



E-BOOK

THE STRATEGIC IMPERATIVE FOR BOUNDLESS CYBERSECURITY

Mobilising for your new normal

SONICWALL® SHOP
A Breathe Technology Business



INTRODUCTION

Legacy cybersecurity approaches fall short. They have you playing “threat roulette,” unable to stop hidden and unknown malware, and creating seams and blind spots in your visibility, protection and analysis.

Moreover, they can be real budget-busters. Rising costs of conventional security, shrinking budgets and staff, as well as a limited availability of qualified personnel, all make it hard to keep up. And suddenly, with the disruption of the traditional office-centric workforce, the new normal is that everyone is remote and unsecure.

SonicWall believes there is a way forward. This e-book takes a closer look at how your organization is facing a cybersecurity business gap, and why you have a strategic imperative to bridge that gap with a new Boundless Cybersecurity model.



“In an age of anywhere, anytime, hyper-distributed business, how can you protect your operational integrity while mitigating risk? SonicWall believes there is a better way forward.”

Bill Conner
President & CEO
SonicWall

THE ERA OF **HYPER-DISTRIBUTED,** **REMOTE-FIRST BUSINESS HAS ARRIVED.**

Today's massively expanding distributed IT reality is fueled by:

- The race to digitise
- The proliferation of apps and devices
- Componentised and virtualised capabilities
- The pervasive cloud
- Borderless organisations
- Evolving regulatory compliance
- Sensors everywhere





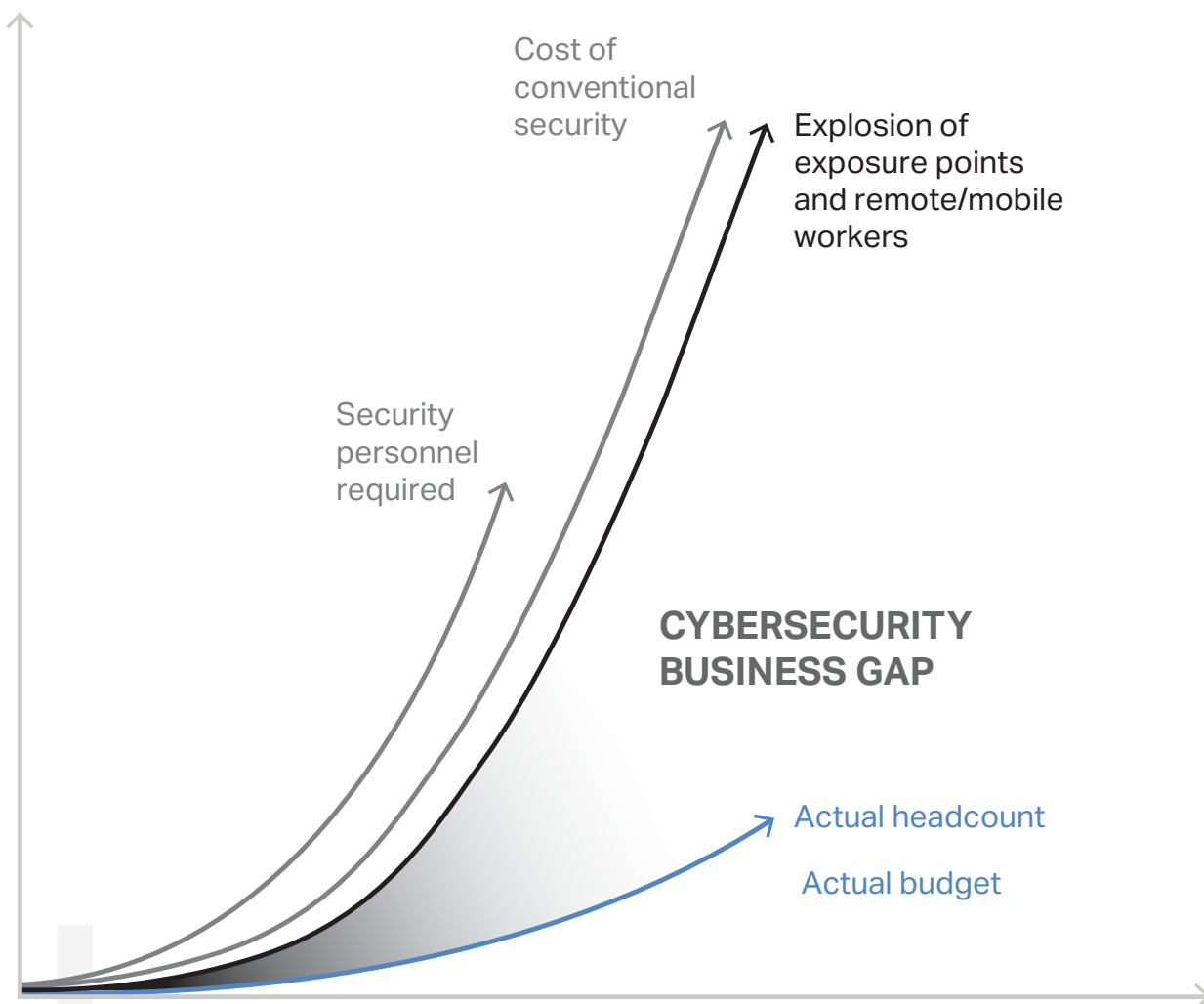
AND AN UNEXPECTED ACCELERATOR.

A new work reality has hit with deep and sudden impact.

Everyone is remote.
Everyone is mobile.
Everyone is less secure.

WE'RE FACING A CYBERSECURITY BUSINESS GAP.

- **Risk** escalates with the explosion of exposure points and remote/mobile workers
- **Cost** grows increasingly prohibitive and the shortage of trained personnel becomes more acute
- Constrained **resources** simply can't keep up



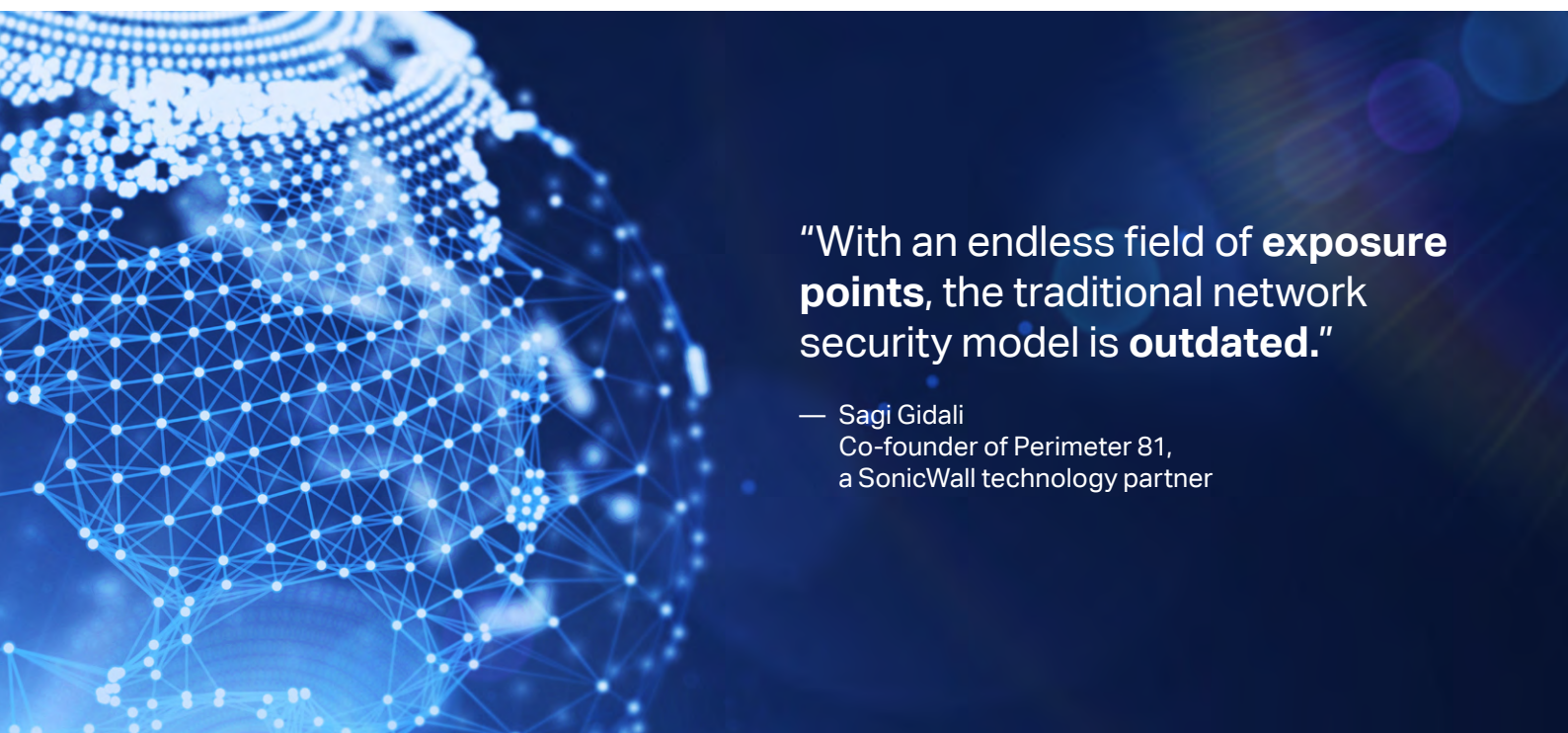
THERE IS AN EXPLOSION OF EXPOSURE POINTS.

Citing the rapid emergence of IoT across multiple industries, [Gartner states](#) 5.8 billion endpoints will be in use in 2020.

Predictions forecast up to over a trillion programmable endpoints over the next two decades.

Our cybersecurity defenses are confronted with an explosion of endpoints.

- Myriad endpoint devices
- 4- and 5G mobile devices
- Networking and security devices
- Public and private cloud applications
- Email
- Wi-Fi
- IoT devices
- BYOD



“With an endless field of **exposure points**, the traditional network security model is **outdated**.”

— Sagi Gidali
Co-founder of Perimeter 81,
a SonicWall technology partner

THREATS ARE INCREASINGLY EVASIVE.

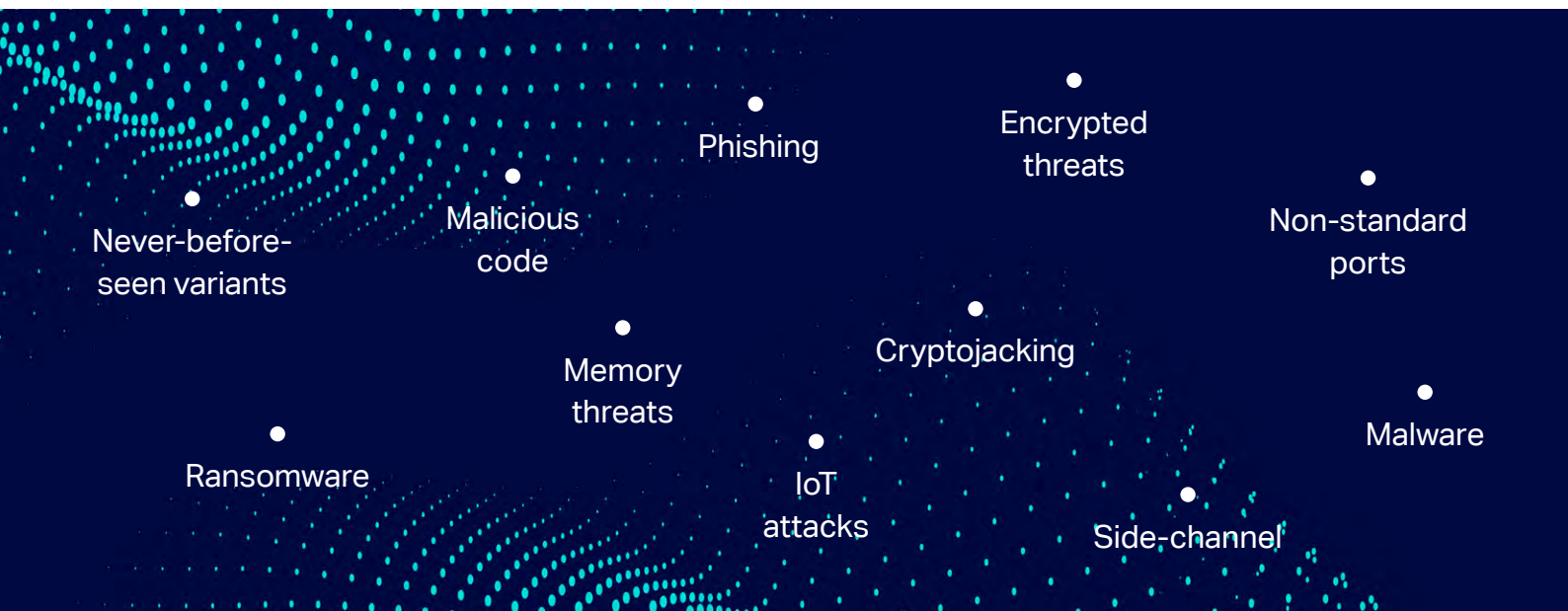
Across all threat vectors, the array of threat types are also expanding, deepening and getting smarter.

Never-before-seen variants are up 145% year-over-year. Organizations are seeing a 60% change in types of threats and 45% increase in the number and frequency of threats.

Zero-day and other emerging threats are successfully bypassing traditional firewalls and sandboxes at an alarming rate.

Your organisation may have no idea of what's being missed

- File-less attacks
- Encrypted threats
- Phishing & spear phishing
- Memory-based malware
- Side-channel attacks



SECURITY COSTS CONTINUE TO RISE — AND SKILLED STAFF IS HARDER TO FIND.

While no surprise, the cost of cybersecurity continues to rise. Gartner notes an 8.7% year-over-year increase in IT security spending last year.

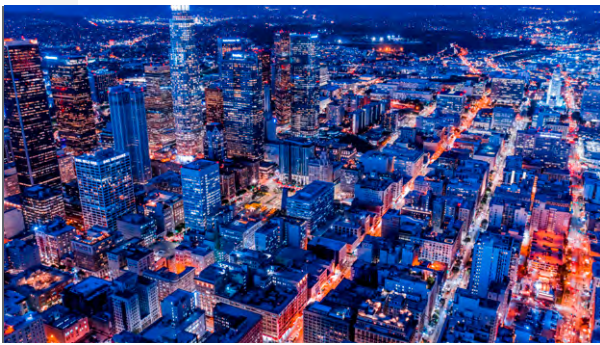
And while many organisations plan on increasing the size of their departments, a growing number of those face challenges with inadequate security budget to fill those slots.

- Global cybersecurity spending to cap **\$1 trillion** by the end of this decade
- **39%** of organisations have inadequate security **budget**
- **59%** have too few security **personnel**
- **51%** report cybersecurity personnel missing **skills**
- **Unfilled** cybersecurity jobs are expected to reach **1.8 million** by 2022

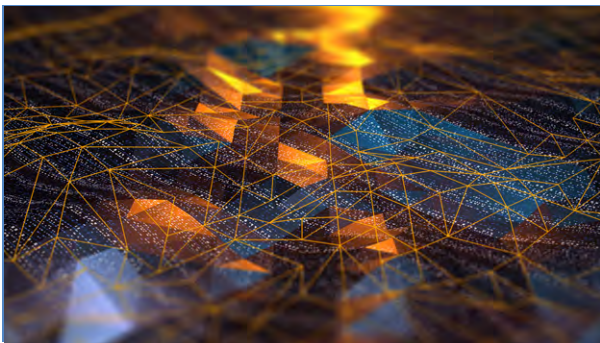


SHIFT TO A BOUNDLESS CYBERSECURITY MODEL

Break free from untenable technology, staffing and economic constraints – and mobilize for the new business normal of a 'boundless workforce' – with a new paradigm that lets you:



Know the Unknown



Unify Visibility & Control



Disrupt Outdated Economics



KNOW THE UNKNOWN

- Identify, authenticate, verify and safeguard known and unknown remote users and employees
- Spot and prevent unknown, evasive threats in real time, blocking them until verdict
- Protect all attack surfaces with seamless, multi-layered security coverage
- Deliver security to users, devices, and data anywhere and everywhere
- Provide security that is always on, learning and catching threats as they emerge and evolve
- Leverage a real-time network of global cybersecurity intelligence, AI and machine learning

UNIFY VISIBILITY AND CONTROL

- Connect and secure a boundless workforce across all environments to eliminate blind spots
- Gain a unified view of risk, including prioritization and control across your entire organization and multiple generations of IT infrastructure
- Increase visibility and control over dispersed remote, mobile and work-at-home employee systems and traffic
- Integrate unified end-to-end visibility and control over technology, services and solutions to eliminate siloes
- Establish a continuously adaptive security posture that dynamically molds to the changing needs of your business

DISRUPT OUTDATED ECONOMICS

- Break free of conventional cost constraints with scalable TCO (total cost of ownership)
- Make it cost-effective to protect your business, not just in procurement, but over the life of your solution
- Lower overhead by reducing human intervention and easing use with intelligent automation and zero-touch deployment

SONICWALL BOUNDLESS CYBERSECURITY

BRIDGES THE CYBERSECURITY GAP

Leveraging our global threat intelligence, seamless real-time protection and scalable low TCO, SonicWall Shop can bring you into the Boundless Cybersecurity era.



Network Security

NETWORK SECURITY FIREWALLS

Advanced threat protection, from small businesses to global enterprises and cloud environments. Discover network security made boundless.



Email Protection

HOSTED EMAIL SECURITY

Protect against today's advanced email threats using a cloud email security service.



Advanced Threat Protection

CAPTURE ADVANCED THREAT PROTECTION (ATP)

SonicWall Capture ATP is a cloud-based, multi-engine sandbox that revolutionizes advanced threat detection. Included with Capture ATP, SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) blocks zero-day and unknown threats at the gateway – even those that hide via encryption or don't exhibit malicious behavior.



Secure SD-Wan

SECURE SD-WAN

Secure Software-Defined Networking in a Wide Area Network (WAN)

SD-WAN technology allows organizations and enterprises with branch locations to build highly available and higher-performance WANs. By using low-cost internet access (broadband, 3G/4G/LTE, fiber), organizations can cost-effectively replace expensive WAN connection technologies such as MPLS with SD-WAN. SonicWall delivers comprehensive, industry-leading security solutions that simplify SD-WAN deployments.



Virtual Firewall

NSV SERIES VIRTUAL FIREWALL

Get the scalability and agility of the cloud with all the security advantages of a physical firewall. The NSv Series is custom built to secure the cloud and shield your enterprise from resource misuse attacks, cross-virtual-machine attacks, side-channel attacks and common network-based exploits and threats.



Simplified Management

SONICWALL CAPTURE SECURITY CENTER

Watch over your entire security ecosystem with a scalable and synchronized SPOG management solution.



Wireless Security

SECURE WIRELESS ACCESS POINTS

SonicWave Wireless Access Points from SonicWall provide your business with an enhanced user experience by delivering the performance, range and reliability of 802.11ac Wave 2 and 802.11ax technologies. Benefit from advanced, industry-leading security and wireless features. Leverage ease of deployment and management at a low total cost of ownership.



SaaS Security

CLOUD APP SECURITY

Next-Gen Security for Office 365, G Suite and Other SaaS apps.

SonicWall Cloud App Security offers next-gen security for your users and data within cloud applications, including email, messaging, file sharing and file storage. For organizations adopting SaaS applications, SonicWall Cloud App Security delivers best-in-class security and a seamless user experience.



Secure Remote Access

SECURE MOBILE ACCESS (SMA)

Secure your infrastructure while empowering your workforce. The Secure Mobile Access (SMA) series offers complete security for remote access to corporate resources hosted on-prem, in cloud and in hybrid datacenters.




Endpoint Protection


CAPTURE CLIENT


SonicWall Capture Client is a unified client platform that delivers multiple Endpoint Detection & Response (EDR) capabilities, including behavior-based malware protection, advanced threat hunting and visibility into application vulnerabilities.

NEED A SECURITY CONSULTATION?

If you'd like an assessment of your security strategy, or have specific questions about the SonicWall Boundless Cybersecurity model, call us today!

 www.sonicwallshop.com
(*chat with a live representative*)

 0800 5202201 | 01223 209927

 enquiry@sonicwallshop.com

CONTACT A SECURITY EXPERT