# 10 Steps to Evaluate Your Access Strategy for Remote Assets

**In a business world dominated by trends like commercial globalization, knowledge process outsourcing, and a shortage of high-quality professionals in many areas, remote access to corporate IT resources is not a luxury—it is a necessity.**

While the need to conform with regulatory compliance requirements may make things more complicated for you, business requirements will prevail—you must deal with the challenge of accessing necessary IT systems from a location other than the office.

The market for remote access tools and solutions is not a young one. It has existed since the dawn of the Internet. Remote access tools offer various solutions from both large and established vendors as well as young innovators. Recent years have brought some fresh demands (particularly around the use of mobile devices in corporate), as well as new solution approaches and architectures.

This document outlines 10 fundamental points that must be considered when either planning a new remote access strategy or evaluating the effectiveness of an existing one.

## Step 1: Identify Different Remote Access Scenarios

When approaching any discussion about remote access strategy, the starting point should always be about the organizational access scenarios. A remote access scenario is a simple description that consists of the following mandatory and optional pieces of information:

**Mandatory**

- Roles/individuals that perform remote access in this scenario
- Authentication means for these roles/individuals
- IT resources accessed (web applications, file repositories, remote desktop servers, Linux servers, and so on)
- Locations of the above IT resources (particular networks in on-premises data centers, public cloud, networks in hosting data centers)
- Types of endpoint devices used for accessing the resources (corporate-owned PCs, mobile devices managed by a certain MDM, and so on)

**Optional**

- Specific client applications that should be used to access these IT resources
- Multi-factor authentication that is required for stronger authentication of users
- Level of auditing that is required for this scenario
- Level of risk/sensitivity associated with the information that can be accessed in this scenario
- Specific restrictions on entities/individuals getting access
- Should the access be allowed only during working days or 24/7?
- Is there a need to restrict the accessing party to performing only specific operations with the IT resource (read-only access, access without the ability to download large documents, and so on)?

While the above list may require some thinking and analysis, not having the ability to compile all of the remote access scenarios in the organization into such a list inevitably means one thing: you probably don't have a remote access strategy, leaving the control of your information and IT resources to a per-case basis. This dangerous approach has resulted in significant data breaches and damage to organizations.

## Step 2: Consolidate Access Infrastructure

In many organizations that we've worked with, consideration of different remote access scenarios had led IT leaders to the inevitable realization that they needed to deploy different remote access solutions to support different scenarios.

Traditionally, organizations would use separate tools for providing access from trusted devices (devices used by employees), such as IPSEC Remote Access VPN solutions versus using proxies and SSL VPN solutions for providing access to third-parties or untrusted devices.

Then, after organizations started allowing access from mobile devices to parts of the corporate IT resources, an additional access infrastructure was created for these scenarios, usually based on solutions provided by Mobility Management. For organizations that provided access to sensitive infrastructure, there would be scenarios with requirements for Privileged Session Management capabilities, leading to the adoption of additional access solutions.

Throw requirements for various public cloud solutions into the mix (IaaS, PaaS, SaaS), season with increasing demand for API access and automation driven by DevOps, and you get a very complex dish. The challenges of having a divided access infrastructure are quite significant.

The list below outlines just the main challenges that have caused harm at companies with such architecture:

- **High TCO:** Not just the cost of each and every solution and the cost of a professional workforce that would be proficient in managing every part, but also the cost of consolidating monitoring, onboarding, and offboarding of users/locations/services, the cost of consolidating and normalizing events, and the cost of integrating each solution into orchestration procedures.
- **Low level of security:** Enforcing uniformly granular policies and handling events in a heterogeneous environment is almost impossible. All organizations that have such environments inevitably reach a point where the organizational security policy is not enforced properly, opening various IT resources to the risk of attack and data loss.
- **End users' confusion:** Different access solutions have different functionality, inevitably leading to the situation where users will wonder why they can access certain IT resources and perform certain operations from one location or device but cannot do it from another. The reason for this is the lack of parity between the capabilities of different access solutions used for different scenarios.
- **Low agility:** Every change in the data center network topologies, onboarding, and offboarding of users and applications would have to take place in multiple systems, resulting in the lower agility and flexibility of the whole architecture.

The Symantec® team recommends consolidating the infrastructure used for various scenarios into an architecture that has as few different access paths as possible.

## Step 3: Use Identity Management

The field of Identity and Access Management (IAM) combines strong identity with RBAC policies but doesn't dictate anything about the access itself. Many IAM vendors partner with Access vendors to provide an end-to-end solution for defining and controlling access to corporate resources. Regardless of the level of consolidation of one's access infrastructure, it is always an industry best practice to manage roles/groups as much as possible with the IAM solution, in order to have maximum control over the onboarding/offboarding of users.

The biggest challenge faced by many organizations is having multiple "sources of truth" for identity without any federated identity solution. Such a situation will cause different corporate IT resources to use different identity providers for authentication and authorization, contributing to the following challenges:

- Inconsistent access control (the same users will have different accounts in different systems)
- Lack of ability to audit and govern access tightly (this might be a strong requirement for any kind of organizational audit)
- Complex onboarding/offboarding and troubleshooting processes

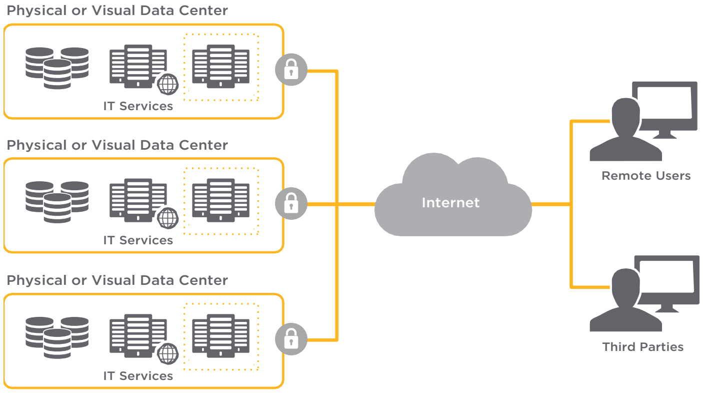
The absolute best practice is straightforward: have a single source of truth for identity and roles in the organization. Using access solutions that can translate organizational identities to global roles for technical interfaces (for instance, User Accounts for Linux Servers) will allow you to extend the role of corporate Identity Management even further in the organization. Such functionality used to be reserved for dedicated Privileged Access Management solutions but has now become more common for the modern DevOps-driven access tools.

**It is always an industry best practice to manage roles/groups as much as possible with the IAM solution, in order to have maximum control over the onboarding/ offboarding of users.**

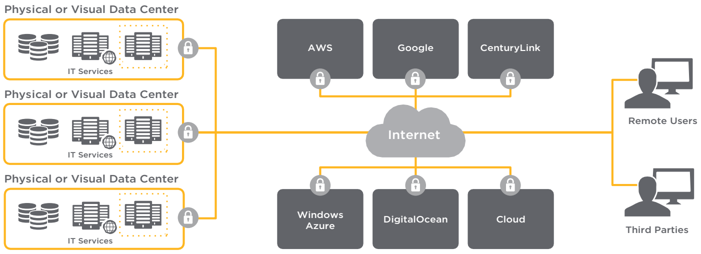
## Step 4: Consider Hybrid Cloud and Multi-Cloud Environments

Building a remote access architecture for environments with a fixed number of data centers was a challenging, but at least achievable, task. Cloud adoption has made this task even more complex.

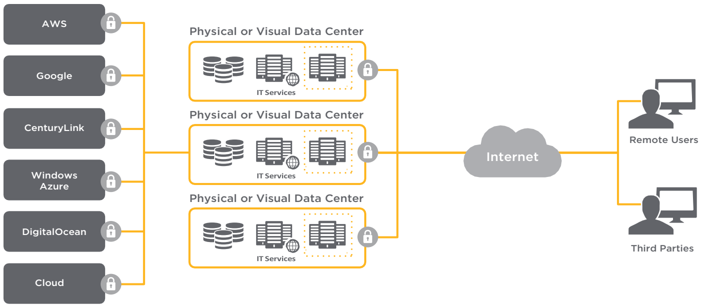
Instead of providing remote access to a fixed number of locations for users, consider something like the below:


Physical or Visual Data Center
IT Services
Physical or Visual Data Center
IT Services
Physical or Visual Data Center
IT Services
Internet
Remote Users
Third Parties

We now have complex remote access to an increasingly large number of enclaves that contain corporate resources, like the one below:



Clearly, the complexities of the two problems are nowhere close to one another. The number of separate networks hosting corporate IT resources in the modern hybrid cloud enterprise is much larger than it used to be. As a result, managing access policies and educating users to connect to various sites becomes increasingly cumbersome and unmanageable. Additionally, managing a dedicated remote access infrastructure at every one of these separate locations becomes an impossible task for corporate IT, leading to pass-through remote access architectures, creating non-granular tunnels between sites and requiring remote access users to pass through one site to get to others, similar to the architecture opposite:



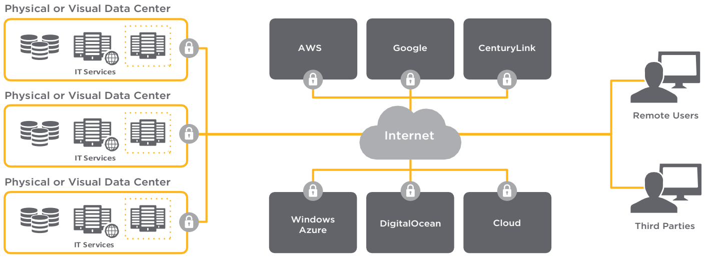
The above approach might be easier to deal with for the users accessing the corporate systems, as they remain unaware of multiple sites, but it complicates the management of the whole environment and ultimately results in poor security policy enforcement and inadequate auditing. The last time user identity played any role was when connecting to the remote access gateway located in one of the original data centers. From that point on, segmenting network access based on user identity and enforcing identity-centric access policy, when routing network traffic internally to another location, is very complex and rarely done.

Additionally, a very common outcome of such infrastructure is high latency for the users, depending on the geographic locations of various corporate data centers. Traffic backhauling becomes a real issue. Consider the following:

- A user based in the United States is working for a company with European headquarters
- The company's traditional data center is in Europe, but the company is deploying cloud-based IT resources in the United States
- The user will access US-based cloud resources via remote access infrastructure located in Europe, experiencing the effects of traffic backhauling

What is the architecture that is suited for hybrid cloud and multi-cloud organizations? As these two are new trends in the IT industry, there is still no definitive response yet. The challenge is definitely there, and new approaches are being offered. The recent Market Guide for Secure Enterprise Data Communications released by Gartner suggests a new direction: Cloud-based Secure Communications providers. In this category, different vendors are taking a step towards cloud-centric access architecture that is particularly suitable for hybrid cloud and multi-cloud environments, as it is located in the cloud itself, and can be delivered from "points of presence" hosted in different geographical regions.

The architecture with such an approach will look like the following:



**The benefits of this approach over traditional architectures presented above are as follows:**

- No need to take care of deploying access infrastructure at each location
- Ability to quickly adapt the architecture to include new locations
- Best possible user experience, without any traffic backhauling
- Uniform security, accessibility, and auditing of corporate resources across any location

Switching from an existing remote access strategy to one based on cloud services doesn't have to be achieved in a single rip-and-replace process. Instead, benefits of this approach can be tested on a per-application or per-scenario basis to see whether this is the right choice.

## Step 5: Perform Scaling, Capacity Planning

Capacity planning for a remote access infrastructure is one of the most important considerations. The challenge is usually that to perform such planning, one must produce answers to impossible questions.

Exactly how many users will access your corporate systems simultaneously? How much bandwidth will they consume when doing this? And how latency-sensitive are their applications going to be? These wonderful, but completely unanswerable, questions are just the tip of the iceberg of the various parameters that should drive the decision on what kind of computer, networking, and storage resources your infrastructure will require.

Some vendors even offer various calculators that can help you understand the load that you will generate on your remote access infrastructure. While seemingly more accurate, these don't necessarily produce results that are more realistic than just a high-level analysis of the use cases.

If you would like to approach sizing of your remote access infrastructure in a realistic manner, consider the following issues:

- The amount of concurrent connections. As your remote access gateways will be performing CPU-intensive encryption/decryption/key exchange operations, the load may grow significantly during peak times.
- Some connections will require low bandwidth (web applications, email clients), while others will require high bandwidth (loading large attachments, high-resolution remote desktop, and so on).
- When working with an occasionally remote workforce, the peaks in load on the infrastructure may become seasonal (during heavy weather more people work from home, and so on).

How does one make sure that the remote access infrastructure will satisfy the needs of the business? Every vendor that provides network appliances will offer impressive quantities of users that every model of the appliance supports, and sometimes, when using a software package that runs on an open server, requirements will be provided in terms of RAM, CPU, and Disk requirements.

These approaches could have worked for the traditional, relatively static, networks, but what happens in modern dynamic networks—networks that consist of dynamic infrastructure, either hosted privately or in the public cloud? How do you even start to estimate the requirements of an infrastructure for accessing the constantly growing number of applications?

That's when the term "elastic infrastructure" starts popping up. What does it mean, exactly? It means that certain aspects of your remote access infrastructure will be able to grow as the consumption grows and, as an additional important feature, those aspects of the infrastructure will also be able to shrink when they are no longer required. This helps the cost of your infrastructure better fit your actual consumption, rather than designing it for peak consumption.

**How do you achieve this? There are three possible approaches:**

- Deploy your remote access solution on a private cloud infrastructure, such as OpenStack or VMWare
- Deploy your remote access solution on a public cloud infrastructure, such as AWS, Microsoft Azure, or Google Cloud Platform
- Consume remote access solution "as a service"

The first two options can be automated to an extent using deployment templates provided by remote access solution vendors in collaboration with infrastructure service providers. Still, it will leave you in a situation where you own the virtual infrastructure that you need to monitor and scale. In very rare cases will this become a fully automated task, as long as the infrastructure is being managed by internal teams.

The third option, available in various flavors, outsources the problem completely. Consuming any kind of IT application as a service means that you never have to worry about uptime and scale (provided you have chosen the right service provider, of course).

In the modern approach to corporate IT infrastructure, our firm recommendation is to rely on external services (as long as they are certified to provide enterprise-grade service) so that you take less operational overhead upon yourself and can focus on the real capabilities critical for the business, rather than re-creating generic infrastructure all over again.

## Step 6: Upgrade, Update, and Patch without Downtime

When your remote access infrastructure is deployed, it should be considered as a critical infrastructure for your organization. Without it, various users are unable to reach the relevant IT resources to perform their functions in the organization. On the other hand, it consists of software packages that need to be updated, upgraded and, if there is a problem, patched. All of the above should happen without creating downtime.

How to achieve this? A traditional data center approach would suggest clusters: duplicate gateways or even "sites" (meaning, a pair of gateways) used for supporting your remote access scenarios. Most existing remote access products support No-Downtime upgrades using clusters, at least, through minor releases and consecutive major releases. Does this approach have any downsides? Why yes, of course—managing a physical or virtual appliance and the related networking is a complicated task. Managing a cluster of these appliances, or even a number of sites, is an even bigger headache.

Just as with the discussion on scaling and capacity planning, an alternative would be consuming access infrastructure as a service, which would, in turn, mean someone else would deal with upgrading and updating the infrastructural components, while being obligated to you via a Service Level Agreement (SLA). Service organizations that provide important infrastructure services should be able to provide very clear and measurable SLAs, as well as clear visibility into the service availability history.

**Proliferation of standard web-based interfaces, accompanied by a RDP/ VDI approach to legacy applications access, makes Application Layer access a much better option for organizations overall.**

## Step 7: Consider Network vs. Application Access

For many years, most of the access infrastructure used by corporate IT organizations focused on providing TCP/IP-level access to various data centers and subnets, assuming that it was the basic requirement to access any corporate applications. This picture is very different now, as our numerous surveys and discovery conversations with Enterprise IT Architects and IT Infrastructure owners have indicated. We see that in modern enterprises, when dealing with business role players accessing various corporate IT assets, the following protocols are used:

| Protocol | Prominence in enterprise networks | Comments |
|---|---|---|
| HTTP/HTTPS-based protocols for Web Portals/ Applications/ Services | >92% | Protocol includes mobile applications traffic and REST/SOAP services |
| SSH | 3–6% | Higher end of the range used by organizations that deploy systems in the cloud |
| RDP/VDI | 2–5% | Higher end of the range used by organizations that are using extensive Microsoft or Citrix infrastructure |
| Special TCP-based protocols | <2% | Legacy applications based on proprietary protocols and "fat clients" |

The table above clearly shows that the vast majority of your users will never need to get network-level connectivity to the data centers. In fact, it makes perfect sense. Most of your organizational users are just information employees who need access to certain data repositories and applications.

Even technical users, that need access to certain services with SSH or RDP protocols, don't ever require access on the network level.

In the past, the amount of dedicated proprietary network protocols for various applications (email, document lifecycle, CRM, ERP, and others) would be very high, resulting in the only possible strategy of providing network connectivity.

In modern networks, more and more applications use standard protocols (usually based on HTTPS) for accessing knowledge management systems, allowing IT infrastructure leaders many more flexible and secure ways of ensuring efficiency of the remote workforce, while maintaining the security of their infrastructure. Proliferation of standard web-based interfaces, accompanied by a RDP/VDI approach to legacy applications access, makes Application Layer access a much better option for organizations overall. Application Layer access brings very significant benefits, both on the operational plane (no need to take care of endpoint agents, manage network segmentation, deal with overlapping internal IP networks, and so on) and on the security plane (significantly reduce the attack surface on the organizational data center infrastructure, eliminate the possibility of lateral movements on the network level, and so on). Avoid broad network-level access when possible, so that you can simplify the organizational networks and significantly reduce attack surface for network attacks.

## Step 8: Monitor Your Access Infrastructure and Handle Security Events

When relying on remote access infrastructure to support business-critical processes, one must definitely consider its resilience and develop a reliability strategy that will include monitoring the infrastructure to ensure its continuous availability.

Monitoring the access infrastructure doesn't mean just verifying that it operates. That's clearly not enough, because when you find out something is out of order, it's already too late. Naturally, your monitoring should be targeted at predictive maintenance, identifying problems before they happen, and mitigating the potential downtime. When running access infrastructure based on physical or virtual appliances, the above is a challenging task.

Surely, these products come with an ability to integrate with monitoring tools (for instance, using SNMP), but typically, these integrations are only good for understanding if the system is operational. When it comes to predicting upcoming problems, usually the owners of such appliances are on their own. In fact, there are lots of communities and even commercial products targeted at smart monitoring of self-owned access and security infrastructure, incorporating a lot of know-how related to the architecture of the access products. This can lead to understanding of potential operational problems.

**Serving the required applications/services to the relevant users is the topmost priority. Identifying and handling potential security events comes as a close second.**

Here are just some examples that require deep understanding of the architecture of the access product used:

- How much disk space is being consumed by log data? How aggressive is the rotation policy and how will it affect the log retention?
- How does the concurrent use affect the utilization of computer/network/memory resources? How can the system deal with the steady growth in utilization that is leading to the inability of the infrastructure to serve the required capacity?
- How does the system identify Denial of Service attempts and manage to work under load?

Modern Site Reliability Engineering doctrines used by enterprise-grade Software-as-a-Service (SaaS) vendors or Managed Services Providers can deliver a significant improvement in the ability to predict upcoming operational issues and to handle problems with the infrastructure ahead of time to ensure its continuous operation.

While it may sound counterintuitive at the beginning, a managed service or a SaaS solution will offer better operational reliability than a self-hosted infrastructure. The logic behind this claim is pretty simple: operational excellence is achieved by investments (in monitoring, automation, replication, and so on) that are only feasible when dealing with scale.

Remote access infrastructure is a critical layer of Information Systems that allows operations for important business processes. While making sure that it is constantly available and operational, serving the required applications/services to the relevant users is the top-most priority of anyone operating such an infrastructure. Identifying and handling potential security events comes as a close second.

What kinds of security events can originate from a remote access infrastructure? Actually, lots of different kinds of events. The list below draws attention to a number of representative cases, but is not all-inclusive:

- **Unauthorized access attempt:** This is the most straightforward security event that needs to be monitored. It simply means that an authenticated person tried to access a resource without authorization. On its own, this event might not be very interesting, but when it comes in masses, it could indicate an attempt to elevate permissions, break in, or use a stolen identity.
- **Usage of a shared/unauthorized endpoint device:** Mapping between the users and the devices gives you the power to identify the situations where there is a mismatch. Such events will be indicative of shared credentials or a potential deception to access information without authorization.
- **Usage of a non-compliant endpoint device:** Clear risk of either intrusion into the organizational resources or data exfiltration from sensitive systems.
- **Sharing/loss/theft of user credentials:** Particularly frequent in third-party situations, this is a very dangerous event, robbing the organization of the ability to audit and govern access to sensitive information in an effective way.
- **Scraping or exfiltration of data from corporate services:** Even when the user is fully authorized to access certain applications or information repositories, it doesn't mean that absolutely anything they do should be considered okay. When a user is accessing simply too much information within a single session, suspicions should be raised and handled.
- **Privilege escalation attempt:** A very clear menace: an authorized user trying to get access to a wider range of information or operations than they should be allowed to.

The ability of a remote access system to deal with events similar to the ones listed above is critical. Some traditionally minded security specialists would argue that the remote access system only provides a tunnel, and that the events listed above should be handled on the application activity level by Next Generation SIEM. The challenge with this approach is that SIEM systems are usually not in line, and to make any kind of enforcement of security policies, they need to launch orchestrated responses that involve multiple deployed products—a reality that usually restricts them to a monitor-only position. We believe that any modern secure remote access system should come well-equipped with capabilities to identify and respond to security threats.

## Step 9: Introduce Adaptive Risk-based Controls

Each access granted (or not granted) by a remote access infrastructure can have a significant impact on business-critical information or processes. Making a policy that is too restrictive will mean robbing the relevant business processes of agility and the availability of users who are involved in them. Making a policy that is too permissive will mean putting business-critical and sensitive information at risk.

How can one build a framework of risk-based controls that ensures business agility and continuity while preventing loss of sensitive data? Consider the list of inputs that such a framework will require in order to perform reasonable risk-based decisions:

- Location of the accessing party
- Device used for accessing the information
- Authentication factors used
- Sensitivity of the application/resources being accessed
- Behavior of the same accessing party across multiple accessed resources

While building a comprehensive policy consisting of risk- based controls is a complex undertaking, it is Symantec's recommendation to verify the remote access solution chosen by your organization can support risk-based considerations and has the capabilities of adaptive controls enforcement. Even if such capabilities will not be used during the initial deployment, as the amount of access scenarios grows, the need to implement them, even if on a per-case basis, will grow as well.

## Step 10: Measure User Satisfaction

Traditionally, considerations for user satisfaction used to be far from the top of the list when it came to evaluating enterprise software. Corporate users were a captive audience for their enterprise information systems, and they had to align themselves to the standards of UX that such systems offered.

Those days are long gone. The enterprise users of today are spoiled by modern user experiences offered by various Enterprise SaaS solutions such as SalesForce, Office365, SuccessFactors, ServiceNow, and more. The user experience of these modern solutions is in line with what all of us are used to in our private lives—accessing our Gmail, Facebook, or any other internet-based service. No wonder that various studies show that the level of complaints from corporate users about the convenience of use of the enterprise systems is at an all-time high (and still on the rise).

**The enterprise users of today are spoiled by modern user experiences offered by various Enterprise SaaS solutions, such as Salesforce, Office365, SuccessFactors, ServiceNow, and more.**

What's the card that users can play in this game? Their availability and willingness to perform their work-related duties remotely and while they're off-duty. If access to their corporate systems is convenient, they will do it from their laptops and mobile devices, they will enjoy doing it, and this process will make a significant contribution to the productivity of the organization. If the users don't enjoy their experience or can't use their favorite devices, your organization's productivity will simply not get that extra bump.

When it comes to remote access, what are the things to consider when trying to measure or evaluate user satisfaction? From our experience, the list below offers a good starting point:

- **Connecting experience:** Do we need to remember many different passwords? Do we have to use inconvenient multi-factor authentication applications/devices? How frequently do we have to re-authenticate if we are working for a long period of time?
- **Working experience:** How quickly does the application load? How quickly does it respond to user operations? Can we still use our convenient copy-paste and other shortcuts?
- **Stability:** Can we count on application availability when we need it, whether for a shorter or longer work session?

If we can accommodate our users with the above, they will respond with higher job involvement and contribution.

How can we measure user satisfaction and understand what our users really think and how it changes over time? The simple approach is to ask them. Sending out surveys and measuring responses over time can bring in information, but it will always provide inaccurate results for the following reason: people who are unhappy will always be more interested in providing the feedback, whereas people who can just work with the infrastructure won't care enough to express this. The only measurement that will provide a clear picture has to come from the access infrastructure solutions. This way, the results will include all of the activity—from both satisfied and unsatisfied users.

## Summary and Recommendations

This document summarizes what a modern Enterprise Remote Access Strategy should look like. We have become avid advocates for modern IT architecture, based on the following principles:

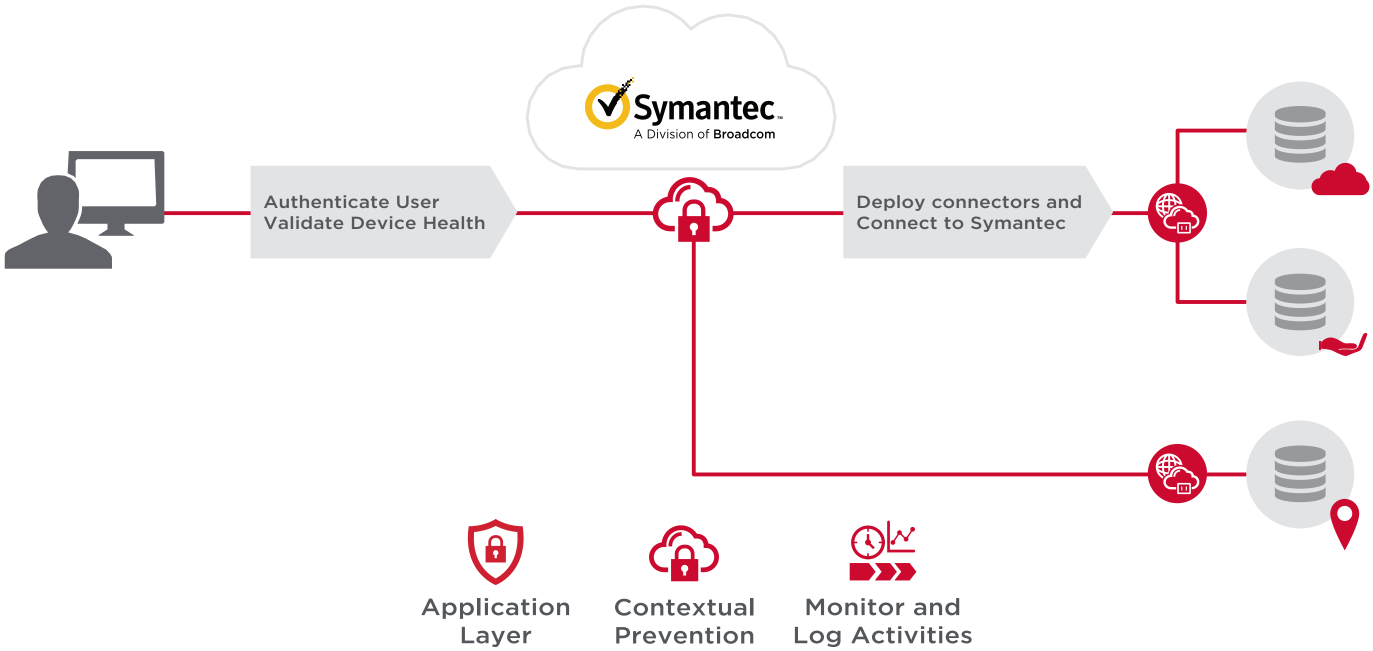
- Default-deny configuration, not exposing any part of the corporate infrastructure to unauthorized parties
- Reliance on Identity Providers and IAMs for governing access to corporate assets
- Consolidation of infrastructure and reliance on services (rather than self-hosted/managed appliances) wherever possible
- Introduction of application layer (Layer 7) access instead of network (Layer 3/4) connectivity, that allows you to both eliminate classes of attacks on the corporate infrastructure and to introduce contextual governance of data and behavior

The above principles are in line with frameworks evangelized by the leading analysts, as well as projects implemented by innovative companies, such as Google and Amazon Web Services. The points listed in this document could be implemented either as a group or separately. Evaluating existing remote access strategies in light of these points could help prioritize gradual refactoring projects targeted at improving the existing environments and making them better suited for fitting the organizational goals.

## Symantec® Secure Access Cloud™

Symantec enables security and IT teams to create Zero Trust Network Access architecture without traditional VPN appliances. Symantec Secure Access Cloud™ securely connects any user from any device, anywhere in the world to corporate on-premises and cloud-hosted applications while all other corporate resources are cloaked. No network access is ever granted to prevent any lateral movements to other network resources while eliminating the risk of network-based attacks. The solution can be deployed without an agent in less than five minutes, without forcing a disruptive change in the organization's existing architecture, user permissions, and applications. Symantec Secure Access Cloud™ provides full governance and real-time enforcement of users' actions in each corporate application.

## How It Works: Secure Point-to-Point Access


Symantec
A Division of Broadcom
Authenticate User
Validate Device Health
Deploy connectors and
Connect to Symantec
Application
Layer
Contextual
Prevention
Monitor and
Log Activities