Connecting All the Dots: Do You Know **What's Missing** in Your Network?

Juniper Networks | **Engineering** Simplicity

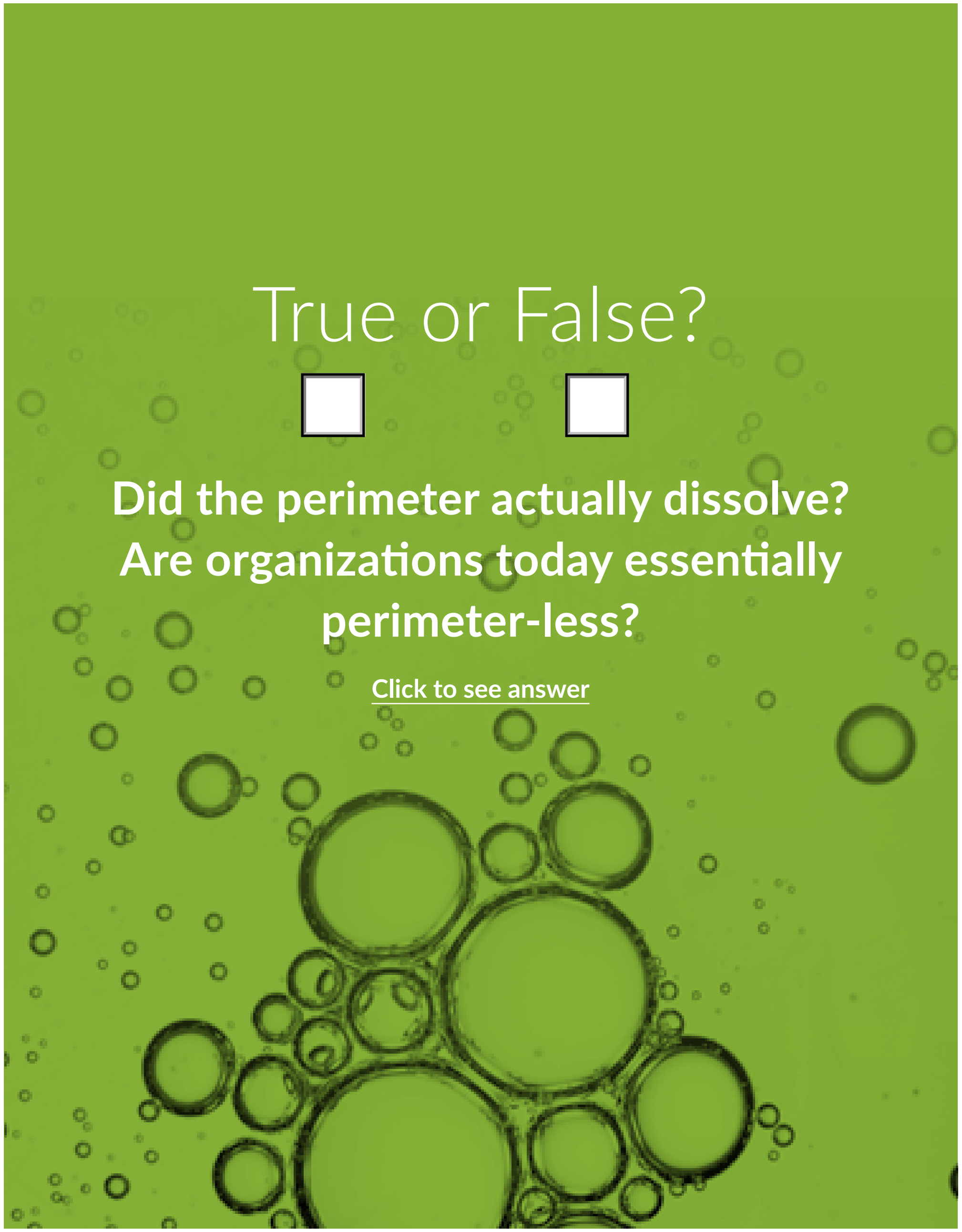
August 2019

Introduction

As organizations move increasing numbers of workloads to distributed, multicloud environments and adopt connectivity-dependent trends such as the Internet of Things, the simpler networks of yesterday have steadily morphed into something considerably more complex. It's this growing complexity that is the ultimate enemy of effective security.

Successful cybersecurity breaches continue seemingly unabated, as organizations struggle to overcome complexity and improve the security of their networks. One response is to layer on more security tools, and businesses are doing just that; they are spending more than ever on security tools to protect their networks, applications, and data — all to little avail.

This begs the question: Are organizations missing something fundamental in their approach to network security today? The short-and-simple answer is yes, and it's what this ebook is all about. Read on to test your security knowledge while discovering the missing, essential aspects of effective network security.



True or False?

□ □

Did the perimeter actually dissolve? Are organizations today essentially perimeter-less?

Click to see answer

Find the **Weakest Link**

Gartner forecasts that worldwide spending on information security products and services will reach $124 billion in 2019, an increase of 8.7 percent compared to 2018.[1] This continued growth includes spending on security technologies and solutions such as: next-generation firewalls, sandboxing, cloud access security brokers (CASB), security information and event management (SIEM), and endpoint protection, to name a few.

Yet recent experience shows that buying more products that do not integrate with each other, or the network, is not effective at identifying and stopping cyberattacks. Cybercriminals can still find weak links and use them to execute successful attacks and breaches. At this point, company leaders and security stakeholders realize that their considerable investments in best-of-breed security products are not yielding the promised level of protection.

To find the answer, these leaders need look no further than their complex, siloed solutions across the network. The key is integration, where products and components work together. A network is only as secure as its weakest link, and without deep collaboration and synchronization between all parts of the network (including security products), enterprises still have security weaknesses that leave them vulnerable to attack.

Spot the Network Security Weakness

1

Security solutions must be able to communicate with and take advantage of your networking components and endpoints; otherwise, you lose ____________________.

2

Security solutions must be able to ____________________ reports of abnormal behavior from all different sources such as firewalls, switches, endpoints, other network and security elements.

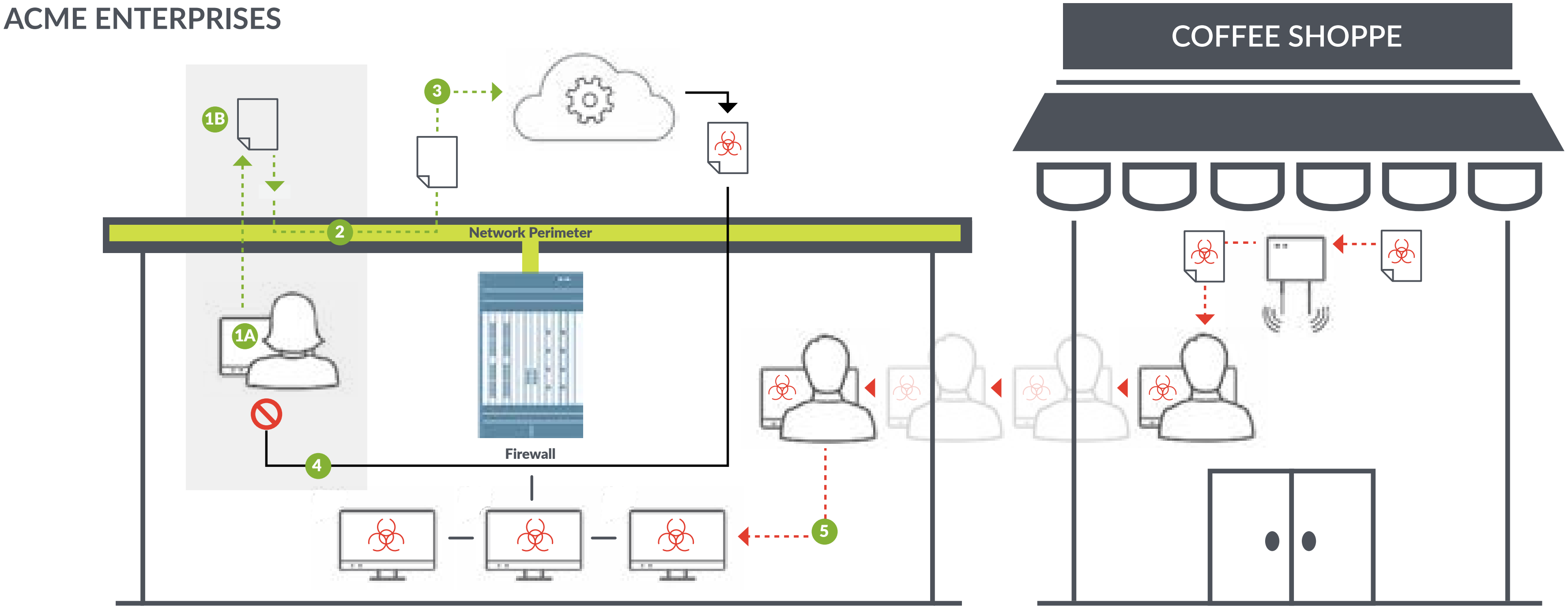
Click to see answer

[1] "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," Gartner, August 15, 2018

Mind the **Gap**

In this diagram of a network compromise, can you find the gap in security that allows malware to spread to all other reachable hosts?

1. A host within the corporate network (A) attempts to download unknown malware (B).
2. The file containing the malware is scanned for known threats at the perimeter firewall.
3. The firewall sends the file to an antimalware service for analysis, which notifies the firewall that the file contains malware.
4. The firewall blocks the file, preventing it from being downloaded.
5. **FIND THE GAP:** Despite these measures, a different host within the network is able to spread malware throughout the network as shown in the diagram. Why can't the firewall prevent the spread of the malware like it did with the first host in the example? Click to see answer



Transform Traditional Networks Into Secure Networks

Now we know that the missing piece of effective network security today is integration. Seamless integration enables security and networking technologies to work together, even if the products are from different vendors. With integration, existing network and security elements combine in a multivendor environment, with centralized policies, analytics, and management across all of the components.

Connecting and automating network and security technologies is what Juniper Connected Security is all about. With Juniper, you can safeguard users, applications, and infrastructure by extending security to all connection points across the network, even taking advantage of other vendors' technologies. With the entire network and cloud as enforcement points, you improve protection against threats across your environment, eliminating gaps in security.

With Juniper, you gain the end-to-end and top-to-bottom visibility you need to see who and what is on your network or in your multicloud environment. By connecting security and network components, you get visibility, analysis and correlation of potentially malicious network traffic on premises or in the cloud, all with consistent security policies.

Question: What Makes Juniper Connected Security Work?

To connect your security with your network at all connection points, you need the ability to build on the security solutions and infrastructure you already have. And to build on what you have requires ______________.

Click to see answer

Understand the Challenges of Security In **Multicloud Environments**

Modern environments are increasingly distributed, with workloads running across multiple public clouds as well as private cloud. While enabling superior time-to-market, scalability, resiliency and agility for the business, modern environments create greater operational complexity and expand the attack surface—all of which can lead to weaknesses in defense.

While security practitioners must allow the flexibility of cloud development to happen, they still need to minimize risk to the business. This can be challenging because multiple clouds—when running in silos instead of under the control of a single, secure enterprise network—create gaps in visibility while making it difficult to implement consistent security policies across the entire environment.

For example, a company may have manufacturing applications and data in one public cloud and its enterprise resource planning system in a different public cloud, each one essentially running in its own silo. Without centralized and integrated security across the network, a configuration error in one of the public cloud services could go undetected and make the company vulnerable to a data breach on the effected cloud. It could also potentially enable an attacker to move laterally into workloads on other clouds or in the data center.

That's why connected security must not only include the cloud, but integrate and support a multicloud environment as a single, cohesive infrastructure.

Test Your Cloud Security Knowledge

1 **Who is responsible for security in the cloud?**

- □ **A. The cloud provider**
- □ **B. The cloud customer**
- □ **C. Both the cloud provider and the cloud customer**

2 **True or False?**

□ □

Cloud providers are responsible for the security of traffic between different clouds, while cloud customers are responsible for the security of traffic between their data centers and the cloud.

3 **Most ________________ that have occurred on public cloud servers have been the cloud customers' fault.**

Click to see answers

Secure and Automate **Your Multicloud Environment**

Multicloud is about connecting and securing applications end-to-end, from the data center to the business edge, across many clouds, as simply as if they were in one cloud. A secure, multicloud solution lets you create consistent security policies that follow workloads wherever they need to execute, whether that's in a private or public cloud.

For example, a gaming company may start with its own private cloud, but for its next game it moves to the public cloud for greater elasticity (the ability to grow or shrink infrastructure resources as needed automatically). The company wants to take its security with it to the cloud, and would like the ease and consistency of using the same policies for enforcement and management both on premises and in the cloud.

The gaming company can achieve its goals with Juniper Connected Security. Juniper automates security coverage from endpoints to edge and every cloud in between. It lets the gaming company see security events and threat intelligence, protect your network by translating information into insight, and automate remediation of threats across all connection points.

True or False?

□ □

Companies can be infected by ransomware through the use of cloud applications.

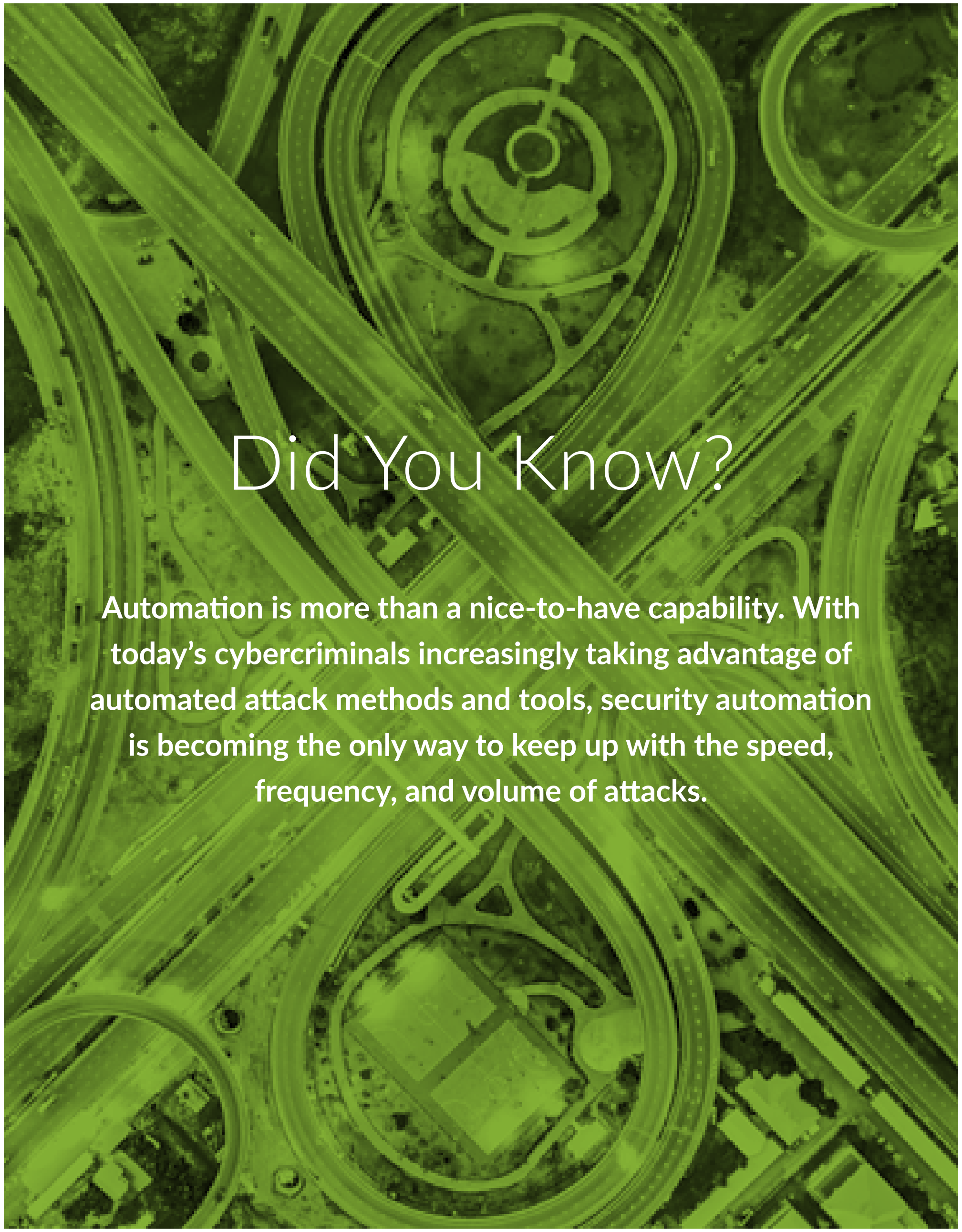
Click to see answer

Connect All the Dots With **Automation**

Security teams often face tens or even hundreds of thousands of alerts per week, with one report showing that they are inundated with more than 174,000 alerts on a weekly basis.[2] This enormous volume of data is generated by numerous, disparate sources and then presented to overworked, understaffed security teams for review. The effort to analyze, correlate and prioritize disparate threat data and alerts is simply overwhelming, making threat detection and mitigation incredibly difficult, and increasing time to remediation.

While the security industry has acknowledged the need to automate these manual efforts, solutions to date haven't taken a holistic approach. Instead, organizations end up with isolated pockets of automation, which are siloed by vendor. For instance, a threat detection and response solution from one vendor may automate detection of a threat, but doesn't integrate with network components from a different vendor to automate investigation and policy enforcement.

Juniper Connected Security is the answer. With seamless integration with security and network solutions, you can detect threats and automatically enforce security policy throughout your network, including your multicloud environment. Juniper includes automatic enforcement at Juniper switches, third-party switches across wireless networks and within workloads in the cloud to block threats at the network level.



Did You Know?

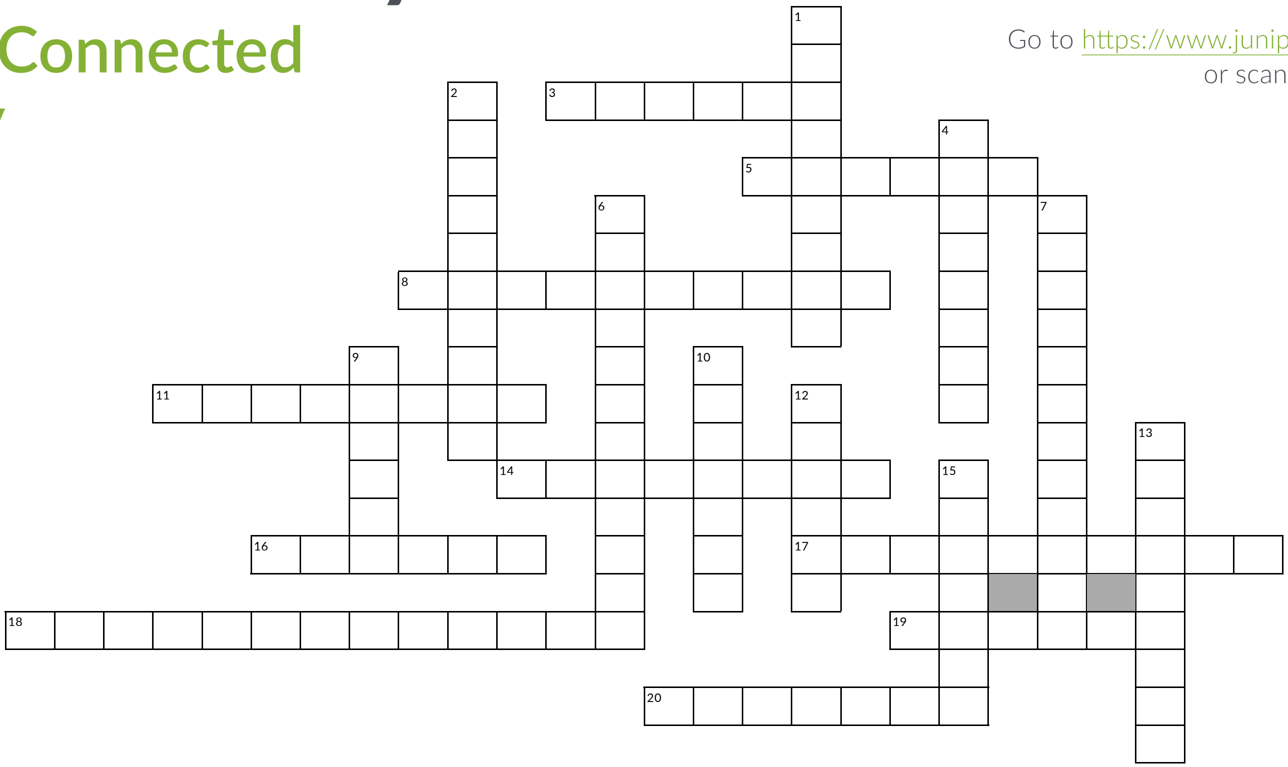
Automation is more than a nice-to-have capability. With today's cybercriminals increasingly taking advantage of automated attack methods and tools, security automation is becoming the only way to keep up with the speed, frequency, and volume of attacks.

[2] "Latest Research Shows Security Teams Review an Average 12,000 Alerts/Week, Setting the Stage for Automation," Demisto, September 2018

Solve the **Security Puzzle**

Juniper Connected Security

Go to https://www.juniper.net/us/en/crossword-answers
or scan the code below for the answers.



ACROSS

3. Term given for the smallest unit of information transmitted across networks
5. Private, secure path through an otherwise public network
8. Process of changing data into a form that can be read only by the intended receiver
11. An attempt to acquire sensitive information by masquerading as a trustworthy entity
14. Security gateway positioned between two networks
16. An attempt to exploit vulnerabilities in hardware and software
17. The act of abiding by and adhering to a set of standards, rules, and laws
18. A characteristic or weakness that renders an organization or asset open to exploitation
19. A collection of computers compromised by malicious code and controlled across a network
20. With Juniper Connected Security, you can see, automate and ___________________

DOWN

1. An unauthorized act of bypassing the security mechanisms of a network or information system
2. Authentication, authorization and ___________________
4. The designated threat level of an attack
6. A method of protecting information and communications through the use of codes
7. The unauthorized transfer of information from an information system
9. A person or object that presents a danger
10. Designed to disrupt computer operation, gain access to private systems, or gather sensitive information
12. Set of rules defining access to your network
13. A recognizable, distinguishing pattern
15. A technique to breach the security of a network or information system

See, Automate and Protect With **Juniper Connected Security**

With Juniper, you can see, automate and protect network and security technologies to effectively safeguard your organization, while streamlining operations. Our seamless security architecture:

- Safeguards users, applications and infrastructure against advanced threats
- Automates security coverage from endpoints to edge, and every cloud in between
- Delivers multicloud-readiness where everything works together at scale
- Lets you see who and what is on your network and enforce across all connection points
- Provides end-to-end, top-to-bottom, best-in-class secure networking
- Is interoperable so you can build on security solutions and infrastructure you already have

Answers

True or False?

False. Contrary to popular opinion, the perimeter did not dissolve. However, it has evolved in significant ways that mean you can no longer rely solely on security at the perimeter to protect your organization.

◀ *Back to page 3*

Spot the Network Security Weakness

1. **Visibility** (without which you can't effectively identify and prevent threats.) You also restrict the number of points in your network where you can enforce security policy.
2. **Aggregate.** You need a solution that collects and aggregates data and distills it into actionable intelligence.

◀ *Back to page 4*

Find the Gap

Perimeter enterprise network firewalls are designed to block unauthorized content such as malware from entering the network from external sources. However, they typically do not block threats that are traveling within the network (known as east-west traffic). In our scenario, a host has been compromised with malware while it was outside of the corporate network (i.e., a non-enterprise environment) or by manual means. Upon reconnecting with the corporate network, it then infects all other reachable hosts in the network because the firewall is only protecting external (north-south) traffic and because the malware mimics legitimate network traffic.

◀ *Back to page 5*

What Makes Juniper Connected Security Work?

Interoperability. Juniper Connected Security allows you to keep your existing networking and security gear while transitioning to a more secure network. By partnering with other network and security vendors, Juniper offers a collaborative and comprehensive approach to network security.

◀ *Back to page 6*

Test Your Cloud Security Knowledge

1. **C.** Both the cloud provider and the cloud customer are responsible. Called the Shared Responsibility Model, security is a shared responsibility between these two parties. The cloud service provider is typically responsible for protecting the hardware and software that the cloud runs on, while cloud service customers are responsible for securing their assets running within the cloud, such as networking, workloads and data.

2. **False.** Cloud customers are responsible for securing traffic both to and from the cloud as well as between different cloud environments. A secure, multicloud environment has consistent protection across the entire infrastructure within the campus, across branches, between clouds and inside the data center.

3. **Breaches.** The overwhelming number of security breaches in the cloud are preventable and are caused by cloud customers not following configuration and security best practices. In fact, research firm Gartner, Inc. predicts that "through 2022, at least 95 percent of cloud security failures will be the customer's fault."[3]

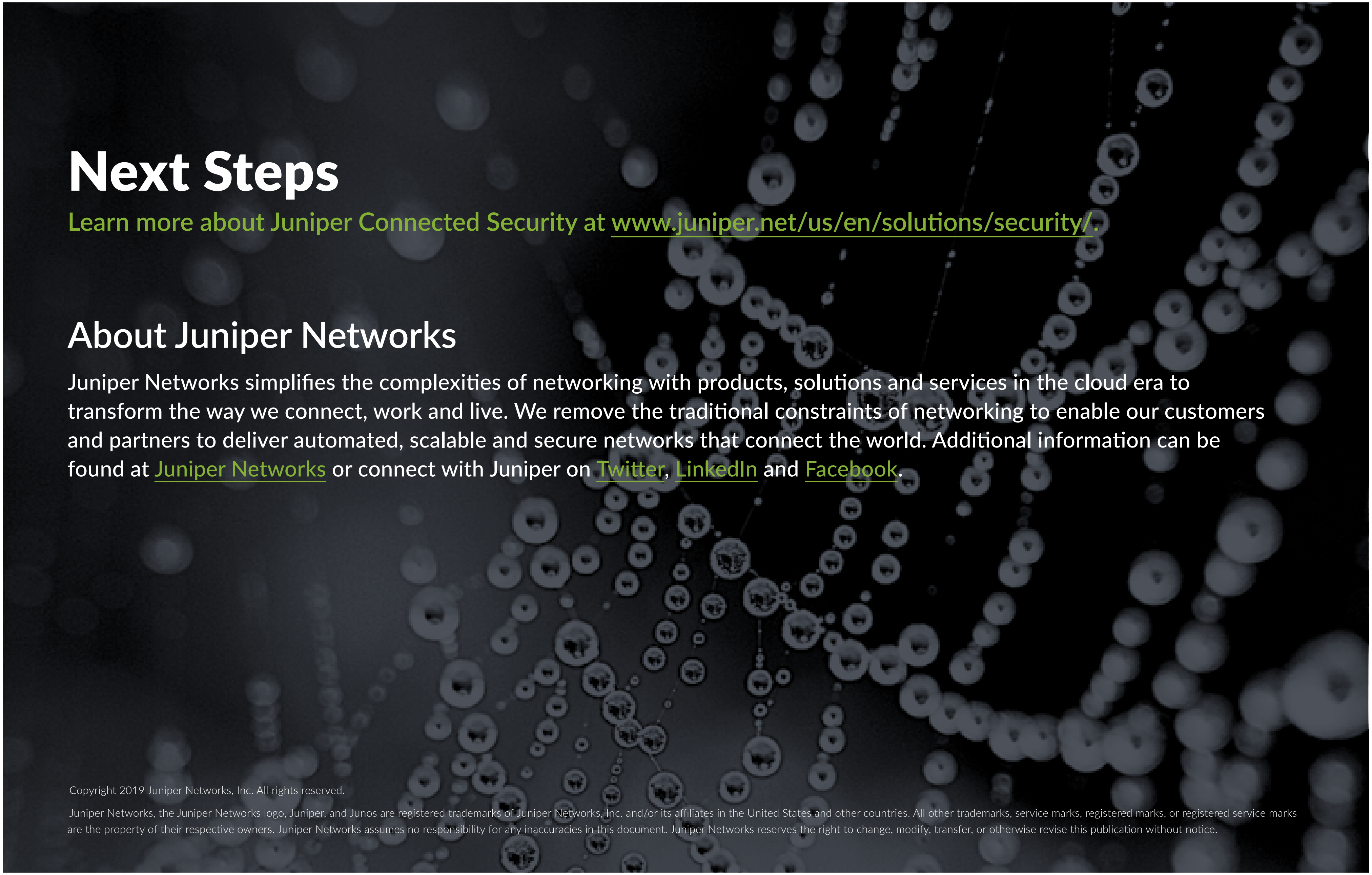
◀ *Back to page 7*

True or False?

True. Cybercriminals target cloud applications because of the ease and speed of disseminating malware such as ransomware. That's why you need connected security that detects and prevent threats from spreading to all points in your network when one user logs into an infected cloud application.

◀ *Back to page 8*

[3] "Is the Cloud Secure," Smarter with Gartner, March 27, 2018



Next Steps

Learn more about Juniper Connected Security at www.juniper.net/us/en/solutions/security/.

About Juniper Networks

Juniper Networks simplifies the complexities of networking with products, solutions and services in the cloud era to transform the way we connect, work and live. We remove the traditional constraints of networking to enable our customers and partners to deliver automated, scalable and secure networks that connect the world. Additional information can be found at Juniper Networks or connect with Juniper on Twitter, LinkedIn and Facebook.