Securing and Enabling Your Remote Workforce

WHITE PAPER

5 ways to keep workers productive — and data and device secure

ABSOLUTE®

As organizations adapt to — and even embrace — remote work, enabling productivity without sacrificing security is more important than ever. Here are five steps to help you along the way:

1

Ensure clear lines of communication

Reliable and secure collaboration apps are a necessary condition for effective communication. Ensure you have the right infrastructure in place, and use it with intention — so you can close loops and get projects delivered on time.

2

Keep track of your devices and their health

Remote work has only magnified the need for an up-to-date, accurate device inventory: it reduces the load on your IT team, gets devices to workers who need them, and ensures that issues don't slow down end users.

3

Retain control of every endpoint

Devices still need to be updated and remediated when they're remote, and it will take extra effort to maintain their health and security from a distance.

4

Secure sensitive data, no matter where it is

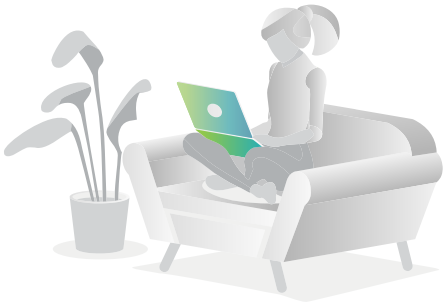
Cyber attacks and breaches are a rising threat, since remote work is straining security controls and inducing users to download sensitive data to off-network devices. Your team needs a plan to adjust to this new reality.

5

Strive for resilience, not perfection

There's no escaping it: remote work will challenge your organization's ability to remain secure and productive. Adopting a resilient mindset — and making your security resilient— will help your organization thrive in this "new normal."

1 Communicate and collaborate with clarity



In-person communication has nuances that don't translate through screens and speakers. These strategies can help your team establish clarity of communication, even if they're not in the same room.

WHAT YOU CAN DO:

Reassess the effectiveness of your collaboration apps. While you may already be using apps for communication, file sharing, and project-management, now is time to review their efficacy. Ask which problems your team faces with collaboration, and explore applications that solve them. Don't keep using the same software just because "it's what we've always used."

Take a page out of Agile development. Daily stand-up meetings can help everyone stay on the same page: each team member reports what they worked on yesterday, what they're working on today, and any blockers they need help with. This 15-minute meeting can save time as you manage shared timelines.

HOW ABSOLUTE CAN HELP:

Make sure your collaboration apps are secure. Our internal data shows that the use of instant-messaging, video-conferencing, and other collaboration apps is skyrocketing. If users are installing unauthorized apps — which increases the attack surface — Absolute lets you remotely uninstall these apps to keep devices secure.

2 Keep track of your devices and their health

When devices stay "in the wild," your usual endpoint management tools can become less effective. But an up-to-date inventory lets you stay on top of endpoint security issues and ensure that end users have a seamless work-from-home experience.

WHAT YOU CAN DO:

Follow best practices for your VPN. The VPN connects users to critical tools and data and ensures up-to-date intelligence on device health and security. Keep it as an asset — not a liability — by requiring 2-factor authentication, using strong encryption, and keeping VPN-connected devices up-to-date on antivirus and anti-malware.

HOW ABSOLUTE CAN HELP:

See all your devices, all the time. When devices don't call in, they can develop hidden vulnerabilities. Since it's firmware-embedded at the factory, Absolute's undeletable digital tether lets you reliably gather hundreds of data points per device. In addition to security and usage, Absolute collects geolocation data so you can always see where all your devices are.

Make your essential applications self-healing and resilient. The same technology that makes Absolute resilient and self-healing can extend to endpoint management tools like SCCM, Workspace ONE, Citrix Workspace, Ivanti, and Tanium modules for endpoint management, making them undeletable. You can even persist your VPN client, ensuring that it's always installed, active, and configured properly.

Survey your fleet with pre-built and customizable reports and alerts. Built-in features such as the Dark Devices report can rapidly inventory devices that haven't called in. Create your own custom reports to quickly assess devices based on any data point Absolute collects, and set alerts for when your devices become vulnerable.

3 Retain control of every endpoint

Without physical access to your helpdesk, your devices risk drifting from their desired image, reducing user productivity and creating vulnerabilities. In addition, remote work raises the possibility that devices will go missing and never return. Here's how you can address those problems.

WHAT YOU CAN DO:

Ensure patches are being applied. Up to 60% of breaches are linked to unapplied patches[1],and end users are notorious for delaying updates. Nudge your users to apply patches early and often, and follow up to ensure that your devices are getting critical security updates.

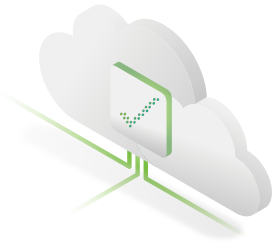
HOW ABSOLUTE CAN HELP:

Remotely manage devices as if they were in front of you. If you can do it in PowerShell or BASH, you can do it remotely with Absolute Reach, our remote query-and-remediation tool. Force updates, solve device issues, and query devices across groups and platforms, even off-network. Choose from 130+ pre-built scripts, or create your own.

Force endpoints to call in. If a device doesn't call in for a specified period of time, you can automatically freeze it with a custom message for the end user, asking them to connect to the network to regain use of their machine. So no matter what, devices will stay visible.

Define and enforce the places your devices can go. Create geofences that alert you when devices stray beyond them. Respond to perceived risk by freezing or wiping devices — even if they're off the corporate network — and call in the Absolute Investigations team to help recover devices that are missing.

4 Secure sensitive data, no matter where it is



When devices are remote, it's harder to keep security apps updated and functioning. Rather than risking a breach or compliance violation, you can use Absolute to strengthen your security posture and remotely manage your sensitive and valuable data.

WHAT YOU CAN DO:

Keep your data in the cloud. As remote work is becoming more common, sensitive data is migrating to endpoints. Establish company-wide mandates to only download when absolutely necessary, to use encryption whenever handling sensitive information, and to remove the data from endpoints afterwards.

HOW ABSOLUTE CAN HELP:

Know where all your valuable data is. When teams work remotely, sensitive data often migrates to endpoints.[2] Use the Endpoint Data Discovery tool to routinely scan endpoints for PII, PHI, PFI, IP, and more.

Respond quickly when data is compromised or vulnerable. When you discover sensitive data on an unsecured endpoint, you can freeze the device with a custom message for the end-user, or wipe some or all data from the endpoint.

5 Strive for resilience

The new paradigm of remote work is creating challenges that your team will need to rise to, and your response will define help your organization as we co-create a new reality.

WHAT YOU CAN DO:

Be proactive about cyber defense. Malicious actors aren't concerned with how secure you were last week. As the threatscape constantly changes, so should your approach to cybersecurity. Hire pentesters, probe and pressure the IT environment, and adapt when you discover weaknesses.

HOW ABSOLUTE CAN HELP:

Grant self-healing to your mission-critical apps with Application Persistence. While every security control eventually fails, those supported by Absolute can revert to their desired image. The same technology that makes Absolute self-healing and resilient can extend to these applications so they self-heal or reinstall when their functionality is compromised.

---

[1] Costs and Consequences of Gaps in Vulnerability Response, Ponemon, 2019.

[2] Impact of COVID-19 on Remote Work and Distance Learning, Absolute, 2020.

[3] **Endpoint Trends Report**, Absolute, 2019.

For more information, visit our Resource Centre for Remote Work and Distance Learning, featuring trends and insights gathered from over 8.5 million devices.

RESOURCE CENTER

To learn more about how Absolute can keep your workforce secure and productive, please contact us for a custom demo.

CONTACT US

The information in this white paper is provided for informational purposes only. The materials are general in nature; they are not offered as advice on a particular matter and should not be relied on as such. Use of this white paper does not constitute a legal contract or consulting relationship between Absolute and any person or entity. Although every reasonable effort is made to present current and accurate information, Absolute makes no guarantees of any kind. Absolute reserves the right to change the content of this white paper at any time without prior notice. Absolute is not responsible for any third party material that can be accessed through this white paper. The materials contained in this white paper are the copyrighted property of Absolute unless a separate copyright notice is placed on the material.

/ABSOLUTE®

ABOUT ABSOLUTE

Absolute serves as the industry benchmark for Endpoint Resilience, visibility and control. Embedded in over a half-billion devices, the company enables more than 12,000 customers with Self-Healing Endpoint® security, always-connected visibility into their devices, data, users, and applications – whether endpoints are on or off the corporate network – and the ultimate level of control and confidence required to support the modern enterprise. For the latest information, visit **absolute.com** and follow us on **LinkedIn** or **Twitter**.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com

© 2020 Absolute Software Corporation. All rights reserved. ABSOLUTE, the ABSOLUTE logo, SELF-HEALING ENDPOINT, and PERSISTENCE are registered trademarks of Absolute Software Corporation. Other names or logos mentioned herein may be the trademarks of Absolute or their respective owners. ABT-Securing-and-Enabling-Your-Remote-Workforce-WP-E-070620.