COLORTOKENS

MICRO-SEGMENTATION FOR DATA CENTERS

WITHOUT USING INTERNAL FIREWALLS

TABLE OF CONTENTS

INTRODUCTION

Every day there's a breach. Security leaders in enterprises are constantly re-evaluating their strategies to defend from potential breaches. Yet, many are still playing catch-up with the attackers that have gotten sophisticated. Given the many attack vectors and techniques used by the bad actors, and the frequency of the attacks, cyber security has now become a boardroom topic.

All these years, security has essentially remained reactive – looking for the known bad or mitigating the threats after the damage is done. Remember, the attackers are getting smarter every day. So, what can you do?

This paper will give you an idea on why data center micro-segmentation using internal firewalls may not be the best way forward, and why a software-defined approach wins.

YOUR PERIMETER SECURITY IS RIGID

Enterprises have evolved over the last decade – with hybrid data centers, and dynamic application and user environments. In a typical data center, almost 75% of the traffic flows East-West, and the rest North-South. Yet, enterprises have been relying heavily on perimeter firewalls to protect the data centers.

The perimeter is static. They have rigid policies focusing only on the traffic entering and leaving the data center - assuming the environment south of the perimeter is safe. Enterprise data centers today have workloads spread across a mix of bare metal, virtual machine, and multi-cloud infrastructures.

Maintaining a consistent security policy in these environments is a big challenge using rigid perimeter security. Security teams have to do a lot of heavy lifting to get minimal visibility using perimeter solutions. This limited/incomplete visibility puts a lot of pressure on the admins, resulting in misconfigurations and inconsistent security postures.

PERIMETER FIREWALLS ARE RIGID.

Attackers are no more compromising the perimeter firewalls. They are more focused on getting inside the data center through vulnerable endpoints - through malware, phishing and social engineering attacks. In other words, the attacker is already inside the data center through compromised endpoints, exploring vulnerable ports on critical hosts and moving laterally *(East-West)* without getting detected.

Insider Threats – The Insider Threat Report (2018) from CA Technologies says that 90% of the enterprises surveyed feel vulnerable to insider threats. This is despite the organizations having several point security products like DLP, IAM, data encryption, endpoint protection, cloud access security and more.

Remember, the insider attacks can be from malicious insiders misusing their credentials to deliberately wreak havoc, or the unsuspecting users whose systems have been compromised through phishing, malware and social engineering techniques.

PERIMETER FIREWALL SOLUTIONS ARE INEFFECTIVE IN PROTECTING EAST-WEST TRAFFIC.

In almost all the recent high-profile attacks, it took several days or even months to detect the breach that had spread laterally, eventually exfiltrating sensitive data to the attacker's command-and-control server. By the time the attacks get discovered, the damage has already been done – monetary loss and the subsequent damage to brand reputation.

143 million accounts, **209,000** credit card numbers

– Equifax Data Breach

300,000 computers in **4** days

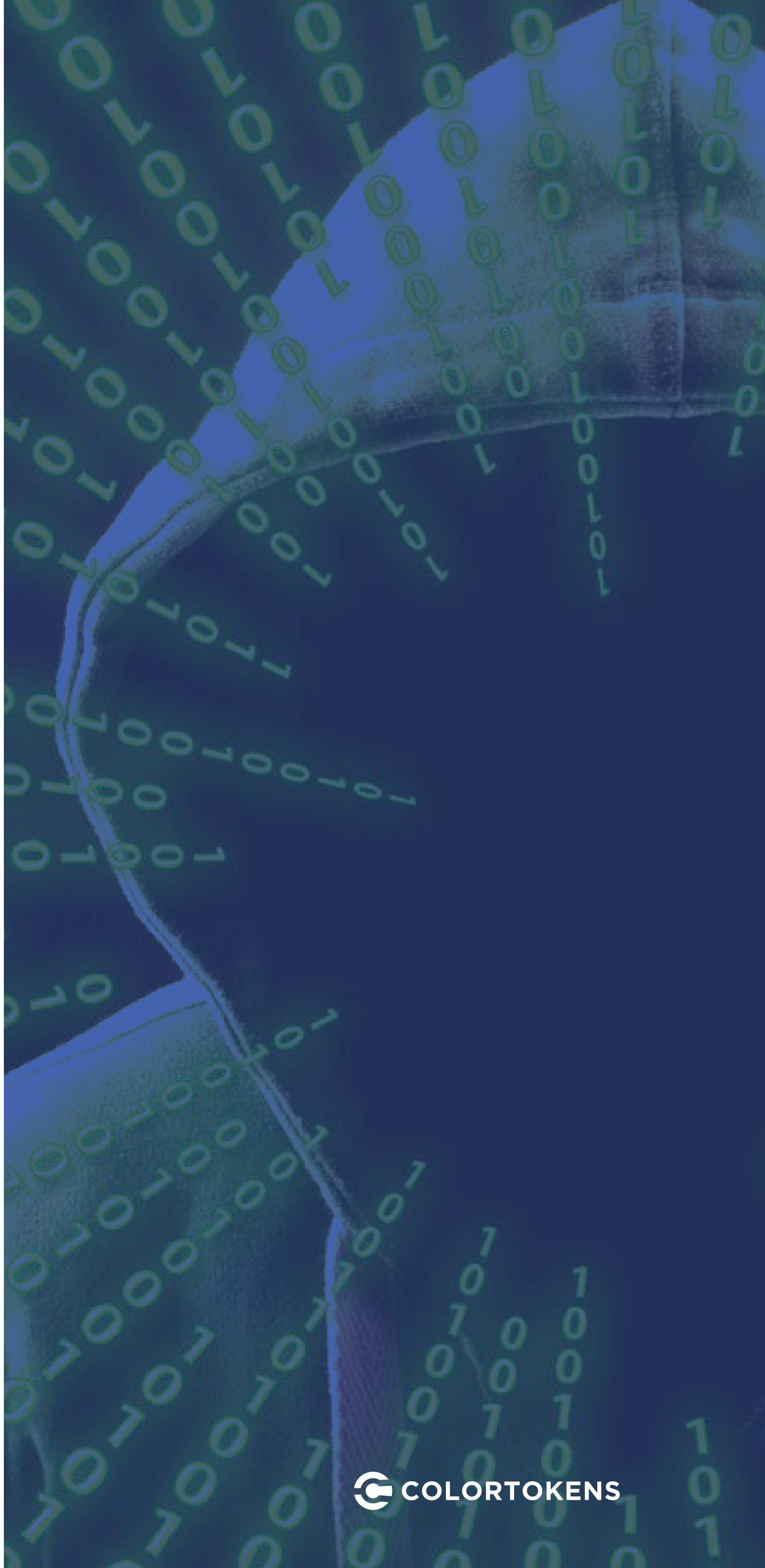
– WannaCry Ransomware

9.4 million passenger records

– Cathay Pacific

AVERAGE DWELL TIME – 191 DAYS[1]

[1] 2018 Cost of a Data Breach Study by Ponemon



SEGMENTATION USING INTERNAL FIREWALLS?

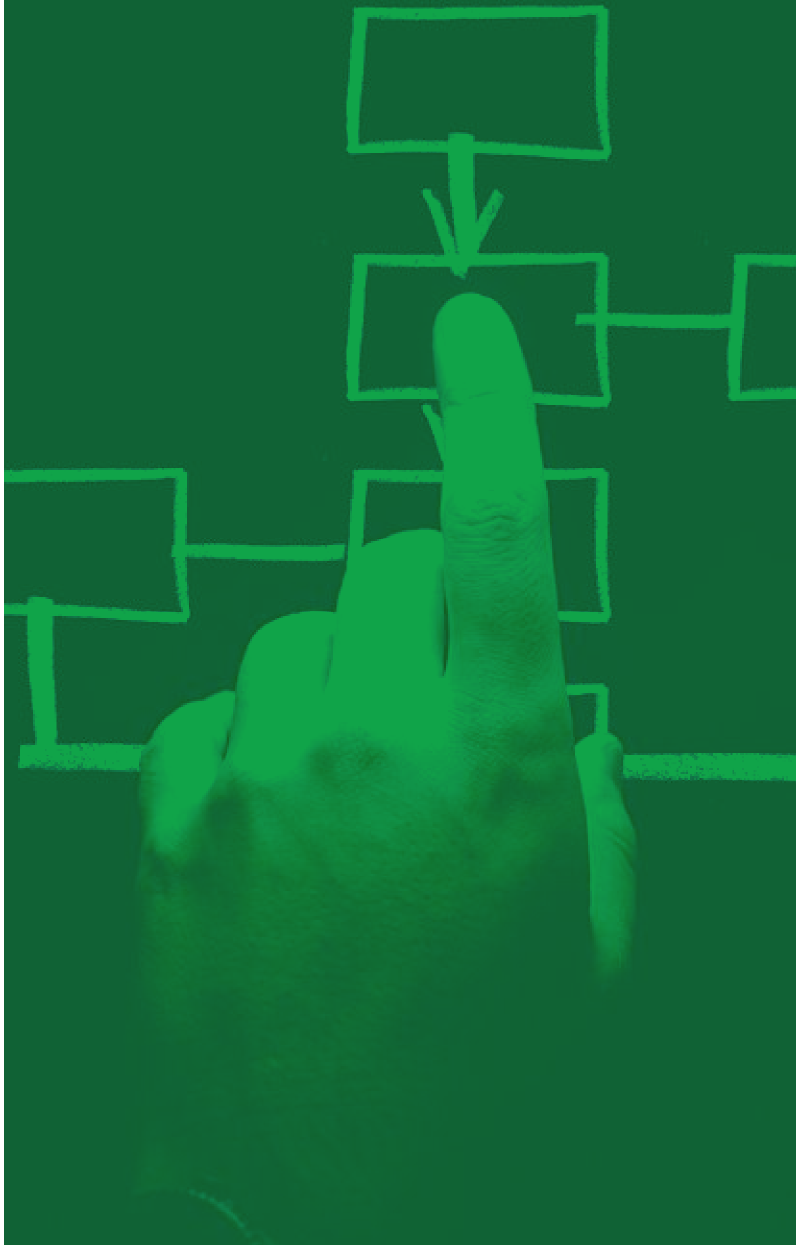
Now that we know perimeter firewalls can't secure East-West traffic, the other option is to protect the data center using internal firewalls. Internal firewalls can be used to segregate the data center into smaller segments and apply resource-access policies for the individual segments. Easier said than done.

Note that today's workloads are dynamic and continuously move from one VLAN to the other - again, adds to the issue on how to manage the policies on these workloads and keep them up-to-date when they move.

Let's say you want to implement environment separation for your application development segments in the data center. One of the most important goals here will be to separate the production environment from development, testing and staging environment.

You will deploy internal firewalls and create rules to make sure the production environment remains isolated from the development, testing and staging segments. You will also create policies based on IP addresses and protocols to define how this firewall should handle network traffic, aligning with your enterprise information security policy requirements.

CONGRATULATIONS!
YOU JUST ADDED CHOKEPOINTS IN YOUR NETWORK.



INTERNAL SEGMENTATION USING FIREWALLS: DISADVANTAGES

- Network-centric approach - creates macro-segmentation instead of micro-segmentation
- Doesn’t necessarily reduce the attack surface
- Extremely complex to achieve centralized visibility across on-premise and multi-cloud data centers
- Difficult to have fine grained/micro policies at workload level
- Policies don’t move across environments when the resource moves
- Difficult to accomplish zero trust security
- Thousands of firewall rules – cumbersome and error-prone in dynamic data centers
- Very expensive to procure and deploy multiple high-capacity internal firewalls
- Performance impact due to additional chokepoints
- Vendor lock-in overhead

MICRO-SEGMENTATION WITHOUT INTERNAL FIREWALLS – THE WAY FORWARD

Software-defined micro-segmentation is the way forward to address the security and operational challenges. One of the most notable advantages of a software-defined approach is that it's platform-agnostic, enabling micro-segmentation to be implemented across data centers without vendor lock-in headache.

Software-defined security, in general, is designed to span subnets, VLANs and firewalls, enabling enterprises to manage security across multi-vendor hybrid infrastructures from a single central console. This will save you from dealing with complex network-level constructs like IP addresses and thousands of firewall rules.

In short, software-defined security works with the customers' existing infrastructure, without zero disruptions - achieves far better results with comprehensive visibility, operational ease, and manageability.

REDUCING THE ATTACK SURFACE: WHAT ELSE IS NEEDED?

The end goal of data center segmentation is to reduce the attack surface and protect the hosts (workloads) from cyber-attacks. Segmenting using internal firewalls cannot achieve this completely.

With software-defined micro-segmentation you can **eradicate the gap between your enterprise's desired security posture and the actual state of security**, by enforcing resource access policies purely based on intent.

In order to significantly reduce the attack surface, the micro-segmentation solution must encompass the following:

- **Threat Visibility** - Granular visibility to understand the state of security across your data center
- **Intent-based Policies** – Assess, measure and continuously improve the security posture
- **Residual Risk Metrics** – Analyze and prioritize security tasks in conjunction with threat visibility and intent-based policies

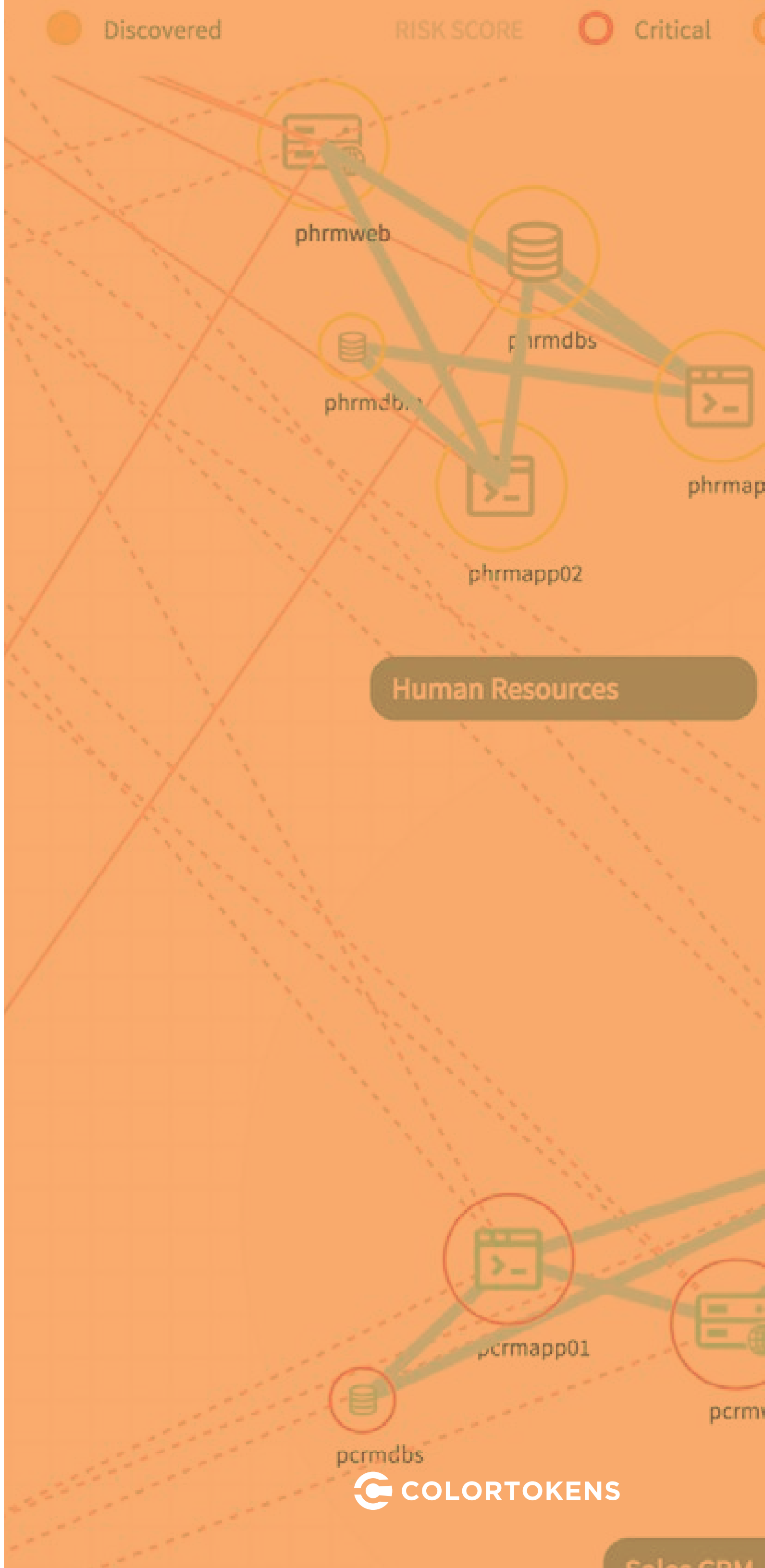
This is because in software-defined, micro-segmentation is done at the host level, instead of at the network level.

SHIFTING TO HOST-BASED SEGMENTATION

With software-defined micro-segmentation, you can shift the segmentation to the host, instead of segmenting at the network level. In other words, it’s akin to implementing perimeter security at every host.

Typically, to make host-based micro-segmentation effective, it must include the following capabilities:

1. A single-pane-of-glass to manage, orchestrate and automate resource access policies across dynamic application environments
2. Leverage security features natively available on the workload
3. Secure and monitor workloads no sooner than they are created
4. Consistent security policies that follow the workload
5. Built on zero trust security architecture
6. Tamper-proof security policies



CONCLUSION

Traditional micro-segmentation techniques resided at the network level – making the security journey of an enterprise cumbersome, error-prone and ineffective. Software-defined micro-segmentation is enabling enterprises make the paradigm shift towards accomplishing security that's not reactive – simplifying the overall security journey.

Host-based micro-segmentation reduces the attack surface and provides granular control over the policies applied to dynamic application environments - irrespective of the operating system, underlying technology and location of the workload. Software-defined micro-segmentation eliminates the need for expensive internal firewalls, enabling enterprises to protect the data centers from sophisticated cyber threats.

PROACTIVE SECURITY FOR HYBRID DATA CENTERS

COLORTOKENS

About ColorTokens

ColorTokens is a Silicon Valley company, backed by legendary investors and advisors who have helped structure the IT industry over last 30+ years. ColorTokens' core team brings deep and innovative industry experience from brands such as Cisco, Juniper, VMware, Microsoft, and Zscaler in domain areas including cybersecurity, networking, and infrastructure. With customers and partners worldwide, ColorTokens is headquartered in Santa Clara (Silicon Valley), CA, USA with a major center of development and sales in Bengaluru, India.

2101 Tasman Drive, Suite 201, Santa Clara, CA 95054 | E: sales@colortokens.com | P: +1 (408) 341-6030 | www.colortokens.com