



WHITE PAPER

One click can trigger an attack – architecture stops it.

Phishing links and malicious files rely on user interaction. Modern security architecture determines whether that action leads to execution or is stopped before damage occurs.

The Risk Behind a Simple Action

Employees open emails, download files, and click links every day. These are normal and necessary actions in modern business environments. They are also one of the most common ways attackers gain access.

User-assisted execution occurs when a user unknowingly triggers malicious activity by opening a file, clicking a

link, or running an application. Unlike attacks that rely on exploiting vulnerabilities or stealing credentials, these attacks depend on a single moment of interaction.

That moment happens constantly. The question is not whether users will click, but what happens when they do.

Anatomy of a User-Initiated Breach

A recent ransomware campaign targeting organizations across multiple industries illustrates how user-assisted execution can quickly escalate into major disruption.

Attackers distributed phishing emails containing malicious attachments and links designed to appear legitimate. When users interacted with the content, malware executed inside the environment and established an initial foothold.

From there, attackers moved quickly. Systems were encrypted, data was exfiltrated, and operations were disrupted across organizations in healthcare, education, manufacturing, and professional services.

The financial impact was significant. Ransom demands ranged from approximately \$100,000 to \$15 million depending on the size and nature of the organization. In many cases, organizations also faced the additional threat of sensitive data being publicly exposed if ransom demands were not met.

This type of attack does not depend on exploiting software vulnerabilities. It begins with a single action.

What Is User-Assisted Execution?

User-assisted execution refers to attacks where malicious code is activated through user interaction.

This typically happens through phishing emails containing malicious links or attachments, infected documents that execute code when opened, or downloads disguised as legitimate files. For example, a user may receive an email

with an invoice attachment that appears normal, but opening it triggers hidden code that installs malware or initiates a connection to an attacker-controlled system.

In many cases, the user does not see anything unusual. Execution happens silently, which is what makes these attacks so effective.

When Execution Leads to Catastrophic Impact

User-assisted execution is not limited to phishing campaigns. Some of the most disruptive cyber incidents in recent years have followed a similar pattern.

In one widely known case, malicious code entered a global organization through what appeared to be a legitimate software update. Once executed inside the environment, the malware spread rapidly and brought down systems across the global network. Operations were halted, critical infrastructure was disrupted, and the estimated financial impact exceeded \$300 million.

In another case, malware execution led to widespread disruption of manufacturing systems in a major pharmaceutical organization. Production was impacted, operations were halted, and losses exceeded \$1 billion.

These incidents reinforce a critical point. Execution is often the trigger, but architecture determines the scale of the impact.

Why Traditional Defenses Are Not Enough

User-assisted execution is not limited to phishing campaigns. Many organizations rely on user awareness training and email filtering to prevent these attacks. While these controls are important, they are not sufficient on their own.

Users will open files, click links, and interact with content that appears legitimate. Attackers understand this and design their techniques accordingly. Malicious files may not contain macros, links may pass through trusted services, and documents may exploit legitimate features instead of obvious vulnerabilities.

In fact, nearly half of malicious Office documents are delivered through phishing, and the vast majority involve common file types such as Word and Excel. These attacks are specifically designed to bypass traditional defenses.

When execution occurs, many environments lack the controls needed to prevent escalation.

Protecting Against Modern File and Link-Based Attacks

One of the most important advancements in modern security is the ability to inspect and control content before it reaches the user. This is critical because many modern attacks are designed to appear legitimate and evade traditional detection methods.

Effective protection includes blocking access to known malicious or suspicious websites, inspecting links in real time to identify phishing destinations, analyzing files before download to detect hidden threats, and controlling file delivery to prevent execution of malicious content.

These capabilities help stop attacks earlier in the chain, before user interaction leads to execution. They also provide a critical layer of defense against evolving threats, including macro-less attacks and files that exploit legitimate application features.

The Architectural Shift: Prevent and Contain

Modern security architectures take a different approach. Instead of relying solely on prevention, they assume that some level of user interaction will occur. The goal becomes both preventing execution where possible and limiting the impact when it happens.

This approach, commonly associated with Zero Trust access, introduces several important controls. These include blocking malicious links, inspecting files before they reach the user, verifying identity and device trust, and limiting access to only the applications users are authorized to use.

Together, these controls reduce both the likelihood of execution and the potential impact if it occurs. A single action should not expose an entire organization.

A Practical Approach for Modern Businesses

Implementing these controls has historically been complex. Many organizations have relied on multiple tools to address different parts of the problem. Modern cloud-delivered platforms simplify this approach.

SonicWall Cloud Secure Edge (CSE) provides integrated protection against both malicious links and file-based threats, combined with Zero Trust access controls.

CSE blocks access to malicious websites and phishing links, inspects and controls file downloads before they reach the user, and helps identify and stop malicious files even when they appear legitimate. It also verifies user identity, device trust, and contextual signals

before granting access and connects users only to the applications they are authorized to access.

Even if a user interacts with malicious content, these controls help prevent attackers from gaining meaningful access or moving laterally within the environment.

Because it is delivered from the cloud, CSE provides these protections without adding operational complexity.

The Business Case for Proactive Security

User-assisted attacks often begin with a single action, but their impact is rarely limited to that moment. For many organizations, the challenge is not understanding the risk. It is underestimating how quickly that risk turns into disruption.

Reactive security is unpredictable. It introduces unplanned downtime, emergency response costs, and business interruption that can affect revenue, operations, and customer trust. Proactive security is different. It is planned, controlled, and aligned with how the business operates.

By investing in modern access and threat protection, organizations can reduce risk before it becomes disruption and avoid the cascading impact of a single user action. The decision is not whether to invest in security. It is whether to invest before or after an incident.

Final Thought

User-assisted execution is one of the most common ways attacks begin, and one of the hardest to eliminate entirely. Users will click, files will be opened, and links will be followed.

Modern security architecture recognizes this reality. By preventing malicious content where possible and limiting the impact when execution occurs, organizations can significantly reduce the likelihood that a single action becomes a major breach.

Security is not about expecting perfect behavior. It is about building systems that remain secure even when behavior is not.

Learn how simple it can be to [implement Zero Trust access](#) in your organization.

To explore how modern Zero Trust access and Internet Threat Protection protect your organization from today's most common attack paths, visit our [Before the Breach: A Proactive Security Guide page](#).

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035 | [Refer to our website for additional information.](#)

© 2026 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

Whitepaper_CSE_User_Assisted_Exploitation_12224