



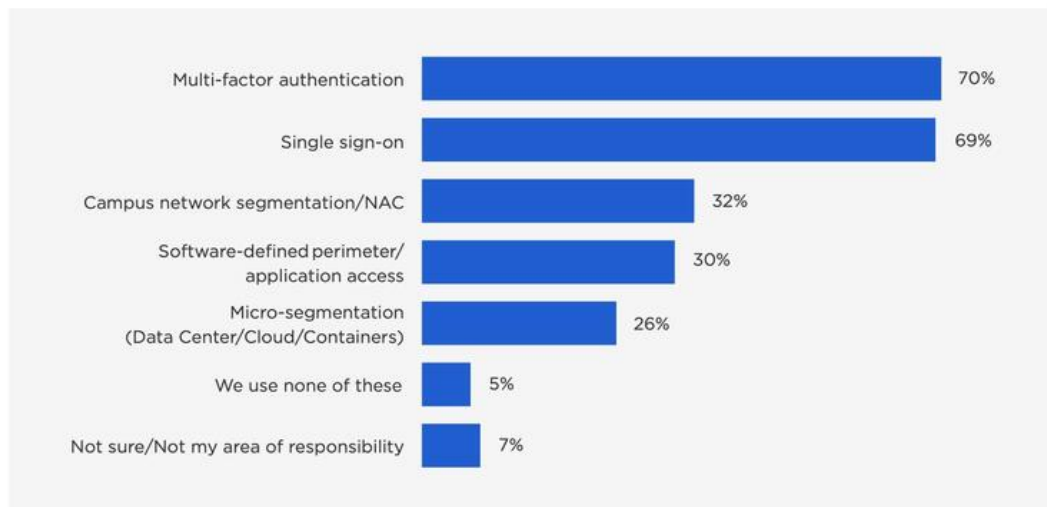
Security Newsletter

17 August 2020

[Subscribe to this newsletter](#)

NIST Issues Final Guidance on 'Zero Trust' Architecture

WHAT ZERO TRUST TECHNOLOGIES DO YOU USE TODAY?



NIST Special Publication 800-207 is designed to help CISOs, security professionals and network administrators gain a better understanding of the zero trust concept. By adopting a zero trust strategy, organizations can help prevent data breaches and limit attackers' lateral movement, the NIST guidance states.

"Perimeter-based network security has also been shown to be insufficient, since once attackers breach the perimeter, further lateral movement is unhindered," the guidance notes.

The publication states that any organization in the private sector or the government can adopt the zero trust guidelines. In fact, most organizations already have some elements of zero trust in their enterprise infrastructure, NIST notes. But enterprises that are geographically dispersed or have a large mobile workforce are more likely to benefit from deploying the latest zero trust guidance. These include enterprises with satellite facilities, those using multi-cloud or cloud-to-cloud approaches, organizations that rely on contracted services and enterprises with public- or customer-facing services.

[Read More on BankInfoSecurity](#)

[Zero Trust is critical, but very underused \(TechRepublic\)](#)

More #News

- [Security in the 'new normal': Passwordless is the way forward](#)
- [Flaws in Samsung Phones Exposed Android Users to Remote Attacks](#)
- [Microsoft Reveals New Innocent Ways Windows Users Can Get Hacked](#)
- [DEF CON: New tool brings back 'domain fronting' as 'domain hiding'](#)
- [China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI](#)
- [Google Chrome Bug Could Let Hackers Bypass CSP Protection; Update Web Browsers](#)
- [SANS infosec training org suffers data breach after phishing attack](#)
- [Your digital security is as strong as your weakest recovery email](#)
- [Signal adds message requests to stop spam and protect user privacy](#)
- [Amazon Alexa Bugs Allowed Hackers to Install Malicious Skills Remotely](#)
- [New Attack Lets Hackers Decrypt VoLTE Encryption to Spy on Phone Calls](#)

#Patch Time!

- [Microsoft August 2020 Patch Tuesday fixes 120 vulnerabilities, two zero-days](#)
- [Adobe fixes critical code execution bugs in Acrobat and Reader](#)
- [TeamViewer fixes bug that lets attackers access your PC](#)
- [Critical Flaws Affect Citrix Endpoint Management \(XenMobile Servers\)](#)
- [SAP updates security note for critical RECON vulnerability](#)
- [A New vBulletin 0-Day RCE Vulnerability and Exploit Disclosed Publicly](#)
- [Citrix fixes critical bugs allowing takeover of XenMobile Servers](#)
- [Microsoft's Patch for LSASS Flaw Incomplete, Google Researcher Says](#)
- [Potentially Serious Vulnerability Found in Popular WYSIWYG Editor TinyMCE](#)

#Tech and #Tools

- [Pysa: An open source static analysis tool to detect and prevent security issues in Python code](#)
- [Process Spawn Control: Powershell tool for behavioral analysis of malware.](#)
- [Intel Owl: Open source threat intelligence solution](#)
- [How Malicious Tor Relays are Exploiting Users in 2020](#)
- [A Change of Mythic Proportions: Apfell C2 update](#)
- [Splunk Vulnerability Scanner plugin](#)
- [SNlcat: Circumventing the guardians](#)
- [Exploiting vBulletin: "A Tale of a Patch Fail"](#)
- [PIN Bypass in Passwordless WebAuthn](#)
- [Exposing and Circumventing China's Censorship of ESNI](#)
- [Defending Your Malware](#)
- [Security best practices for Windows Server Update Services \(WSUS\)](#)
- [SysmonTools: Sysmon utility toolbox](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>