

# Five reasons for the rise of the secure internet gateway

Security in a mobile, cloud-enabled world

## The way we work has changed



Branch/field offices

**70%**

connect directly to the internet<sup>1</sup>

Workforce

**49%**

are mobile workers<sup>2</sup>

Applications

**70%**

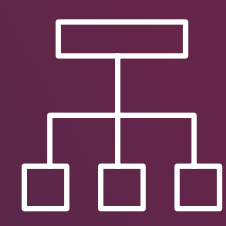
increase in SaaS app use<sup>3</sup>

## Security must also change

Built to solve the security challenges of today's mobile, cloud-enabled enterprise, a new category of products is emerging — the secure internet gateway.

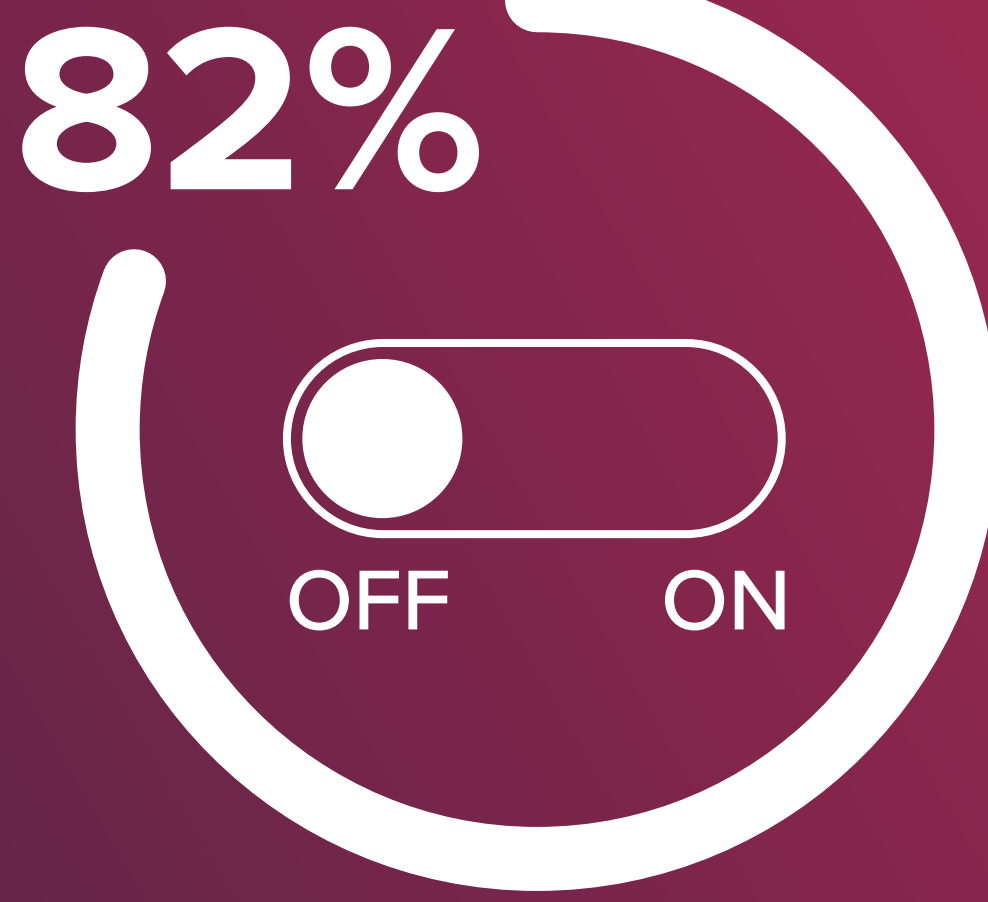
## Traditional Security vs. Secure Internet Gateway

82% of mobile workers admit that they do not always use VPN when working<sup>4</sup>



**Enforcement only on your network**

Perimeter security provides visibility and control for employee activity only when on your corporate network.



**Enforcement everywhere**

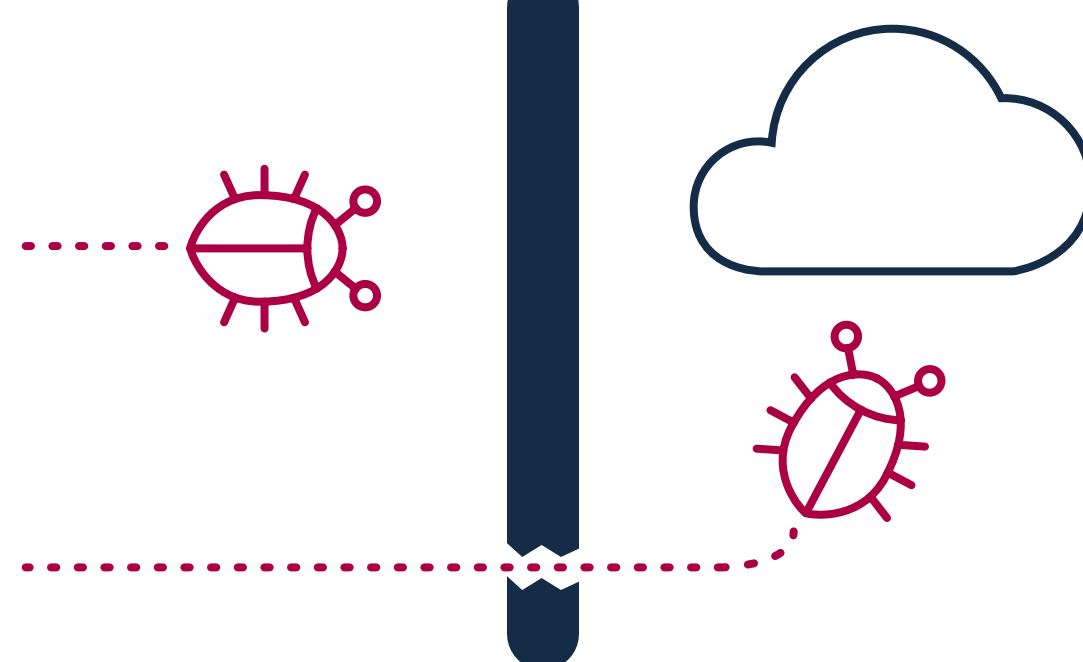
A secure internet gateway protects all devices on your network and roaming users.

15% of malware command and control (C2) callbacks use ports other than 80/443 to exfiltrate data<sup>5</sup>



**Protection against threats over web**

Web gateways only protect employees from threats over web ports 80/443.



**15%**



**Protection over all ports and protocols**

A secure internet gateway provides comprehensive protection over all ports and protocols.

60% of the time attackers penetrate and compromise an organisation within minutes, while detection takes days or more<sup>6</sup>

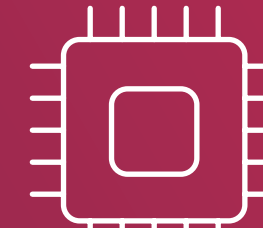


**Threat intel from only static reputation scores**

Traditional security neutralises threats only after detection. Appliance processing power limits hardware-based tools.



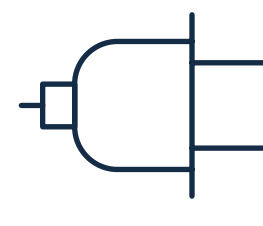
**60%**



**Threat intel from live internet requests**

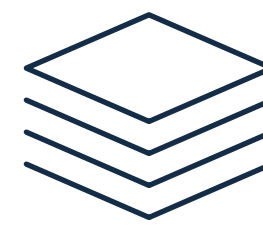
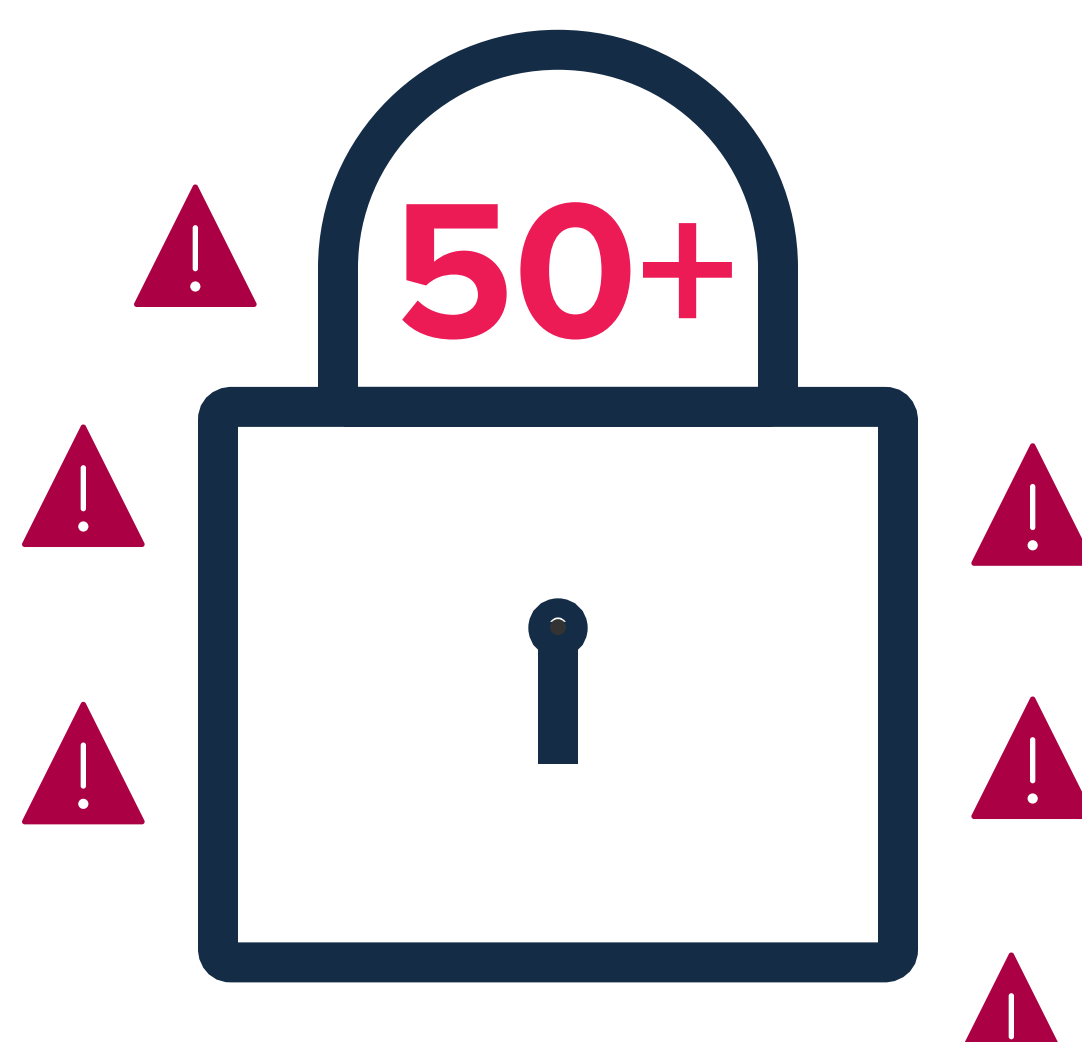
A secure internet gateway uses real-time threat intelligence from global internet activity to uncover attacks before launch. And, because it's cloud-delivered, it's not limited by appliance CPU.

Some companies use up to 50 different security vendors<sup>7</sup> and generate almost 17,000 alerts per week<sup>8</sup>



**Limited integration**

You likely have many different security products, but they work in silos with zero interoperability.



**Open platform**

A secure internet gateway provides APIs and built-in integrations to easily add and share intelligence among systems.

On average, companies use more than 475 third-party applications<sup>9</sup>



**Lack of visibility for SaaS apps**

With traditional security, you have limited or zero control over sensitive data in the cloud.



**475+**



**Discovery for SaaS apps**

A secure internet gateway helps you address risky or unsanctioned SaaS apps by easily identifying all accessed apps across an organisation.

Discover how a secure internet gateway can help your organisation protect users anywhere they access the internet.

Get the details by reading [“The Rise of the Secure Internet Gateway.”](#)

### Sources:

<sup>1</sup> “Securing Direct-To-Internet Branch Offices: Cloud-Based Security Offers Flexibility And Control,” Forrester, 2015

<sup>2</sup> “Securing Portable Data and Applications,” SANS, 2015

<sup>3</sup> “Keeping SaaS Secure,” Gartner, 2016

<sup>4</sup> “Your Users Have Left the Perimeter. Are You Ready?” IDG, 2016

<sup>5</sup> “Visual Investigations of Command & Control Botnet Behavior,” Cisco (Lanclope), 2013

<sup>6</sup> “2015 Cost of Data Breach Study: Global Analysis,” Ponemon Institute, 2015

<sup>7</sup> “Cisco 2017 Annual Cybersecurity Report,” Cisco, 2017

<sup>8</sup> “The Cost of Malware Containment,” Ponemon Institute, 2015

<sup>9</sup> “Cloud Cybersecurity Report: The Extended Perimeter,” Cisco (Cloudlock), 2015