



EBOOK

# Combating the Surge of Modern Malware and Ransomware





## TABLE OF CONTENTS

State of Cybercrime .....	3
Cyberattack Drivers .....	4
Impact of Cybercrime .....	5
Cyberattack Origins .....	6
Zero Trust .....	7
Protecting Your Data .....	8
Conclusion .....	9
About A10 Networks .....	10



## THE POST-PANDEMIC STATE OF CYBERCRIME

Cyberattacks have soared over the past year. Even before the outbreak of the COVID-19 pandemic, cybercrime tactics and technologies were growing rapidly in sophistication, driving a rate of nearly 1,300 incidents per day in the US alone in 2019. Now the numbers are spiking even further, with 80 percent of firms seeing an increase in 2020 in incidents from **DDoS attacks**, **ransomware**, and data breaches to phishing attacks. The COVID-19 pandemic was blamed for a **238 percent rise in cyberattacks on banks**, while phishing has jumped 600 percent since the end of February 2020.

This eBook will explore the reasons these attacks have increased so dramatically, and more importantly, how to build a strategy to protect your data and networks against these attacks.

We'll look at four key areas:

1. What is driving these cyberattacks?
2. What is the impact of cybercrime?
3. Where are cyber criminals hiding?
4. Why you need to implement a Zero Trust strategy now?



*Read on to learn about what's going on with cybercrime in the new normal, and what you can do about it.*



**1,300**  
INCIDENTS PER DAY  
in the US alone in 2019



**80%** OF  
FIRMS  
are seeing an increase in  
cyberattacks since 2020



PHISHING  
HAS JUMPED  
**600%**  
since the end of  
February 2020





## WHAT IS DRIVING THESE CYBERATTACKS?

As the pandemic took hold, society went through a sudden and often haphazard shift to doing everything online. Offices closed and employees began working from home, while schools and universities began giving classes online. Even healthcare moved from in-person to remote appointments, with a rapid rise in telehealth consultations. For all kinds of people, with all kinds of organizations, remote access to resources became a mainstay of daily life.

### The sudden and unplanned shift to remote work created opportunities for cyber criminals

Given the unexpected and rushed nature, as well as the unprecedented scale of this shift, attackers knew there would be ample loopholes available to exploit. Many organizations were unprepared for the abrupt increase in cloud utilization necessitated by shifting demands, leaving security gaps. Home-based workers relying on consumer broadband and personal devices destroyed any notion of a secure perimeter, while best practices for password hygiene, safe browsing, phishing awareness, and other critical measures were often forgotten. An information-hungry public confused by misinformation, especially around COVID-19 provided easy targets for phishing attacks.

Taken together, the links between the pandemic and the rise in cybercrime are clear. Consider just a few **statistics from 2020**:

- Attacks targeting home workers rose fivefold in six weeks following the lockdown
- Cloud-based attacks rose 630 percent between January and April 2020
- Apple accounted for 10 percent of branded phishing attempts in Q1 2020
- 394,000 unique IP addresses attacked UK firms in Q1 2020
- Visits to hacker websites and forums rose 66 percent in March 2020

**The pandemic was a boom time for cybercriminals, and they made the most of their opportunity.**



**630%**  
CLOUD-BASED  
ATTACKS ROSE  
between January  
and April 2020



**394K**  
UNIQUE IP  
ADDRESSES ATTACKED  
UK firms in Q1 2020



**66%**  
INCREASE IN VISITS  
TO HACKER WEBSITES  
and forums in March 2020





## WHAT IS THE IMPACT OF CYBERCRIME?

The **May 2021 ransomware strike** that shut down the Colonial pipeline, a critical fuel pipeline in the Eastern US, drew attention for its scale and impact, but it was hardly an outlier. Ransomware attacks rose 148 percent in March 2020 alone, while the average ransomware payment rose by **33 percent to \$111,605** compared with Q4 2019. By Q3 2020, the average payment had reached **\$170,000**.



*It's estimated that a ransomware attack will strike every 11 seconds by the end of 2021.*

### Why has this been this happening?

Before 2020, these attacks largely followed a predictable pattern: hackers encrypt your data, demand a ransom, and then either decrypt your data or not. Either way, your data stayed in some form on your own servers, within your own organization. However, attackers are increasingly using ransomware attacks for data theft, eventually offering the stolen data for sale on the black market. Whether the target is a **municipality, a corporation, a healthcare system**, or a **university**, the impact of ransomware can be devastating. In some cases, it can even be **lethal**.

### The direct financial costs of cybercrime are only part of the picture

A recent report by McAfee found that, taking into account hidden costs such as system downtime, reduced efficiency, incidence response costs, and brand and reputation damage, cybercrime costs the world economy **more than \$1 trillion**, or just more than one percent of global GDP—up more than 50 percent since 2018. Perhaps just as alarming, 56 percent of surveyed organizations in the report said they do not have a plan to both prevent and respond to a cyber incident.



RANSOMWARE  
ATTACKS ROSE

**148%**

in March 2020 alone



CYBERCRIME COSTS  
THE WORLD ECONOMY  
MORE THAN

**\$1 Trillion**

or just more than  
1% of the global GDP





## WHERE ARE CYBER CRIMINALS HIDING?

In the old days, cybersecurity models focused on the idea of hardening the perimeter against external threats. Over time, this notion has proven to be less and less relevant to reality. For one thing, more open computing architectures and a more mobile, distributed enterprise workforce have rendered the idea of a network perimeter increasingly obsolete. Just as significantly, it is shortsighted to assume that every attack will originate from an outside party. In fact, trusted insiders—people with legitimate access to your network—can also be a threat to your security, even if they do not always realize it.

### Who is an internal threat actor?

Internal threat actors can generally be grouped into two types. The first include disgruntled employees, corporate spies, or impostors with a conscious intent to abuse your resources or cause harm to your organization. But often, internal threat actors fit a second, less obvious description: well-meaning employees who inadvertently enable an attack through simple carelessness or lack of awareness. Their impact can be just as damaging, as seen in recent waves of ransomware attacks in which phishing emails tricked employees of **several small city governments in Florida** into triggering an infection. In one case, the accidental inside threat actor led to a \$600,000 payment to cybercriminals.



# \$600,000

*was the amount an accidental threat actor tricked a Florida police department to pay cybercriminals.*

### The pandemic strengthened the resolve of attackers

The pandemic made phishing attacks easier to carry out. In many cases, employees working from the comfort of their homes were relatively relaxed about data security in general, and online security in particular. In this context, phishing attacks as simple as a fraudulent text link or email with a coronavirus-related header would be enough for employees to throw caution to the wind.

### Once malware is activated, traditional security fails

Whether the cyberattack is initiated from the outside or within, once the threat actor downloads and activates a malware, or ransomware, it can start spreading laterally within the network. This spread cannot be detected or stopped with the traditional “secure perimeter” approach as there’s no way to check the spread within the network.

Add to this the fact that most of these malwares and ransomwares are increasingly using encrypted channels for communications with their C&C servers, and within the network itself, it is almost impossible for traditional security to detect and stop cyberattacks.

That is why organizations need to start looking into ways through which they can, not only tie all of their security solutions together, but make sure they know what’s going on within their networks, at all times.



## WHY YOU NEED TO IMPLEMENT A ZERO TRUST STRATEGY **NOW**

The prevalence of insider threat actors—intentional or not—combined with the evolution of more distributed and porous technology environments has helped drive the rise of Zero Trust as a core principle of modern cybersecurity. As the name suggests, **Zero Trust** asks us not to trust anything or anyone—inside or outside the network.

### Core concepts of Zero Trust

The first step with Zero Trust is to move away from the idea of inside versus outside, protected or trusted zone versus the (untrusted) internet. Instead, cyberdefense is redesigned in terms of secure micro-perimeters, with multiple points of network defense distributed throughout the network to be able to control, inspect, and restrict traffic going in and out of the network, or east-west within your organization's network.

Users must be subjected to checks and balances each time they cross into a different domain or try to access a new set of resources to verify that they have a legitimate need as well as the appropriate privileges. That's why limiting excessive privileges is another key tenet of the Zero Trust model.

Access and credentials must be revoked and refreshed periodically to prevent excess privilege from accumulating over time. Visibility is crucial for monitoring who's accessing what, who has access to what, and the level of risk these activities might present.

**In essence, Zero Trust is the ultimate recognition of the nature of today's cyber threats:** an attack can come from anywhere, with the help of anyone, in any form. That realism makes it the **definitive strategy for modern network defense**.



## ZERO TRUST

Is the a core principle of modern cybersecurity. It asks us not to trust anything or anyone—inside or outside the network—with access to our networks and computer systems













## HOW DO YOU PROTECT YOUR DATA MOVING FORWARD?

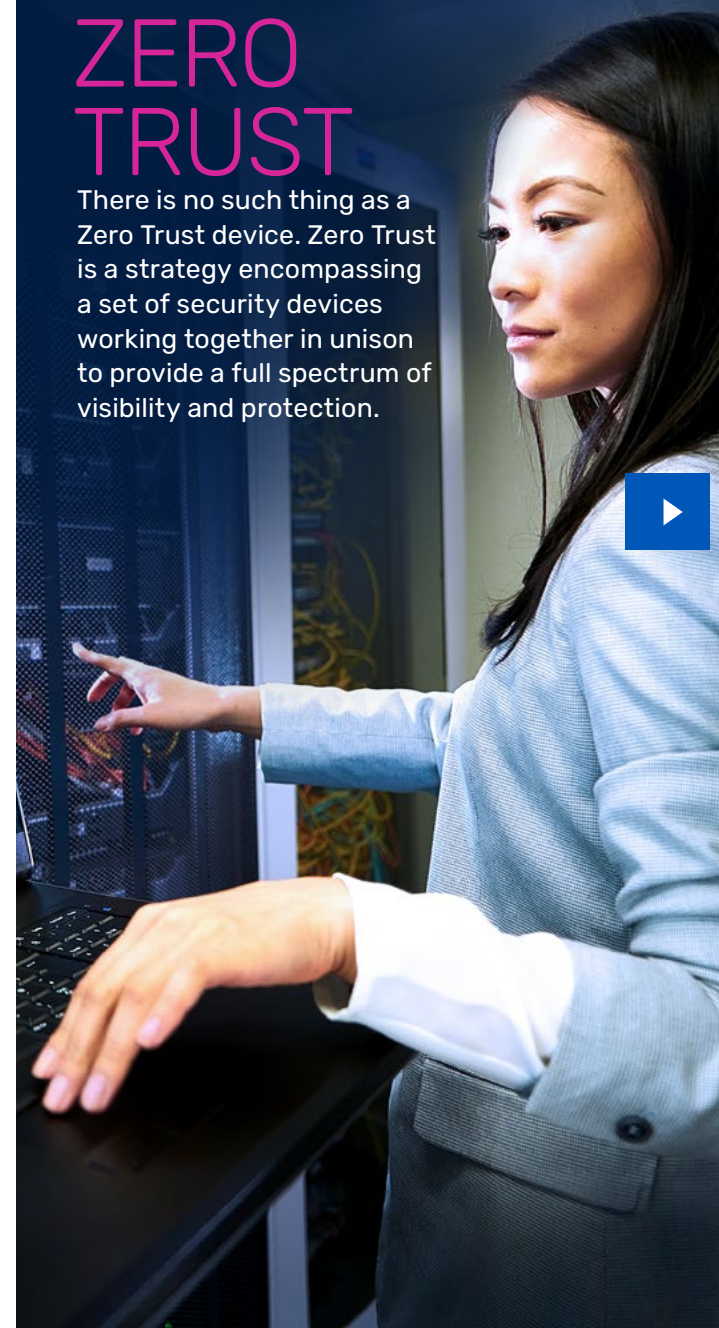
Nobody wants to be the company named in the latest high-profile cyberattack. To avoid making news for the wrong reasons, it is essential to act now to strengthen security. That means implement the solutions needed to enable a comprehensive Zero Trust strategy. With that in mind, here are a few essential elements of a full Zero Trust deployment.

-  **Enable full, centralized visibility** into your traffic (encrypted or otherwise), user activity, data, and workloads, because you can't protect yourself against attacks you can not see.
-  **Provide centralized management** capabilities for uniform security and policy control across multiple deployments.
-  **Implement micro-segmentation** within your networks to perform layered security checks and restrict lateral movement of suspicious traffic.
-  **Enable strict user access control** to track and restrict unwanted data access.
-  **Leverage intelligent automation** to minimize incident response times and maximize operational efficiency.
-  **Provide granular traffic control and detailed audit trails** to make sure compliance and data privacy standards are met.

In addition, it is essential that every network and security solution is easy to use and that each solution should integrate seamlessly into the existing infrastructure. Every solution should also employ fault-tolerance and redundancy mechanisms so that the entire security infrastructure can be resilient and utilized to its fullest potential.

## ABOUT ZERO TRUST

There is no such thing as a Zero Trust device. Zero Trust is a strategy encompassing a set of security devices working together in unison to provide a full spectrum of visibility and protection.







## CONCLUSION

The “new normal” of cybersecurity can seem like a dangerous place—and it is—but that doesn’t have to strike fear into your organization. By taking a proactive approach to security with an effective Zero Trust implementation, you can detect and respond to threats more quickly, wherever they originate and whatever form they take, mitigating the risk and damage while holding those who are responsible, accountable.

If you want to discuss your business needs, technology strategy, and application delivery requirements, A10 Networks has extensive experience helping organizations of all kinds achieve their digital transformation and resiliency goals.

[Contact us](#) any time or request a [free demo](#).



Read the latest white paper:  
**Zero Trust is Incomplete  
without TLS Decryption**

[Read Now](#)



Watch our latest On Demand webinar:  
**Zero Trust and the New Normal  
for Cybersecurity**

[Request a Demo](#)

## ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit [A10networks.com](https://a10networks.com) and follow us [@A10Networks](https://twitter.com/A10Networks).

Learn More  
About A10 Networks

Contact Us  
[A10networks.com/contact](https://a10networks.com/contact)

©2021 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder, Lightning, Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: [www.a10networks.com/a10-trademarks](https://www.a10networks.com/a10-trademarks).

Part Number: A10-EB-14145-EN-01 JUNE 2021