T. Daniels Consulting

THE STATE OF OFF-PREM SECURITY

How Networks Without Borders Make User-Focused Security Paramount

INTRODUCTION

The Changing Landscape of the Remote Workforce

Each year, the industry continues to see cyber security breaches and attacks increase in volume at a staggering pace. For example, there were **16,555 known security vulnerabilities logged in 2018**; an increase of more than **10,000 since 2016** *(according to the Common Vulnerability and Exposures (CVE) list)*. Furthermore, there was an estimated **$45 billion in business losses worldwide** from cyber attacks *(according to the Online Trust Alliance)*, and a **62% increase in malware detections in Q1 2019** *(according to WatchGuard's Internet Security Report)*. Amidst these increasing threats, organizations are having to adapt to a shifting network perimeter driven by an increasingly remote workforce. To better understand the state of remote workforce security, WatchGuard commissioned a survey of US-based IT administrators and managers.

The findings below show just how pervasive remote work has become.

92%
of organizations **allow remote workers**

The average employee works **2+ days** from **home per week**

80%
expect the **remote workforce to grow** over the **next three years**

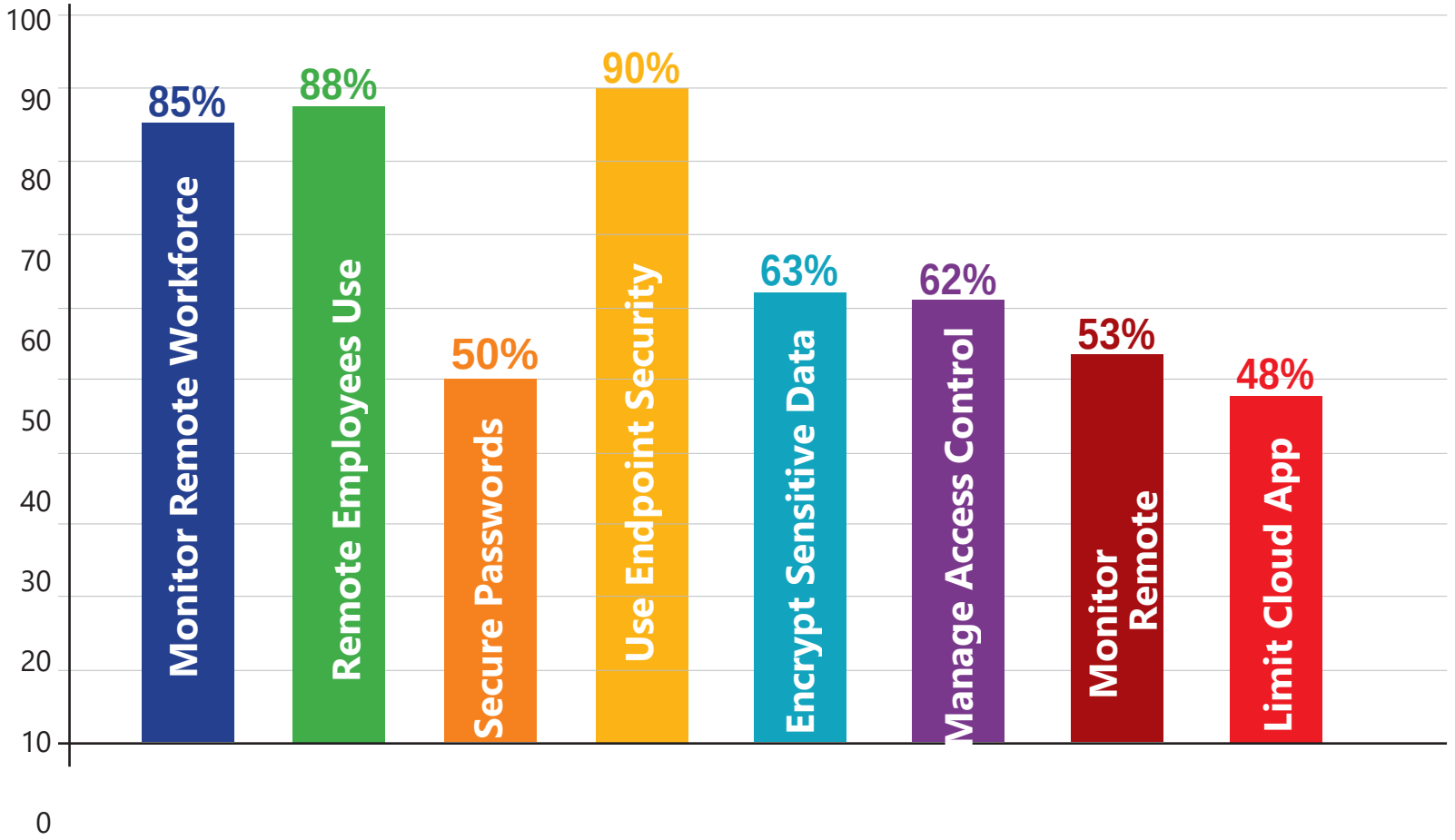
With this growth, remote employees must be protected against phishing attacks, credential theft, advanced malware, virus infections, unauthorized access to corporate resources and much more. To accomplish this, organizations are deploying a variety of technologies to help secure off-network endpoints and offer effective protection for employees working outside the core network perimeter.

But, how well are they doing?

Let's look at the rest of the survey results.

IT Admins Are Confident in Their Ability to Protect

The numbers are impressive! **IT pros appear to be incredibly confident when it comes to off-network security.**



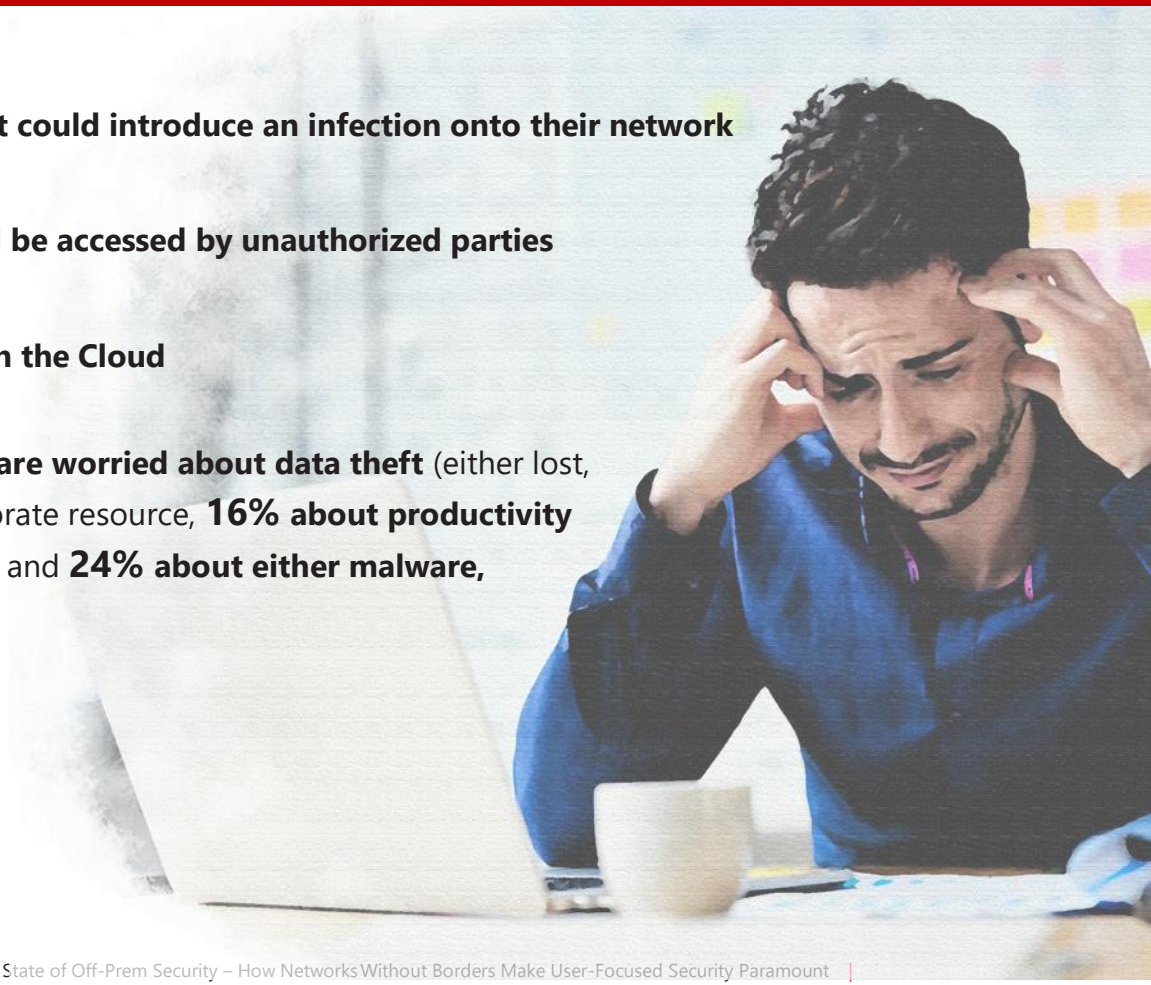
Contributing to this sense of confidence is the fact that 82% claim to have security awareness training programs in place, with **51% administering trainings on a quarterly basis**, and a massive **92% saying additional employee training happens immediately following a security incident**. And, more than **85% believe their employees are well-trained enough that they can identify and avoid phishing emails**.

But Is There a False Sense of Security at Play with Remote Employees?

Is this rapidly changing landscape creating some confusion about what it means to protect the remote workforce? As it continues to grow, IT administrators have some very real concerns and are making some startlingly inconsistent claims about their level of security preparedness.

Despite their confidence in protecting remote workers,

64% of IT administrators claim a remote worker has been the victim of a cyber attack.

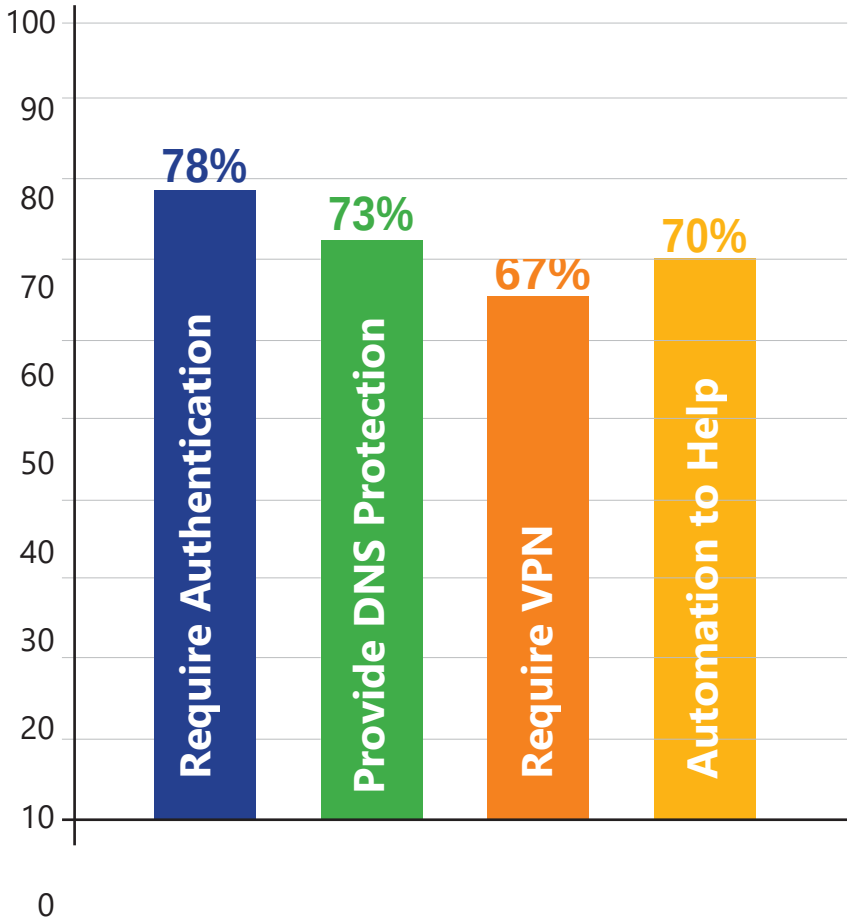


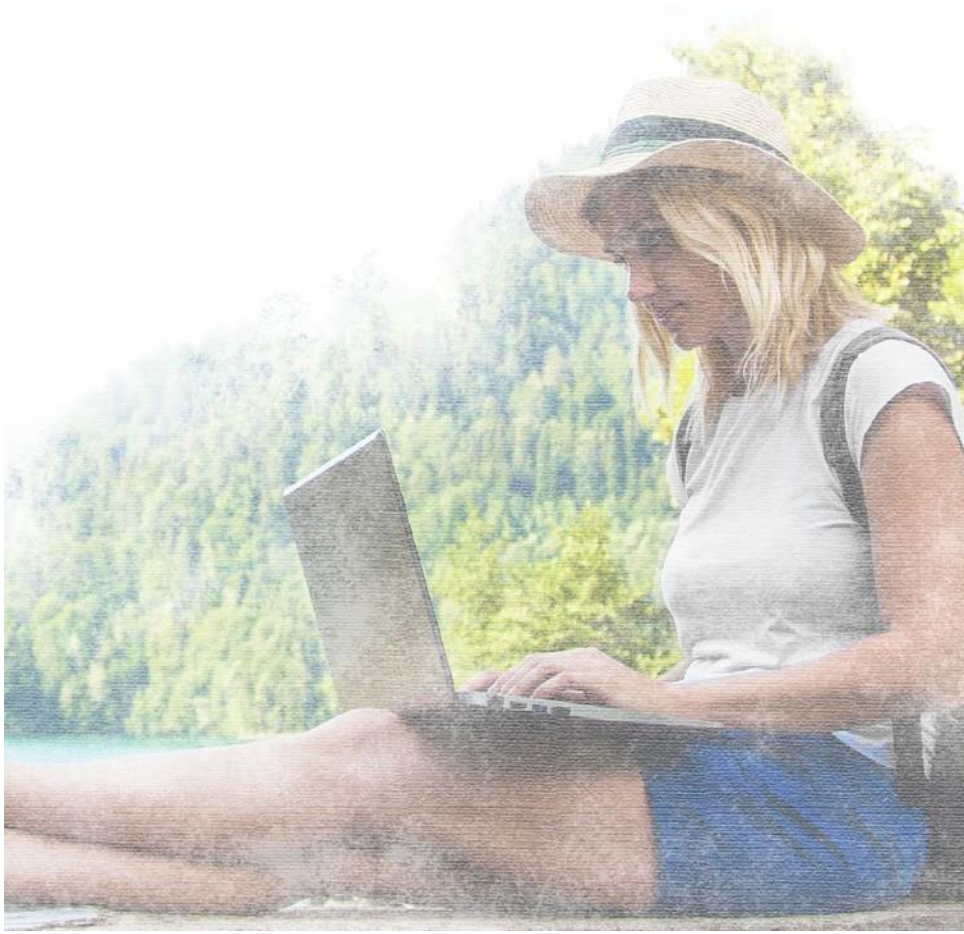
- **91%** state they're concerned that an **infected endpoint could introduce an infection onto their network** (despite 90% using an endpoint security solution)
- **89%** are worried that **remote employee devices could be accessed by unauthorized parties** while out of network
- **90%** are concerned with **sensitive data being stored in the Cloud**

Furthermore, when it comes to their remote workforce **31% are worried about data theft** (either lost, stolen or copied), **17% about unauthorized access** to corporate resource, **16% about productivity and availability**, **10% about access to prohibited content,** and **24% about either malware, phishing or credential theft.**

Organizations Are Vulnerable and IT Admins Must Remain Vigilant

Despite the disconnect between the security controls respondents claim to deploy, and the peace of mind they get from doing so, protecting the remote workforce takes a layered approach. And luckily, organizations and IT administrators do report using a variety of tactics to protect remote workers today.





While it is heartening to see organizations deploying multiple security solutions, it's important to continue emphasizing the fact that no single security service or program is perfect. A layered approach to information security is the most effective way to prevent cyber attacks and data breaches, especially when it comes to the remote workforce.

T. Daniels Consulting Offers Several Endpoint Security Solutions Designed to Provide User-Focused Protection, Including:

SecureDNS – a new Cloud-based security service that automatically detects and blocks phishing attacks, command-and-control callbacks and data exfiltration attempts against users outside the network perimeter. The solution offers DNS-level protection and content filtering to protect remote employees, while providing automated end-user security awareness and education designed to help prevent future security incidents – all in a simplified, cost-effective solution that's easy to deploy and manage. Find out more **here**.

SecureFactor – a Cloud-based multi-factor authentication service, T. Daniels Consulting's SecureFactor reduces the likelihood of network disruptions and data breaches resulting from stolen credentials and eliminates the complex integration processes, considerable up-front expenses, and burdensome on-premises management requirements preventing midsized enterprises from adopting traditional MFA solutions. Leveraging an innovative approach to user authentication called "Mobile Device DNA," the service distinguishes cloned and malicious login attempts from legitimate ones. Once installed on an endpoint, the SecureFactor app creates a personalized "DNA" signature for users' devices and adds them to the calculation to ensure that authentication messages not originating from a legitimate user's phone will be rejected. Find out more **here.**