Secure data and boost employee productivity

The next steps in your digital journey

Insight guide

orange™

Business Services

A next generation hybrid network

Be digitally ready with a next-generation network

Connectivity has never been more important to your business.

But without the right type of connectivity, employees become less efficient and face long waits for reports to run, files to open and save and the frustration of dropped and disrupted VoIP and video calls. More worryingly, hybrid connectivity increases the risk of security breaches while data is in transit and being stored.

This insight guide provides practical tips on how you can use your network more strategically to overcome these challenges. It outlines how to safeguard performance and security, while containing connectivity costs.

By taking these steps, you can ensure your enterprise is digitally ready to drive profitable revenue growth.

A new era of professionalized cybercrime

Cybercrime has become a board-level priority because of the frequency and scale of attacks and their financial and reputational impact. Today enterprises need to understand cybercriminals' objectives so they can be fully prepared to counter an attack.

Business demands:

- Protect data to safeguard customer and employee privacy and our corporate reputation
- Defend our enterprise against the theft of high value IP, counterfeiting and espionage, which affect brand and price differentiation
- Prevent system outages as part of a ransom attack that may be ideologically motivated

Cyberattacks costs businesses $400 billion a year.[1]

We've seen the rapid rise of "multi-vector" attacks. Working as syndicates, hackers target end users, mobile and IoT devices, networks, applications and data centers in parallel to find a weak link. They increasingly use advanced DDoS (distributed denial of service) attacks as a diversionary tactic while extracting data over time or crippling your ability to operate.

IT pain points:

- In the era of the cloud and mobile working, the secure network perimeter is a thing of the past. Traditional firewalls and anti-virus protection are no longer enough
- It's a matter of when, not if, breaches will occur. IT teams need to be able to anticipate emerging threats as well as identify and mitigate the impact of breaches fast

$40K per hour – the cost of a successful advanced DDoS attack to a typical enterprise.[2]

[1] Source: Intel [2] Source: Incapsula

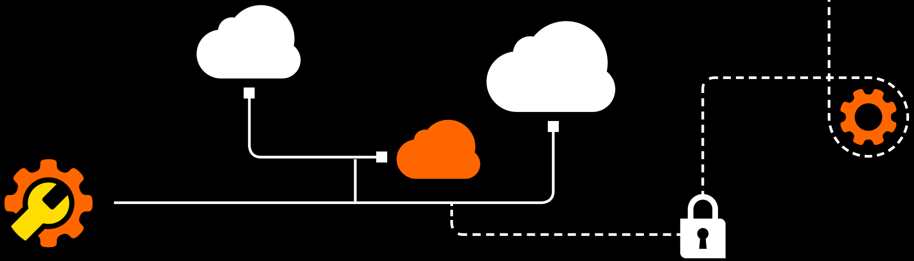
Take a network-enabled approach to security

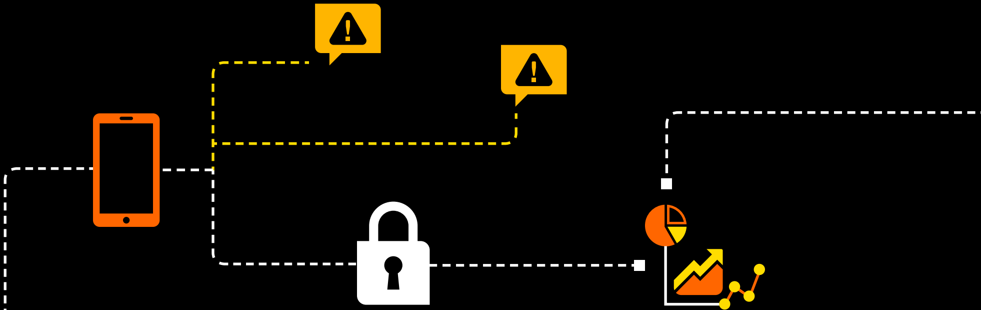
A multi-layered defense strategy – spanning end users, transport links, applications and data centers – is needed in the era of sustained multi-vector attacks.

1. Distributed real-time cloud control

Cybercriminals are able to hide malware behind traffic from “trusted” https sites. A cloud-based security platform – provisioned from regional distributed Internet gateways – can inspect this encrypted traffic at high speed. It protects smartphones, tablets, PCs and servers with continuous updates in response to emerging threats.

In contrast, traditional branch office appliances are unable to support deep content inspection due to the latency caused by the distance data needs to travel to the data centers. They leave mobile devices vulnerable to attack and are time consuming to update and scale.





2. Choose your network path based on the data risk profile

Enterprises should use a mix of public Internet and private WAN links depending on the business risk associated with each data workflow.

- **Private MPLS connectivity:** provides the highest level of protection and speed of service for business-critical traffic to and from your cloud providers’ data centers
- **Distributed Internet gateways with cloud-based security:** offer optimum control over your security policy in real time, while eliminating the latencies caused by regional Internet gateways
- **Local Internet gateways:** keep low-risk traffic private until it reaches cost-effective, local break-out points using secure IPSec tunneling
- **Dedicated Internet gateways:** eliminate the risks associated with shared infrastructure

3. Securely authenticate users before they access any enterprise resources

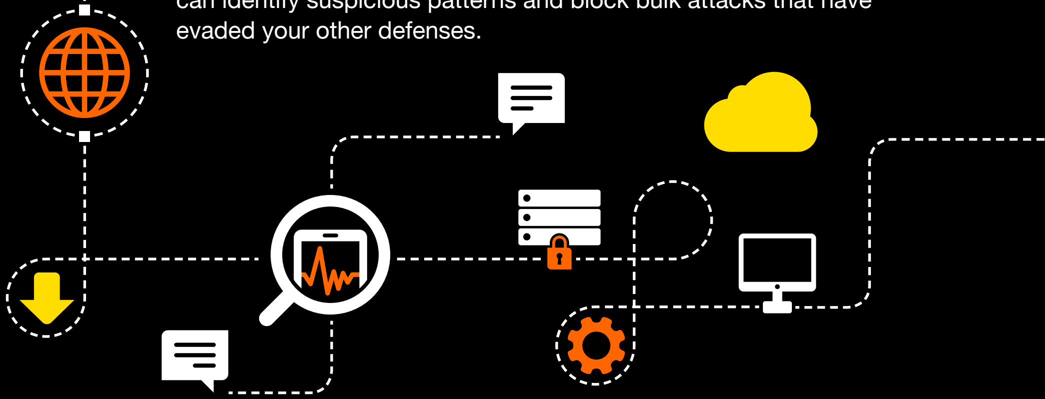
A federated identity and access management (IAM) scheme gives approved employees and partners access to cloud and on-premise applications from any device using a single login. Multi-factor authentication protects VPN access over unsecured Internet connections, for example an airport waiting lounge or café.

Access control is also vital to protect operating control systems in the manufacturing, oil, gas and utilities sectors. Sensitive data, such as customer records in Salesforce, should be encrypted and tokenized before being processed and stored in private sovereign data centers or a virtual private cloud.

4. Ensure the availability of IT network and resources with DDoS protection

The scale and frequency of distributed denial of service (DDoS) attacks are increasing. Volumetric attacks can now reach up to 500GB/s. Three tiers of advanced DDoS protection are required.

First, use next-generation firewalls on your premises to detect and quarantine threats at the network edge. A sustained attack will overwhelm your Internet connection, enabling cybercriminals to target application layers in stealthier ways. The second layer of defense – a cloud-based DDoS protection service – uses probes to inspect in-bound and out-bound traffic. This prevents malicious traffic from reaching your infrastructure as well as data exfiltration attempts. The third tier is an attack mitigation appliance in the data center, which can identify suspicious patterns and block bulk attacks that have evaded your other defenses.



5. Use big data intelligence to detect new threats and react to attacks

Enterprises take an average of 205 days to discover they've been compromised and a further 31 days to contain the breach when working on their own.[3] A managed security service provider shrinks to a fraction of the time.

A security information and event management (SIEM) platform is essential to correlate security alerts and turn them into actionable intelligence. It can identify malware and abnormal application access requests to detect intruders in your network. Big data analytics powers real-time threat visualization, dynamic incident response and post-event forensics. It's also important to draw on the widest possible range of external global threat intelligence sources to pinpoint emerging risks.

[3] Source: Arbor Networks

6. Manage risk using a strategic CyberSOC

Security experts from a CyberSOC can help you prioritize which data is most important to your business and outline ways to reduce attack risks.

The CyberSOC tracks traffic flows, identifies exceptions and acts decisively when an attack occurs. Geolocation-based policies and blacklisting reduce the risk of attacks via botnets, malware hosting sites and spam. Probes detect attacks and divert traffic to centralized mitigation centers where they can be blocked.

Cybersecurity skills command a high premium in the job market, and employees change jobs frequently. This makes the support of a managed provider with excellent people, processes and tools, as well as enviable staff retention rates as a top global employer, invaluable.

Boost employee productivity

Slow application response times and dropped video and VoIP calls reduce the ability of teams to collaborate and may make employees reluctant to adopt new digital ways of working.

Business demands:

- Ensure applications – including those in the cloud – run at optimal performance on any mobile device or computer, anywhere in the world
- Eliminate the frustration of dropped and disrupted VoIP and video calls
- Keep control of connectivity costs while meeting greater bandwidth needs

To meet these demands, IT teams need greater flexibility to balance performance, security, capacity and cost requirements when provisioning connectivity at all locations.

IT pain points:

- Increase confidence that cloud applications can be used easily anywhere in the world
- Regain control over connectivity speeds and security over public Internet links
- Ensure high-quality real-time VoIP and video communications on private WAN links
- Pinpoint performance problems easily across server, network and application layers

Central control over application performance

Enterprises need to prioritize and optimize on-premise and cloud application data flows in real time across diverse transport links.

1. Take the fastest path from the end user to the application

The public Internet often becomes congested, impacting cloud application performance. In addition, increased network latency for employees located far from their cloud service provider's data centers can lead to simple tasks, such as opening a PowerPoint file, taking up to 20 minutes even during off-peak times.

A "business class" Internet overlay solution improves cloud application performance by minimizing the number of network hops between the data center and user to deliver faster, more reliable connectivity. It uses multiple routes and tests the network using forward error correction to select the best performing path.

2. Prioritize business-critical and real-time traffic

Meet with your business leaders to understand the business criticality of applications and processes. This will enable you to prioritize applications onto different classes of transport link. For business-critical cloud applications, enterprises should also consider using their enterprise-grade MPLS connectivity to benefit from end-to-end speed of service and security guarantees. The interconnection with the cloud data center is within the MPLS network, avoiding the need to use the public Internet at any point. Private connectivity is also essential for reliable real-time video and VoIP traffic.

3. Combine multiple networks to strike the best balance of cost and performance

New software-defined WAN (SD-WAN) technology enables enterprises to use multiple private MPLS and Internet links dynamically during times of congestion. SD-WAN routers today are physical proprietary devices deployed at a branch office level. In the future, lower cost “white box” solutions – also known as virtual customer premise equipment (vCPE) – running on standard servers will enable application-aware routing. This approach enables enterprises to keep intelligence centrally in the network for maximum control and execute faster at a local level.

4. Minimize network data loads with WAN optimization

Use application acceleration appliances to inspect two-way traffic between your data center and branch offices. This allows you to cache relatively static information locally and only send updates if data is modified. Compression can also shrink the size of data packets and further reduce overall network load.

By bundling the multiple protocols sent to acknowledge the transmission and receipt of traffic, you can reduce application chattiness and network traffic volumes. Enterprises can now use virtual optimization appliances within their cloud providers’ data center to optimize software-as-a-service (SaaS) applications. Soft clients – running on an individual’s smartphone and PC devices – ensure mobile and virtual workers benefit too.

5. Apply data analytics and visualization to understand the bigger picture

In the multicloud era, applications often call on multiple services in different locations. For example, a cloud-based fleet management system will draw in third-party weather, GPS and traffic data and validate the end-user's identity using the enterprise's active directory. While the average company uses seven Salesforce plug-ins to manage diverse bid automation, after-sales services and customer satisfaction processes. It's vital to prevent these interdependencies from causing any delay.

Use advanced metrics and root-cause analysis across application tiers and technology stack to get an holistic view of performance from the end-user perspective. This will help you understand if particular applications slow down on certain days, times of the year, or in specific geographies and avoid problems that could impact employees' productivity.

6. Plan for virtualization in all its forms

Rolling out new cloud and mobile applications – or consolidating global workloads into fewer data centers – is easier when you can control end-to-end performance and security. A simple dashboard will help you understand network traffic baselines, port utilization rates along with predicted and actual growth rates.

Such insights also enable IT managers to better prepare for the world of software defined networking (SDN) and network functions virtualization (NFV) and support new digital business workloads with programmable on-demand networking.

Get future ready

CIOs are under pressure to enable new digital workflows and customer interaction channels. Software defined networking (SDN) and network functions virtualization (NFV) promise to bring the agility and control they need over performance and security.

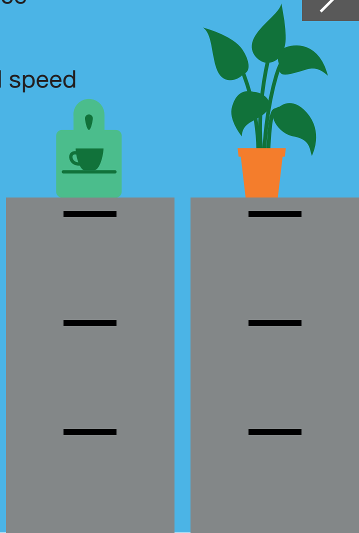
Business goals:

- Deliver positive digital business experiences to our end users
- Minimize network costs and the risks of over- and under-provisioning capacity

IT teams need to prepare for the great wave of change that a move to open, multi-vendor virtualized networking will bring.

IT pain points:

- Migrate more IT services to an on-demand, self-service consumption model
- Automate network tasks to reduce manual errors and speed up time-to-market
- Adapt traffic flows in light of changes in the threat landscape and network loads that would otherwise impact application performance
- Contain costs as bandwidth demands continue to grow



On-demand digital connectivity

Virtualization enables the creation of on-demand digital connectivity services to meet employee and customer application performance needs and data security expectations.

1. Increase business agility

SDN and NFV remove the reliance on inflexible, fixed function hardware in global networks. Instead, network functions can be created in software and run on general-purpose servers in a service provider's central office, regional points of presence (PoPs) or the enterprise's branch offices. This means it takes just minutes to up-scale and down-scale bandwidth capacity or adapt firewalls in response to new security threats. Developers can isolate new application workloads in their live network – speeding up problem solving and deployment times.

2. Keep intelligence centrally in the network and enable faster execution at the edge

SDN separates the control plane (which is responsible for network intelligence) from the data plane (which forwards traffic to selected destinations). SDN makes the network programmable to meet enterprises' changing application performance and security needs. It provides centralized control over global resources and enables faster local execution. For example, service chaining accelerates high-priority traffic through the network or applies additional security steps on demand.

NFV is also required at a local, branch office level. The speed of light is finite and latency increases with the distance to the end user. Virtualized firewall, intrusion detection and optimization capabilities detect security threats and application load variances faster at the network edge.

3. Start small and scale

New branch offices or retail stores with highly variable network requirements are good early candidates for virtualization. Eliminate truck rolls to deliver new equipment, enabling services to be provisioned and configured remotely over the network from the cloud without the need for on-site IT staff. You'll also benefit from the transparency, predictability and control over costs and service levels.

Virtualization enables you to up- or down-scale capacity on demand or provide access to your network to third parties on a short-term basis. For example, you could grant business partners access to shared services in your data centers using MPLS, secured Internet or LTE links via a virtualized VPN and enable them to upload files when tasks are completed.

4. Prepare for the new wave of constantly evolving security threats

It's important to continue to build security into your network fabric during your virtualization program. As your business needs and the security landscape changes, IT teams can update their virtualized intrusion prevention, load balancing and firewall protection to match.

Virtualization enables your network to respond more dynamically and flexibly to threats. Using the NFV control plane, enterprises can quickly provision different types of virtual security appliances from a one-click self-service portal. While the SDN controller can steer, intercept or mirror the desired traffic for security inspection, creating a security service chain.

5. Gain control over latency to deliver better end-user experiences

Some 41% of enterprises report that poor application experiences result in dissatisfied clients or customers according to a global survey by Riverbed, while contract delays are an issue for 40%, and missed critical deadlines for 35%. Virtualization enables latency requirements to be set to meet specific application and end-user needs.

Enterprises will be able to benefit from innovative M2M platforms, high-definition video calling and real-time speech-to-speech translations over the coming years. A virtualized network provides the flexibility to meet such a diversity of latency, bandwidth and security requirements within budget.

6. Ensure a commitment to open, multi-vendor standards

A multi-vendor approach to the routing, security and performance capabilities you need in your network creates healthy price competition and spurs innovation. Opt for a communications service provider who is committed to using open, multi-protocol solutions and is forging a diversity of partnerships with innovative networking vendors to give you optimum choice.

Despite the use of open standards, extensive work is often required to get point solutions to interoperate effectively. This is because open standards may be interpreted in slightly different ways, and vendors may not be contributing back all of their code to the open source communities. Strong R&D, integration and management capabilities are key.

Our vision

Virtualization enables the creation of on-demand digital connectivity services on demand to meet employee and customer application performance needs and data security expectations.

A next-generation hybrid network provides the oxygen of connectivity to enable you to achieve your digital business goals. It helps you to:

- Use your network strategically to manage security in real-time in light of the evolving threat landscape
- Dynamically manage a diversity of transport links to deliver the right high-speed application experiences to end users at remote, temporary and mobile locations
- Adapt quickly to change and meet employee and customer expectations with on-demand cloud applications and virtualized networking

If you'd like to talk to our thought leaders, please fill in the contact form here: orange-business.com/en/hybrid-network-inquiries