Securing Justice in the Digital Age

How Zero Trust Protects Court Systems from Cyber Threats

SOLUTION BRIEF

Court systems are attractive targets for cyberattacks. Judicial systems house incredible amounts of data related to every facet of our lives. Over the past two years, at least eight states reported their court and related systems were forced offline due to ransomware attacks. The security of software across the interconnected criminal justice ecosystem also has an impact on court security as evidenced by the recent attack on PACER that may have compromised the identities of confidential informants involved in criminal cases at multiple federal district courts. The bedrock foundations of the judiciary, having the public's trust and confidence, are at risk when these attacks are successful.

With the digitization of court records and processes growing within this threat landscape, now is the time for courts to re-evaluate how they approach cybersecurity. Traditionally, judiciary agencies operate within a framework built on the principles of trust—trusted systems, networks, and users. In today's reality of remote work, data sharing with external partners, and cloud-based software, this traditional perimeter-based model creates vulnerabilities. By granting wide access to trusted users, the door is open for exploitation by bad actors. It is time to fully commit to a zero trust security architecture and the transition may be easier than you think.

What is zero trust?

Zero trust is a security approach that assumes no one—inside or outside an organization—should automatically be trusted. Instead, it verifies everyone's identity and checks that they have permission before giving them access to anything, every time they try. It's like locking every door in a building and checking ID each time someone wants to enter a room, even if they work there.

This verification is automated with little impact on the end user, in fact it may speed access to needed applications and systems. Imagine your daily commute. You start at your kitchen table, you get in your car, you drive a series of roads, you park, walk into the building, and finally arrive at your desk. Each step of that process has risks — people can see you, you can get into an accident. With a zero trust architecture you are sitting at your kitchen table, you blink and you are at your desk. Your path to work was not visible to anyone on the outside and you got precisely where you needed to be without having to ensure your security along the way.

Many courts have been implementing pockets of zero trust to enable remote work. Now is the time to expand the use of zero trust principles across enterprises to secure the data our courts hold and the trust they work to earn.

BENEFITS OF ZERO TRUST

- **Increased visibility into devices and connections**
  Courts often struggle with managing sprawling networks, encompassing thousands of devices and users and connecting to multiple related judiciary agencies. A zero trust architecture provides visibility to see every connection on your network to help you easily create policies.

- **Improved performance for remote users**
  Zero trust principles allow for the retirement of VPNs improving both security and performance for users.

- **Robust data loss prevention safeguards**
  With data privacy and access controls built into zero trust architectures, the highly sensitive data held by courts stays within court systems.

- **Continuous monitoring to spot anomalies before they become issues**
  The continual validation of users means that vulnerabilities are immediately detected and fixed before they can be exploited. No longer do you have to wait for a vulnerability scan to show an issue then put in the ticket for it to get fixed only to find on the next scan the fix did not work.

- **Cost containment**
  By identifying vulnerabilities as they impact the system, IT teams can get the most out of the security tools they have in place. Instead of rushing into response mode, teams can utilize all of the alerting and repair functionalities built into existing tool sets.

- **Regulatory compliance**
  Zero trust solutions include advanced security controls, encryption and monitoring required by Criminal Justice Information services (CJIS), FedRAMP, and other federal and state regulations.

- **Stop lateral movement**
  With so many external parties including police, legal providers, jails, and more connecting to court systems, zero trust ensures that any malicious inbound activity is stopped before moving throughout the network.

- **Secure public-facing platforms**
  Many courts provide online services, such as filing petitions, paying fines, or requesting case updates. Zero trust architecture protects these applications from threats like DDoS attacks, ensuring uninterrupted digital access for citizens.

- **Enable secure use of Generative AI**
  Regardless of policies against GenAI use, users are going to utilize tools. With a zero trust architecture, courts can lock down the removal of files as well as copying and pasting of data into non-approved AI models.

Zero Trust for Remote Access and Beyond

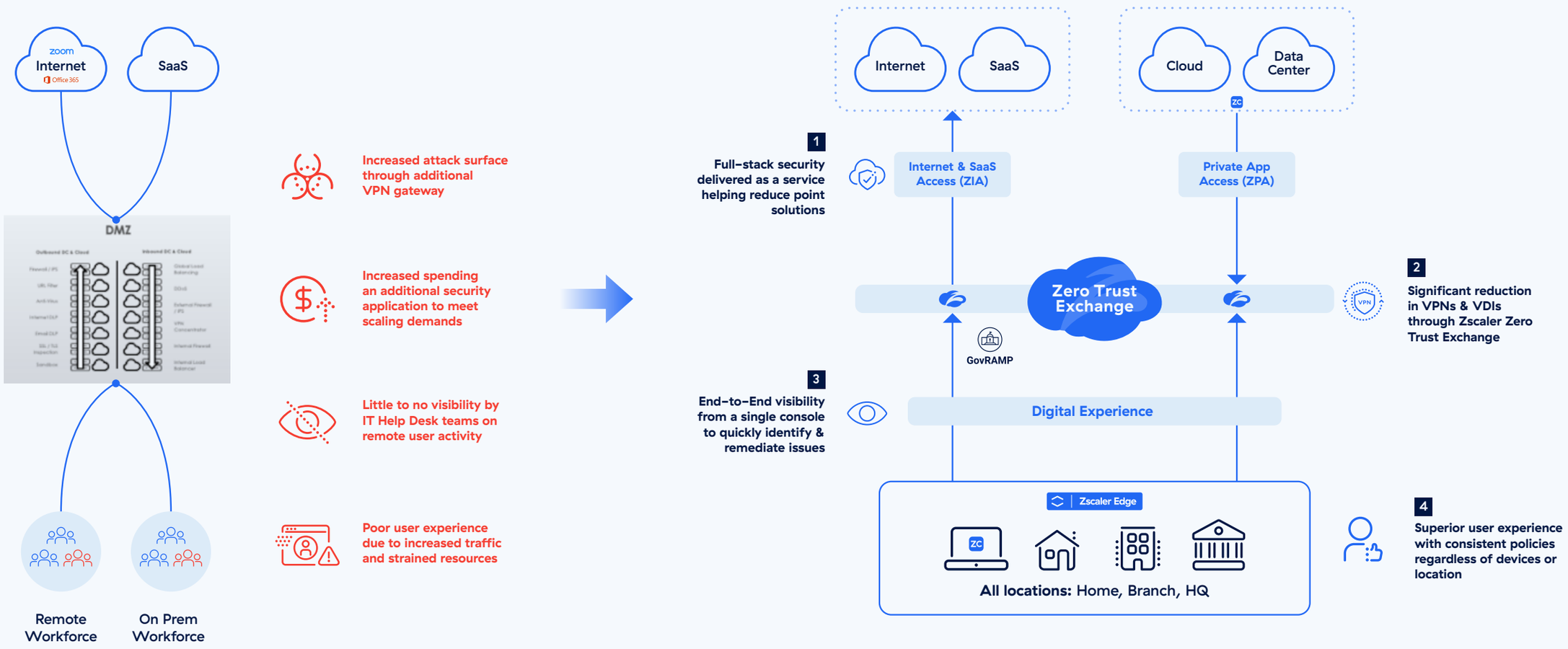
The New Jersey Judiciary (NJJ), encompasses the New Jersey Supreme Court, 21 county courts, and 535 municipal and other courts. NJJ initially implemented Zscaler to enable its 10,000 employees to work securely from anywhere and increase the number of virtual courtrooms from 40 to 400 to respond to COVID-19 pandemic social distancing measures. However, the benefits quickly expanded beyond remote work.

EXPANDING SCOPE FROM CASB TO ZERO TRUST

As part of its digital transformation initiative, NJJ was looking for a Cloud Access Security Broker (CASB) solution to secure infrastructure and prevent shadow IT as the court system began migrating applications to the cloud. Instead, the team was advised to consider a zero trust approach.

New Jersey Courts

A zero trust model was very new to us, but it made perfect sense because you assign privileges to devices and users and only allow access to the applications they need," said Ron Wildmann, NJJ assistant director of Infrastructure and Technical Services. "Zero trust allows us to remove all that implied trust [in legacy architectures] and forces us to architect our security so that we can only explicitly trust the things we want accessing our applications.



Benefits

Estimated $10.7M in reduction of technology costs

Increased number of virtual courtrooms from 40 to 400

Full support of 10,000 employees and 140,000 users

Consolidation of multiple point solution for ease of management

IMPROVED USER EXPERIENCE

With the onset of the pandemic, NJJ was forced to expand its VPN usage from 2,300 users to 8,000, which dramatically degraded user experience and increased VPN-related security risk. Switching from VPNs to the Zero Trust Exchange and Zscaler Private Access (ZPA) for remote access provided a much better user experience with additional layers of security. This led to further expansion of ZPA to every user whether on-premises or off. Now users have a consistent experience across its dynamic, hybrid work environment.

MORE INFORMED IT SUPPORT

After most workers were sent home, the NJJ help desk team found itself spending hours trying to diagnose connectivity issues—difficulty connecting, frequent disconnects, or blurry video conference images. The organization took advantage of the Zscaler Digital Experience™ (ZDX™) user experience monitoring service.

"With ZDX, we can say the problem is in your home or in our network or our data center," said New Jersey Judiciary CIO Jack McCarthy. "We can quickly get to the root of the problem instead of trying to troubleshoot for hours and hours and hours."

Implementing the Zero Trust Exchange dramatically boosted the court system's security posture, improved user experience and productivity, and increased agility in multiple ways. As a result, zero trust has become essential to NJJ's strategic roadmap moving forward.

Building Trust with Zero Trust

As courts continue to digitize their operations, the importance of zero trust will only grow. By removing implicit trust that users and workloads have when on a network, courts can improve both their security posture and operational functionality, building trust in the functions and outputs of their agencies.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere