk.*

TOMORROW: *There is no inside and zero trust is key. Evolve to a cloud-based security architecture, which is straightforward and reduces risk. It uses the Internet as its core network, and removes the complexity that businesses deal with around appliance deployment, management, patching, license counts, and more.*

Future state for many businesses may seem impossible to undertake. However, there are simple ways to start the transition today and score some easy wins that can help you reduce risk and complexity, as well as improve agility.

Here are five areas you can focus on to start your cloud security journey today:

1. Establish Effective Monitoring and Reporting

First and foremost, even with the right systems in place, a key component of zero trust is just that … trust no one. From access to applications and data to malicious and unacceptable content to application performance, everything should be monitored, logged, and reported on.

With cloud-based security solutions, you can export data that enables you to not only look at positive and negative security models in your own SIEM tools, but also start to leverage built-in predictive and behavioral analytics.

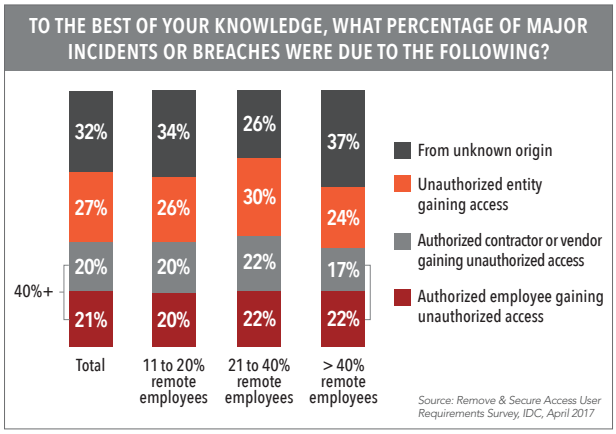
For example, is that 3 a.m. login really a person, or is it a bot? What about traffic leaving the enterprise and connecting to a domain on the Internet? Is it malware command and control communication, an IoT device phoning home, or just an employee trying to access a resource on the Internet?

Full visibility is the first step to effectively applying security policy and enforcing compliance. Adopting cloud-based security helps centralize security policy definition but distribute policy enforcement.

2. Establish New Access Policies

IT must pivot from the common security mantra of "trust but verify" to "verify and never trust" in the new threat landscape. Traditional access solutions grant users full access to the network once they authenticate through user credentials, but is that the most secure approach? Traditional application access approaches require a hole in your firewall, enabling anyone inside of your perimeter to potentially move laterally across your network. Use the concept of least privilege as a guide: Most users only need access to the applications that enable them to successfully do their jobs. This ensures the network remains protected from unauthorized or malicious activity.

If more than 40% of breaches come from authorized users accessing unauthorized systems, why use the traditional access model?



Instead, consider utilizing a cloud security solution to streamline secure access while reducing risk. Look for a solution that enables you to provide access to all applications, regardless of where they are hosted, and provides browser-based, application-specific user access. With this, the user should get authorized, secure access to specific applications, but nothing else on the network. It is also key to obfuscate private enterprise applications and infrastructure from the Internet, which minimizes the attack surface by making enterprise infrastructure invisible. Threat actors can't attack what they can't see.

As you think about potentially utilizing cloud-based solutions for access controls and enforcing security policies, you should consider:

- How often do your users work remotely?
- Should they have full, unfettered network access?
- Is the user an employee or another member of the ecosystem?
- Where are your users accessing applications from?
- What device types are they using?
- Has that device been infected by malicious actors?
- Are you concerned about user credentials being misused or stolen, and a breach occurring?
- Do you need another layer of validation enabled, like multi-factor authentication or client-side certificates?

Evaluating user access is an easy way to start the transition to the cloud.

3. Perform a Health Check on Your Existing Security Controls

In addition to applying "verify and never trust" to users, you should also apply it to devices accessing your applications and data. The threat landscape is becoming increasingly hostile. Targeted threats including malware, ransomware, and phishing are increasing in volume, sophistication, and prevalence.

Most companies have layers of security already in place, but are they really catching everything? Malicious actors are always evolving, circumventing current defense measures, and targeting architectural vulnerabilities inherent to traditional security perimeters.

Simultaneously, users want increased connectivity, open lines of communication, and unhindered application access — from any device, anywhere, at any time. Combine this with the growing reliance on mobile devices, the burgeoning number of connected IoT devices, the increasing prevalence of Bring Your Own Device policies, the inevitable expansion of your ecosystem, and the growing financial incentives for cyber criminals, and it's no surprise that devices are often a point of compromise in security incidents.

Existing security controls are outmatched, and at best static and reactive versus proactive and dynamic. The reality is that your current layers of defense probably aren't protecting you. The best defense is to proactively apply "verify and never trust" broadly, across devices as well as users who access the network. Additionally, complete a health check on your existing security solutions with advanced threat detection and prevention technology to see what your systems might be missing. Once you've completed a health check, you can determine the appropriate plan of action to solidify your defenses.

51%
of organizations have had a global data breach in the past five years.[1]

250,000
Over 250,000 new malicious programs are registered every day.[2]

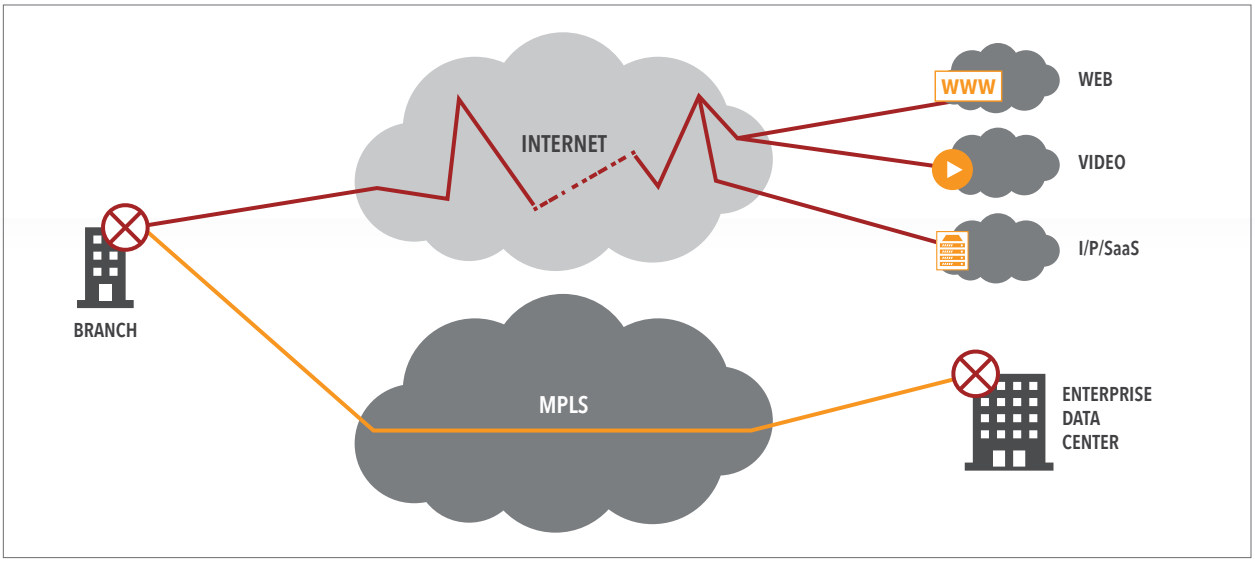
>67%
of workers use their own devices at work.[3]

>20.4 Billion
IoT devices will be installed by 2020.[4]

4. Update Your Application Delivery Model to Offload Your Network and Improve End-User Performance

An enterprise network should be able to accommodate instant, on-demand entry into new regions, peaks in traffic, a diverse user base, and increasingly complex application design. It should also enable IT to deploy new applications quickly and easily, allow delivery and optimization of the entire application portfolio, provide in-depth analytics on the user experience, and handle any type of hybrid network infrastructure.

It's not realistic for IT organizations to establish private network connections between all of their users, data centers, and cloud service providers where their applications are hosted. Nor is it realistic to implement an application delivery box or virtual appliance in every data center, cloud environment, and end-user location. Enterprises cannot rely exclusively on their private WAN to deliver their applications. Instead, consider using cloud-based architecture to take advantage of the ubiquity and scale of the Internet. Although the Internet in its native form is congested, varies in terms of reliability, and is often not secure, it becomes a more viable transport mechanism when controlled and secured with a cloud delivery platform.

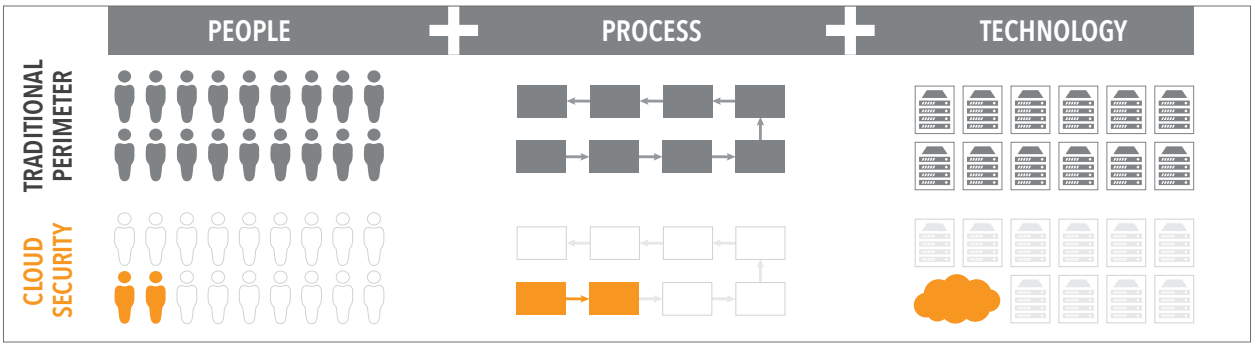


By choosing a cloud delivery platform from a reputable service provider, you can take advantage of web performance technologies like route optimization, which establishes an optimal connection between user and application through the solution's distributed server network; and connection optimization, which can mitigate the effects of latency by performing optimizations such as prefetching and preloading content the user is likely to request next. A cloud-based application delivery platform also helps offload network traffic by caching and delivering at the edge (i.e., closest location to the user), thereby reducing the amount of WAN traffic required and helping to reduce infrastructure costs.

Additionally, a cloud delivery platform further provides a distributed layer of defense against application attacks. Security threats can be mitigated by choosing application delivery solutions that have layered security approaches, obfuscate enterprise infrastructure, and can integrate with your existing identity solutions to control access, in addition to protecting all communications with full encryption.

5. Define Key Capabilities to Validate

Outline the essential competencies to substantiate and prove the migration's progress and success against. The most dramatic and concrete capabilities to validate against will be noticed across impact on people, process, and technology.



Cloud-based security enables IT and security teams to focus on what is important and forward looking, rather than battle daily the complex and brittle systems in place. As such, the number and seniority of security professionals required to monitor, manage, update, secure, and refine security controls will be greatly reduced with a move to the cloud. CIOs can task senior engineers and architects with business imperatives, and a helpdesk professional or application owner can manage application access and rollout in a secure and performant manner. In terms of applying security policy and mitigating advanced threats, the key is to adopt simple, proactive security that is intelligent enough not to require constant care and tuning. This means expedited SLAs, fewer helpdesk calls, less risk, and more satisfied employees. With the scarceness of security expertise, simplicity and automation have never been more critical.

As for process, IT is currently charged with the constant and unenviable questions and actions surrounding changes made to or on the network. It is time to move past the network. Through the adoption of the Internet as transport, DevOps, and continuous deployment, utilizing the cloud streamlines and simplifies process, focusing on ownership and accountability. What's more, the ability to integrate cloud solutions through open APIs into a DevOps and continuous integration workflow will help drive efficiency and speed. As process hurdles and complications are removed, productivity, agility, and velocity will reign.

Finally, on the technology side, a cloud solution breaks the enduring habit and need for racking and stacking new hardware. At this point in IT and technology evolution, the hardware model is unwieldy, difficult to scale, time consuming to upgrade, easily rendered obsolete, and is not centrally managed. Moving into software and migrating to a service in the cloud allows ease of configuration, simple and global deployment, zero downtime, central management, and unified policy across the enterprise.

Other capabilities that can serve as a litmus test for validation include simple, cloud-based service deployment and secure, browser-based, application-specific access including multi-factor authentication (MFA) and advanced threat protection.

To learn more about how Akamai can help you move toward a cloud-based architecture to secure and accelerate your business, visit akamai.com/zerotrust.

[1] 2017 Ponemon Institute Data Protection Risks & Regulations in the Global Economy Study
[2] https://www.av-test.org/en/statistics/malware
[3] CBS Money
[4] http://www.gartner.com/newsroom/id/3598917

Akamai