Symantec

Eight Essentials: Rethinking Security for the Cloud Generation

The cloud has transformed cyber security forever. Here are eight suggestions for navigating the changes.

The Cloud Generation Has Arrived. Are You Ready?

Every IT generation faces its own unique disruptions. The seismic shift from mainframes to client/server. The even bigger explosion of the internet. And now, the universality of the cloud and the complexity of hybrid environments.

Like all the transformational shifts before it, the cloud changes how businesses operate and how people live. In the Cloud Generation, nearly everyone depends on cloud apps and services for nearly everything, at work and in their personal lives. Our identities and personas spread across dozens of different services and platforms. And information flows freely across an ever-growing number and variety of devices, some of which are company-owned, most of which are not.

In the Cloud Generation, information has moved out and away from controlled, protected corporate environments.

But the Cloud Generation is not just about identities and devices. It's also about data. In the Cloud Generation, information has moved out and away from controlled, protected corporate environments. Data lives everywhere, which directly impacts your ability to know what data is important, where it's located, and how to defend it. And of course, the Internet of Things (IoT)—a transformative trend in its own right—adds exabytes of fresh data and billions of new devices to the mix.

For better and for worse, the Cloud Generation is changing everything. Again. For security and IT professionals, its challenges are universal and unavoidable, fueled by an unstoppable drive to become more connected, productive, and competitive.

40%

Average TCO reduction among cloud adopters

19% ▸ 57%

2017 growth in hybrid cloud adoption

53,844

Average number of mobile devices in Global 2,000 enterprises

Is It Cloud, or Is It Chaos?

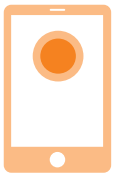
Like every technology disruption before it, the Cloud Generation presents a dark side.

As users connect mobile devices and cloud services outside the confines of the office, they expose themselves to cyber dangers. As data untethers from the predictable, protected pathways of corporate networks and spreads to multiple clouds, it becomes more difficult to manage and protect. And as identities and personas multiply, new opportunities for criminals and attackers multiply.

Ultimately, the success and safety of your organization depend on how well you resolve the fundamental tensions between opportunity and risk; freedom and chaos; agility and security.

A Perfect Storm for Chaos

The benefits and potential of the Cloud Generation are well documented. But the Cloud Generation also introduces new risks for businesses—and new opportunities for cyber criminals:



MOBILITY

Mobility takes users outside the safety net of protected networks.

DIRECT CONNECTIONS

Direct connections to cloud services bypass traditional cybersecurity protections and controls.

CLOUD IDENTITIES

Multiple cloud identities and personas provide new openings for theft.

IOT DEVICES

Billions of IoT devices and connections create countless new attack surfaces.

DATA LOCATION

Data lives everywhere, making it difficult to see, control, and protect.

Finding a Safe Path Forward

Given the unique dynamics of the Cloud Generation—and the new risks and challenges they create—it's abundantly clear that protecting people and information requires a fundamentally different approach to cyber security. And yet, most corporate security investments are still based on the way the world used to work, not the way businesses and people operate today.

So what does complete, effective cyber security even look like in a world where the walls between secure corporate networks and the outside world are dissolving, where the information that powers your business lives everywhere, and where people no longer wait for permission to access and share the resources they need to get things done?

Consider these security realities in the Cloud Generation.

Traditional corporate security measures are still necessary, but they are no longer sufficient. Today, most threats are designed to bypass or avoid traditional firewalls, endpoint protection, and data loss prevention technologies.

The Cloud Generation demands a more global, integrated approach to cyber security where all your technologies, services, and threat intelligence work together to keep people and information safe.

Cobbled-together collections of isolated point products can't protect your organization in the Cloud Generation, no matter how good they are.

It's no longer enough to protect the disappearing perimeter of your organization. Cloud Generation security must extend to the ever-expanding mix of devices, connections, networks, and hosted apps that power your business.

Eight Security Requirements for a Dangerous World

As with any complex undertaking, it's useful to break down the challenges of securing the Cloud Generation into practical, achievable steps.

Requirement #1

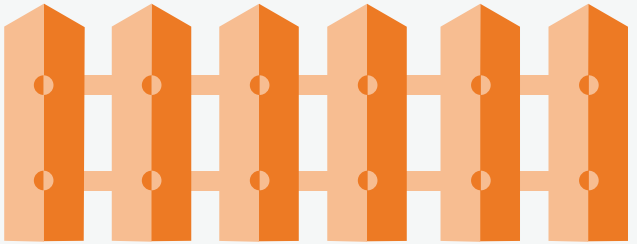
Unify your cloud and on-premises security

The Cloud Generation is rife with changes and disruptions. Your data, devices, and applications are no longer confined by traditional perimeters. The technology and information that powers your business now exists on premises, in the cloud, and in a hybrid state.

Thanks to this widespread adoption of unsanctioned cloud applications and unmanaged devices, a growing percentage of the information you're responsible for falls outside your view. But these sobering realities don't change the fact that your data must stay protected at all times.

We have arrived at a place where even the most capable security infrastructures struggle to keep up. Widespread adoption of public cloud SaaS apps and infrastructure services, shadow IT, and BYOD render already-strained security and compliance stacks even more complex and vulnerable.

The only viable option is a platform approach to cyber security that integrates all the disparate pieces of your infrastructure to eliminate gaps, reverse fragmentation, and increase effectiveness in our mobile, cloud-powered, no-perimeter world.



DON'T GET FENCED IN

In the Cloud Generation, your network perimeter is defined by the location of your information, which is … anywhere and everywhere.

ON PREMISES

MOBILE DEVICES

CLOUD

IOT

Requirement #2

Apply intelligence—human and artificial—to stay one step ahead

Every day, attackers invent ways to pierce your defenses, taking full advantage of artificial intelligence and machine learning technology to do it. To keep up, you have to play the same game—by building the right mix of artificial intelligence and human intelligence into the core of your cyber defenses.

Artificial intelligence enables you to utilize telemetry gathered by security systems and endpoints around the world, parsing trillions of lines of data to uncover malicious files and URL threat indicators at a rate no human can match. Then, you can use that information to block attacks across your endpoint, cloud, and network control points.

But you can't rely on artificial intelligence alone to protect your organization.

Enterprise environments are incredibly complex, and they require careful monitoring and correlation across multiple security tools from multiple vendors. Sometimes, the only way to identify, analyze, and resolve complex incidents before they become major issues is through the applied intelligence of an army of experienced cyber warriors.

MEET THE FUTURE OF CYBER SECURITY

2004

Spyware detection

2006

Detecting proxy bypass websites
Automated Phishing Detection

2008

Malicious file conviction on the endpoint
File Scanning – File Reputation analysis in the cloud, behavior analysis in the cloud

2012

Mainstream Deep Learning

2014

0-day protection against malicious Android APKs using Deep Learning
Symantec CAML founded

2015

Cloud Sandbox

2016

Spear Phishing Detection
File Scanning on the Endpoint

Requirement #3

Protect data everywhere—public, private, and mobile

In the Cloud Generation, mobility is inevitable, which means your sensitive data travels everywhere. So how do you control information that constantly moves in and out of the cloud and across mobile applications? And how do you develop a viable information protection strategy that successfully combines data protection, encryption, authentication, and identity management?

The answers lie in your ability to extend three essential capabilities to every corner of your on-premises, cloud, and mobile infrastructure: visibility, protection, and control. This means adding a variety of new tools and technologies to your existing data protection stack, including a capable Cloud Access Security Broker (CASB), advanced data encryption and tagging, and capabilities that monitor data use both on and off the corporate network to prevent leakage or theft.

EXPLORE

Symantec Information Centric Security

Requirement #4

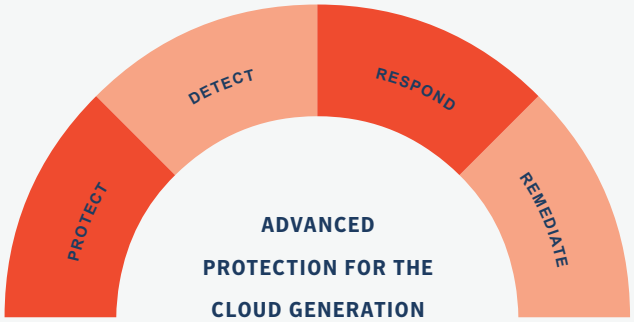
Defend against multistage, multivector, encrypted threats

Cyber attacks target networks, endpoints, the cloud—and sometimes all three. They invade across an increasing number of vectors. And they often conceal themselves in encrypted traffic.

The velocity and sophistication of these attacks make it virtually impossible to stop all of them, even with the best cyber defenses. After they penetrate your infrastructure, they quickly traverse your network, steal credentials, and connect with command-and-control servers—all with the goal of compromising your most critical systems and data.

Stopping threats before they reach your organization is obviously important, but it's no longer enough. Undetected threats and slow remediation leave you vulnerable to loss of sensitive information, financial penalties, and irreparable damage to your reputation. And of course, dealing with the constant security alerts and user impacts that come from infections increase your IT overhead and seriously disrupt your business.

To avoid these problems, you need a more advanced, layered cyber defense system that stops most threats—but then quickly uncovers, prioritizes, and remediates the few advanced threats that make it through. This type of layered, integrated approach holds the key to keeping attackers at bay, no matter how dangerous or sophisticated their methods.



Requirement #5

Control all your endpoints—desktop, mobile, and IoT—with one agent

The cloud enables your users to access data and applications remotely. Employees telecommute regularly from hotels, airports, coffee shops, or any other hot spot (whether they are secured or not). At the same time, the proliferation of IoT devices adds literally billions of new devices to enterprise ecosystems. This requirement for complete mobility—together with the explosion of new intelligent, connected devices—creates obvious new security implications for your business that demand a new approach to endpoint security.

Unfortunately, there's a tendency to treat different types of breaches separately, applying one point product after another as triage. These isolated 'silver bullet' technologies serve a useful purpose, but they never constitute orchestrated endpoint protection. And although this 'band-aid' strategy may work for smaller incidents, it's ineffective against sophisticated, large-scale attacks such as WannaCry.

To provide total endpoint protection in a mobile, cloud-driven, IoT world, you need a multilayered approach that provides advanced machine learning, behavioral analysis, memory exploit mitigation, real-time sandboxing, and file scanning across every device in your ecosystem. All with the simplicity of a single agent.

AN ENDPOINT BY ANY OTHER NAME ...

Cloud Generation endpoint protection replaces the typical ad-hoc collection of point products with a multilayered defense, all from a single agent.

Requirement #6

Lock down network traffic with deep inspection and controls

There was a time when email, ERP, CRM, and dozens of other business applications were built and delivered in a protected data center using a variety of network ports and protocols. In this type of environment, next-generation firewalls had the scale and ability to protect the entire network.

But times have changed. Web, cloud, mobile, and email have all collapsed onto HTTP. And the only way to ensure full protection against threats is to intercept all web-bound traffic, inspect it, and set policies to block both known and real-time threats. You need deep application intelligence to control all the data and files that are transported over HTTP, including web, mobile, and cloud apps. This enables you to decrypt communications using integrated threat protection and information security while still maintaining privacy.

Requirement #7

Secure it like you own it, even when you don't: IaaS, PaaS, and SaaS

The cloud delivers better experiences and lower operating costs, but it also creates significant exposure. It's the Cloud Generation 'Catch 22': The same freedom that makes the cloud so attractive wreaks havoc with your best cyber security tactics.

What's more, according to Symantec research, many CIOs have completely lost track of how many cloud apps are used inside their organizations. This lack of awareness and control leads directly to a lack of sound policies and procedures for accessing cloud services, which in turn makes cloud apps riskier.

To resolve these tensions, many organizations have turned to complex combinations of vendors, solutions, plugs, and fixes, each addressing a specific cloud security issue. Of course, this approach only adds complexity to security stacks that are already too overburdened and fragmented to operate effectively. And cyber criminals exploit the resulting chaos.

Replacing these single-function point products with an integrated security platform brings all your critical security and compliance services together—including advanced threat protection, data loss prevention, workload protection, and other intelligence services. This new approach reduces complexity, vulnerability, and costs without compromising security.

HOW MANY CLOUD APPS ARE YOU USING?

According to recent Symantec research, most CIOs dramatically underestimate the number of cloud apps their employees use:

40

THE PERCEPTION:
Employees use around 40 cloud apps.

1,000

THE REALITY:
Employees use close to 1,000 cloud apps.

Requirement #8

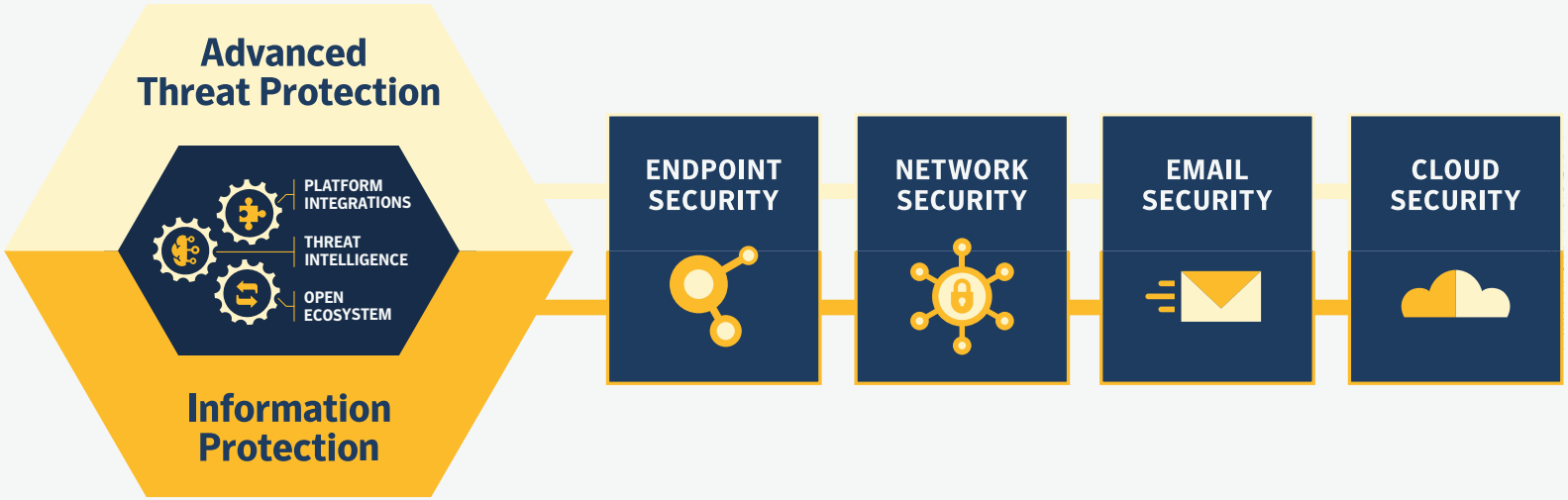
Integrate by design: Existing, new, and future

Today's security infrastructure fragmentation is largely a result of organic, well-meaning reactions to rapid technology shifts and constant innovations in cyber crime. Criminals exploit a new vulnerability or develop a different line of attack; organizations deploy a new product or technology to fill the gap; the criminals adapt and evolve. It's a vicious cycle.

However, this natural response leads to an unwieldy stockpile of security tools from different vendors that typically don't talk to each other. A host of difficult operational problems ensue: Incident response teams are forced to navigate an ever-growing number of interfaces and tools to do their jobs. The move to the cloud intensifies the problem, pushing already fragmented infrastructures to the point where they are no longer capable of providing adequate protection.

Collectively, we have reached a breaking point. Cobbled-together collections of isolated point products simply can't protect your organization in the Cloud Generation, no matter how good they are individually. The only viable, long-term answer is an integrated, platform approach, where all your security technologies, services, and threat intelligence work together to safeguard your people and information.

ANATOMY OF AN INTEGRATED CYBER DEFENSE PLATFORM



Discover the Advantages of an Integrated Cyber Defense Platform

Symantec calls its approach to today's complex, fragmented and hybrid environment Integrated Cyber Defense. And we're ready to support you to complement, enhance, and ultimately transform your existing security infrastructure.

Of course, we can't wave a magic wand and instantly make this hybrid Cloud Generation less chaotic or dangerous. We can't singlehandedly put cyber criminals out of business, make nation states play fair, or magically eliminate every dangerous attack.

But we can put the power of an Integrated Cyber Defense Platform, the depth of the world's largest civilian Global Intelligence Network, the innovation of an unparalleled engineering brain trust, and the reach of an expansive portfolio to work for your business. You'll keep your users, information, messaging, and web presence safe in the Cloud Generation as a result.

Learn more and take full advantage of everything the Cloud Generation offers … without the chaos and risk that go with it.

LEARN MORE