netskope

WHITE PAPER

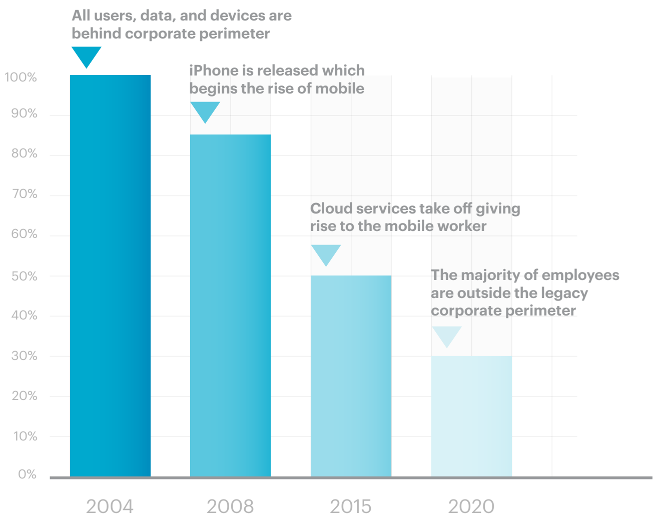
How the Security Inversion Impacts User and Data Protection

Legacy security technologies and approaches leave security practitioners blind. It's time to "invert" networking and security to create a whole new approach to building a security program in a cloud and mobile first world.

INTRODUCTION: THE DIMINISHING RETURNS OF LEGACY SECURITY

The traditional tools and mindset security teams used for building their architecture is quickly becoming obsolete. For the last twenty years, information security teams focused on adding crude perimeter-based and cobbled together controls to reduce cyber risk. Walls were built around the corporate perimeter to keep valuable assets in and threats out. The issue is, now most applications and data are moving outside that perimeter, and those traditional controls are becoming less and less effective. This legacy mindset has caused security teams to struggle with the new realities of how a modern business operates in the digital age.

Return on perimeter investments



Digital transformation has caused an evolution. Workforce mobility has replaced the traditional, cubicle-oriented approach to daily work. Thousands of cloud applications are accessible with the swipe of a credit card and the ongoing exponential collections of data are delivering previously inaccessible business insights and predictive capabilities. The business has become more agile in nature requiring solutions that can keep pace with the needs of individuals—not the security requirements of the past.

> **"THE AVERAGE ENTERPRISE USES OVER 1,295 APPS AND CLOUD SERVICES WHERE MORE THAN 95% OF THESE ARE UNMANAGED WITH NO IT ADMINISTRATION RIGHTS OR EVEN VISIBILITY."**
>
> **2019 CLOUD SECURITY REPORT, CYBERSECURITY INSIDERS**

The degree of change is so rapid and profound it has triggered an "inversion" across both security and network connectivity shifting the focus to users, devices, and data. The continued investment in legacy security controls only furthers the diminishing returns these technologies will provide prior to their complete extinction.

In many ways the book on security needs to be rewritten as the current operating model can not scale. The time has come for a change—starting with how organizations can, and must, reimagine their perimeter.

THE GREAT NETWORK INVERSION

According to a report by Kissmetrics, 47 percent of visitors expect a website to load in less than 2 seconds, and 40 percent of visitors will leave the website if the loading process takes more than 3 seconds. When applied to cloud apps, this latency averse mindset means that consistent, company-wide slowdowns may cause users to seek out more frictionless options to getting their work done. And enterprises only have their own network to blame.

Traditional hub-and-spoke network models, used by many enterprises, had a callous disregard for the amount of latency that was introduced. At a time when everything including applications, data, and users resided "inside" the corporate network, the primary objective was to ensure everything was connected together via MPLS and within the four virtual walls of corporate control. Today, it's still common practice for large organizations to backhaul web traffic to their data center for inspection, creating significant performance issues and a poor user experience. This centralized approach to routing of network traffic is no longer a viable model given the amount of external cloud applications consumed. Businesses today are looking for dynamic access to both internal applications and external cloud applications which requires a more distributed set of access and control points.

> *Generally, big U.S.-based companies will backhaul all traffic to one location in the U.S., one in Europe, or one in Asia. In every case, those round-trip tickets for network traffic add hundreds of milliseconds of extra time to every communication, not to mention the monthly bill for the MPLS bandwidth.*

The impact to user experience and current network architectures has reached such a breaking point that Gartner recently published a research note citing the need for a change across both network and security. In order for organizations to modernize their network architecture they need to get serious about low latency connectivity; something that requires dozens of worldwide points-of-presence (POP). While building and maintaining a POP can become cost prohibitive, there is a real opportunity for partnering and peering to ensure enterprises have the most balanced footprint globally.

THE GREAT SECURITY INVERSION

As digitalization has progressed across industries, tension between infosec, IT infrastructure, and business leaders has increased. This strain has caused two major gaps in how security technology and teams function today:

1. Security and technology teams can't scale with the business, creating friction
2. Security teams don't have the visibility and control required to secure data
3. Security teams have not digitally transformed

Building an Agile and Scalable Security Model

IaaS workloads are continuing to shift from one platform to another and new SaaS applications crop up, and die, continuously. These services communicate through APIs, the language of today's internet, but traditional security tools can’t understand them. There’s no way to apply security policies, monitor for abnormal behavior, or add context to end user activities. Furthermore, advanced persistent threats add additional stress to the traditional security model, and the old methods of selectively adding new controls when old technology can’t keep up isn’t working; the stack of controls is out of control.

> *There are a reported 30,000 APIs in use across the SaaS world already, and that number is growing every day.*

With the shift to a cloud-delivered security services, organizations can begin to consume the security controls they need while gaining the visibility and context required to focus on users and data. Instead of managing security tools, infosec teams can build out the right policies for data protection and adaptive access control. This helps CISOs reduce their security technology footprint without sacrificing capabilities or controls. Overall the infosec team becomes more responsive and agile—enabling better partnerships with business leaders, risk reduction across third-party cloud applications, and providing real-time guidance to the organization.

Blindness

Latency aside, there’s the problem of the massive array of SaaS applications in place in the modern workplace—often well over 1,000 apps at a large organization. As a result, over 85% of an organization's web traffic is cloud traffic. Even conventional web traffic, including CNN, ESPN, and Netflix, can be hard to inspect and manage for many companies. Only about 50% of businesses have SSL decryption, yet 90% of web traffic uses SSL today.

While all of this is taking place, the security team can't see inside the APIs that SaaS and cloud applications use to conduct business. Box, Salesforce, Workday, and more integrate into daily workflows, managing mission-critical data. Many security teams haven't realized the magnitude of the problem because they don't have technologies that provide the necessary level of visibility.

> **“WE HAVE TO PUT BEHIND US THE IDEA THAT AS LONG AS WE CAN SEE TRAFFIC, OR FORCE IT TO COME THROUGH OUR CHECK-POINTS, WE CAN INSPECT IT ON THE WAY OUT. THERE ARE OTHER WAYS TO ACCIDENTALLY OR INTENTIONALLY GIVE A BAD GUY ACCESS TO SOMEONE’S DATA IN THE CLOUD. WE NEED NEW TOOLS THAT ARE DESIGNED FOR THIS THREAT MODEL."**
>
> **ERICK RUDIAK,**
> **VP TECHNOLOGY & CISO**

Even private cloud applications create blind spots. A private cloud app is still a cloud app; they're written for the cloud, using APIs. This is the nature of modern code. Without a cloud-native approach, there’s no way to operate in an open, integrated fashion. If an application isn't cloud-native, it can't scale vertically and horizontally, and will only further hinder the ability for a business and its security team to transform.

The Business Impact

Consider the following resulting changes to the traditional computing model, adding up to a complete security inversion:

- There are more external users working at home, on planes, and in remote locations than classic internal users working on a walled "IP garden" at the physical office
- Increased reliance on IoT, system-to-system interactions exceed human-to-system ones
- More traffic is going to the cloud (SaaS and IaaS) than to the data center
- Workloads usually run on IaaS rather than corporate-owned infrastructure
- Cloud applications are now communicating primarily via API/JSON over ports 80 and 443 outside of the existing perimeter

For example, think about a standard, cloud-based productivity application used by thousands of companies, such as Microsoft Office 365. Businesses rely on authentication controls to keep the associated data secure. The data resides in the cloud, but "inside" the company from a security point of view. Yet, when a Microsoft Office 365 user "shares" a spreadsheet, for instance, no traditional on-premises DLP program or proxy will stop it because the user isn't sharing the data; they're only granting access. This is an outgrowth of a lack of sophisticated proxy and firewalls in the face of digital transformation.

> "AS THE PROPORTION OF SENSITIVE ENTERPRISE DATA INVERTS BETWEEN ON-PREMISES AND IN-THE-CLOUD, TRADITIONAL DATA LOSS PREVENTION (DLP) APPROACHES CAN BE A CHALLENGE TO SCALE. FORCING A SMALL FRACTION OF ENTERPRISE DATA PROTECTION TO TAKE A CIRCUITOUS PATH THROUGH HEADQUARTERS IN ORDER TO INSPECT IT WITH DLP MAY HAVE BEEN TENABLE AS AN EDGE OR CORNER CASE; FOR ENTERPRISES WHERE IT IS—OR SOON WILL BE—THE PRIMARY USE CASE, THE ADDED LATENCY AND USER EXPERIENCE FRICTION BECOME MORE DIFFICULT TO JUSTIFY."
>
> ERICK RUDIAK,
> VP TECHNOLOGY & CISO

It's possible to disable sharing functions across the organization, but this action stifles collaboration outside the company. This eliminates the security problem, but creates a business problem, which never works out well for the security team.

A NEW SECURITY ARCHITECTURE FOR A NEW AGE

> "IT'S ALL ABOUT MAKING CHANGES TO THE SECURITY MODEL TO ALLOW BUSINESSES TO EVOLVE IN SPITE OF THE ATTACK ECOSYSTEM AND REGULATORY ENVIRONMENT."
>
> ERICK RUDIAK,
> VP TECHNOLOGY & CISO

The inverted business and computing model call for a matching security architecture. Data flow needs to be enabled in alignment with business initiatives; this is not data leakage—it's simply the required functionality of a modern business. It's the infosec team's job to enable secure data flow; not prohibit it. Thus, modernizing your security program is about getting from point A to point B in a fast, available, secure manner, all while understanding the language of the Cloud. This shift will change how organizations think about perimeter-based security, bringing the ability to deliver real-time security at the speed and scale of the business.

If security teams are changing their security approaches, then network teams have to change their approaches as well. Security must deliver an entirely new architecture built on a globally distributed, cloud native, as-a-service architecture which provides secure access and inspects content across the organization's cloud and web ecosystem. This shift puts security in the driver's seat when it comes to building a new security architecture, instead of bolting on to something the business built years ago.

A network security architecture for the cloud era starts from the ground up. When taking a modern approach to securing the inverted business and computing model, some clear guiding principles emerge:

- The new security model must focus on providing and managing secure access to internal applications, cloud services, and data (defined as data-centric security), rather than secure systems or a single location
- The perimeter is now a relationship between your users, data, and apps; requiring a global-reaching set of inspection points for all traffic, rather than multiple tools functioning separately and in sequence
- The traditional security perimeter is heavily focused on threats within the enterprise, but lacks the ability to protect data and users from threats beyond the traditional perimeter
- Security must inspect what's happening inside APIs; it's the "language" cloud applications use to talk to each other, share data and authentication, etc.
- Inspection needs to happen as close as possible to the people using the data. For most organizations, inspection takes place via a cloud service with many points-of-presence. While some businesses have the budget and resources to scale out their own security infrastructure, it makes no economic sense to do so for most
- Open APIs and integration within an ecosystem of complementary security and technology platforms is a must for forward looking organizations to help future proof investments
- The internet was built for resiliency and delivery, not security or performance. It is important to provide an "edge fabric" that includes performance and security considerations, not just delivery
- Security can't live in a single stack within the corporate data center or branch offices; it must be omnipresent and as close to the end user as possible (geographically) to ensure an optimal experience

> "IT'S NOT OFTEN WE HAVE AN OPPORTUNITY TO RESTART AND TURN BACK THE CLOCK OF SECURITY PROGRAMS. AS THIS INVERSION OCCURS, SEIZE THE OPPORTUNITY TO BE SECURITY BUSINESS OWNERS. FOCUS ON THE RIGHT LEVEL OF SECURITY FOR THE ASSETS YOU ARE PROTECTING VERSUS TREATING EACH ECOSYSTEM INDEPENDENTLY AND TRYING TO MANAGE IT. WE KNOW THIS DOESN'T WORK ANYMORE."
>
> LAMONT ORANGE,
> CISO AT NETSKOPE

CONCLUSION: RETHINKING HOW TO PROTECT DATA AND USERS IN A CLOUD-FIRST WORLD

Since digital transformation has fundamentally impacted business operations, the security model, which was once highly effective, simply doesn't work today. Due to the merger of security and networking in the cloud, organizations need to rethink how they protect their data and users in a cloud-first world. The rapid pace of change has led to a total security inversion, and the solution is a new, cloud-first security architecture designed to protect and enable businesses concurrently.

Modernizing the security model is necessary for business agility, ultimately supporting an accelerated, enhanced pathway to market. Doing so not only quickens time to market, but also allows businesses to innovate freely, and remain ahead of the attacker ecosystem. This minimizes the potential for operational losses while eliminating the need for lengthy security processes that aren't conducive to business today.

Key takeaways

- Legacy methods for protecting data and personnel forced users behind the corporate security stack. This model is ineffective in a cloud and mobile first world. When evaluating security technologies, look for solutions that are delivered from the cloud and built using cloud-native architectures to support flexibility and scale.
- Security in the cloud requires a new approach because tools and applications are driven by APIs, not hardware appliances. Make sure you evaluate what types of controls you require across each cloud application; out-of-band API connectivity for visibility or inline real-time API inspection that supports granular controls.
- The paradigm shift isn't just about tooling, but enabling business to move faster—the original intent of cloud computing. Instead of applying heavy-handed security controls across all cloud applications, look to develop a triage process based on cloud application risk scores and review those cloud applications that pose the most risk to the organization.

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

To learn more visit, https://www.netskope.com.