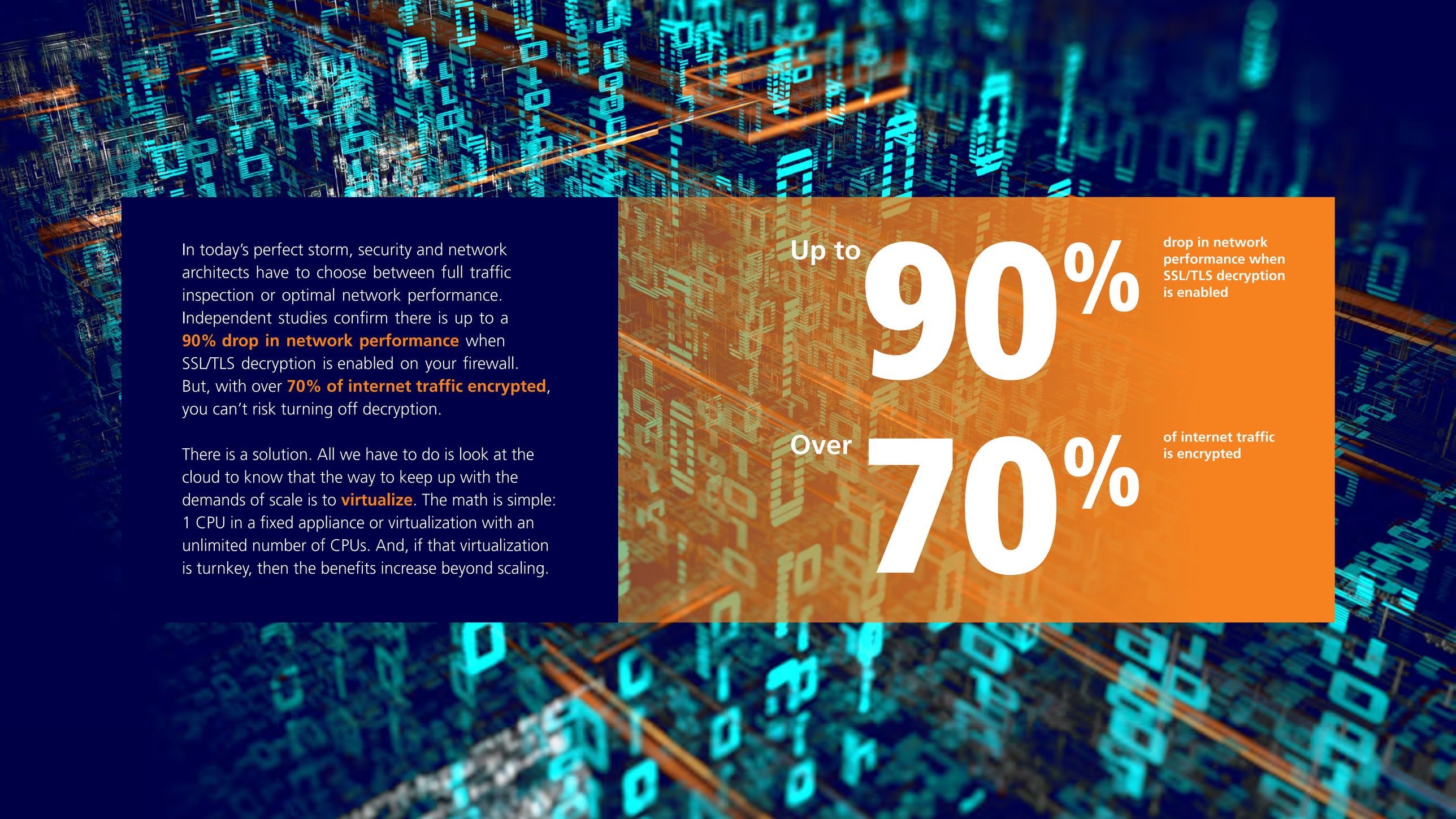
Five Reasons to Virtualize Your Firewall

Scale traffic inspection for complete visibility, even into encrypted traffic

CORSA



In today's perfect storm, security and network architects have to choose between full traffic inspection or optimal network performance. Independent studies confirm there is up to a **90% drop in network performance** when SSL/TLS decryption is enabled on your firewall. But, with over **70% of internet traffic encrypted**, you can't risk turning off decryption.

There is a solution. All we have to do is look at the cloud to know that the way to keep up with the demands of scale is to **virtualize**. The math is simple: 1 CPU in a fixed appliance or virtualization with an unlimited number of CPUs. And, if that virtualization is turnkey, then the benefits increase beyond scaling.

Up to **90%** drop in network performance when SSL/TLS decryption is enabled

Over **70%** of internet traffic is encrypted

FIVE REASONS TO VIRTUALIZE YOUR FIREWALL

1 2 3 4 5

SCALING OF TRAFFIC INSPECTION

ELIMINATE THE FIREWALL REFRESH HEADACHE

ZERO TOUCH PROVISIONING

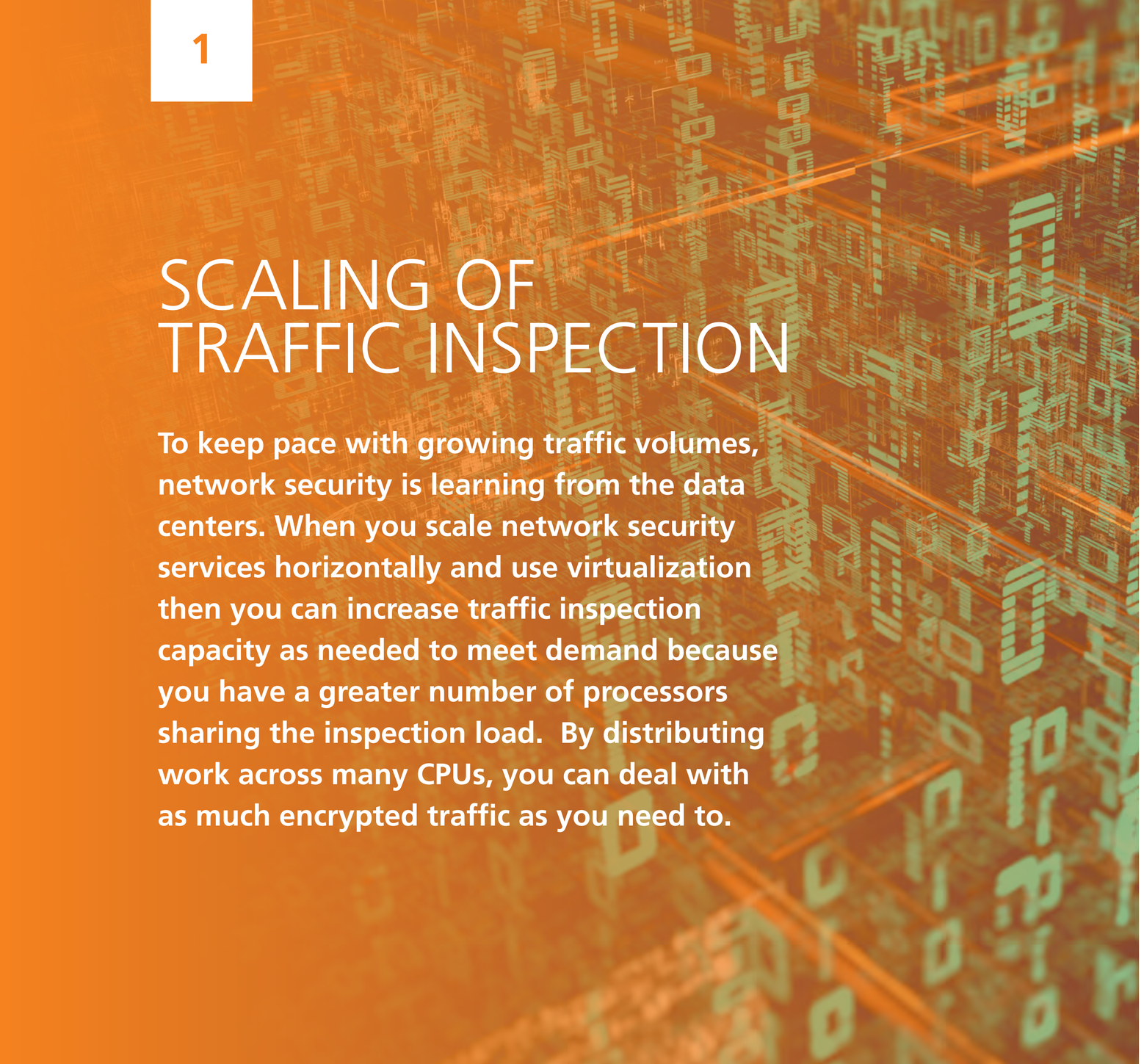
REDUCED TOTAL COST OF OWNERSHIP (TCO)

PAY-AS-YOU-GROW

1

SCALING OF TRAFFIC INSPECTION

To keep pace with growing traffic volumes, network security is learning from the data centers. When you scale network security services horizontally and use virtualization then you can increase traffic inspection capacity as needed to meet demand because you have a greater number of processors sharing the inspection load. By distributing work across many CPUs, you can deal with as much encrypted traffic as you need to.



“

According to Cisco’s Annual Internet Report, **5G, Internet of Everything, and Video** are huge drivers of increased enterprise traffic volumes.

”

2

ELIMINATE THE FIREWALL REFRESH HEADACHE

When you rely on hardware refreshes to keep up with network security demands, your team is forced to spend an inordinate amount of time sourcing, installing and maintaining new hardware. Virtualization eliminates the need for ongoing hardware refreshes, instead giving you an automated, self-service system with pay-as-you-grow scaling of traffic inspection. You can reverse the 80/20 rule so that your team has more time available to focus on high-value, long-term security policy.

> According to Gartner, firewalls are typically on a **five-year refresh cycle**. For each refresh, organizations need to evaluate everything from throughput capacity to required features and deployment criteria to configuration options.

3

ZERO TOUCH PROVISIONING

A virtualized system operates like “just-in-time” infrastructure. Scaling inspection capacity is simple and quick; if resources become scarce, you are alerted by the system. All it takes is the click of a button to add more inspection capacity, while the underlying infrastructure remains invisible to the user. The additional resources are ready for use in minutes as opposed to the days or weeks it takes to set up hardware appliances.

“

One of the greatest benefits of a zero touch provisioning is **speed**. It allows you to focus on what sets you apart as a business rather than getting bogged down with the infrastructure. You gain increased agility as well as costs savings.

”

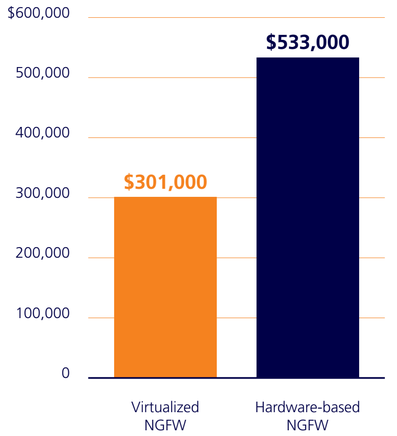
REDUCED TCO

When network security is virtualized, you reduce both capital and operating costs since you no longer have to own and manage hardware. It also means your security team don't have to worry about server CPU sizing or how to model your network accurately in order to purchase enough inspection capacity to last. You specify how much traffic you currently need to inspect, and with what kind of security profile, then the system ships to meet that requirement.

HOW DO THE COSTS COMPARE?

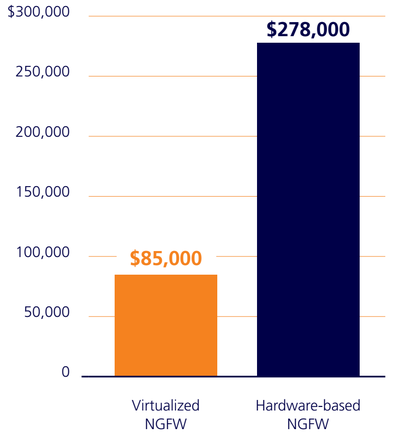
THREE-YEAR TCO

Over 40% lower



TOTAL COST OF ENTRY

3x lower



5

PAY-AS-YOU-GROW

With the growth of your business comes growth in terms of your network and security needs – increased traffic, changes to the traffic mix. Thanks to turnkey virtualization, additional inspection can be provisioned in a matter of minutes, granting companies the ability to deploy resources in an elastic fashion when demand dictates. No forklift upgrades or big network redesigns when you add employees, locations, or resources.

WITH A MONTHLY SUBSCRIPTION YOU BENEFIT FROM:

✓ Greatly reduced up-front costs	✗ Elimination of overprovisioning
✓ Quick and easy scaling	✗ No downtime during upgrades

Scaling network security can seem like an impossible puzzle to solve: find a way to gain 100% traffic inspection while maintaining optimal network performance. **The key lies in virtualization tightly integrated with intelligent orchestration.**

The result? A turnkey, cloud-like platform which quickly and easily lets you scale traffic inspection. A responsive, flexible system which grows with your company, freeing up your security team to focus on strategic priorities rather than fighting fires.

ABOUT CORSA SECURITY

Corsa Security is the leader in scaling network security with the first turnkey network security virtualization platform that simplifies how large enterprises and service providers scale traffic inspection, including SSL/TLS encrypted, at much lower total cost of ownership (TCO). By tightly integrating virtualization with intelligent orchestration, Corsa Security streamlines deployment, management and operations of virtualized next generation firewall (NGFW) arrays for large networks. Customers subscribe to the Corsa Security service based on their traffic inspection capacity needs and then pay as they grow while never having to deal with the infrastructure.

Learn how Corsa is revolutionizing network security at corsa.com or email info@corsa.com

TS-CDD0005-000, Rev 001