The role of authentication in **data protection**

Agencies are shifting from defending a network perimeter to making risk-based decisions about access

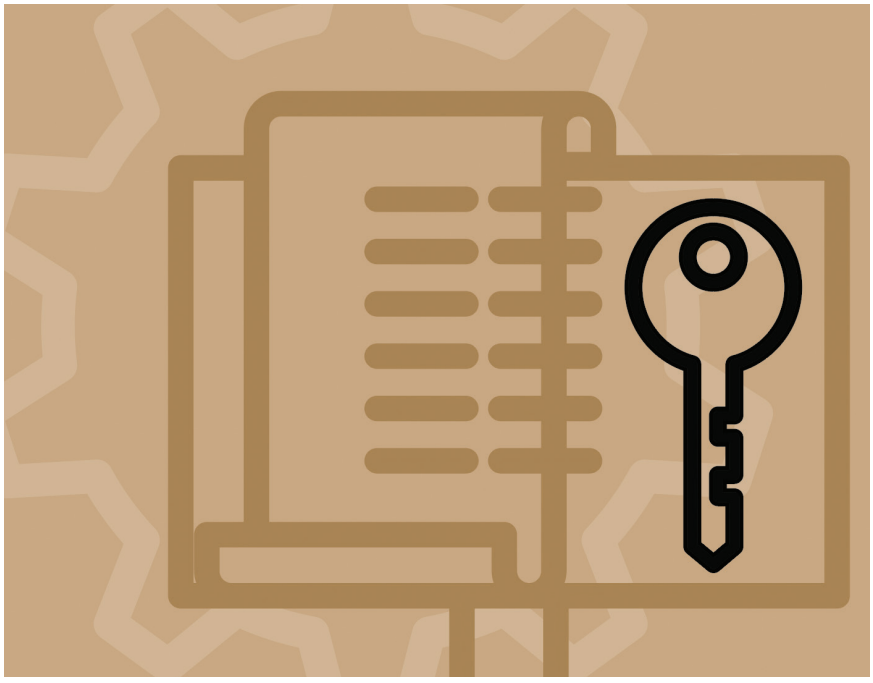
Bill Becker
Vice President of Product Management, Thales TCT

THE ONGOING PUSH TO THE CLOUD and the rise in remote work are making the security landscape less clear for IT administrators. In the 2021 Thales Data Threat Report, 82% of security professionals said they are concerned about the risks associated with remote work. As more employees work from home and other locations, they are logging into government networks via a VPN or accessing cloud-based applications directly while using a variety of devices that may or may not be secure.

Employees are no longer in the office on a regular basis, and neither is their data or their applications. In response, many agencies are moving toward holistic data protection through models such as zero trust so they can make risk-based decisions about who should have access to data and other government resources.

Seamless, secure user authentication

Users who need to access low-risk applications and data — for example, publicly available product information — can use an authentication method such as one-time password tokens. But if that same user wants to access higher-value data such as corporate finance records, the required level of authentication should increase, perhaps requiring public-key infrastructure (PKI) authentication with a smartcard. The key is to manage those activities via one pane of glass or one platform that supports the entire risk-based and continuous authentication process.



In the past, we've been able to base decisions on where users are located — for example, whether they're accessing data from within the network or remotely via VPN — but that is no longer enough. New technology tools enable agencies to gain a deeper understanding of users' online behavior so they can make more informed decisions about authentication.

In addition, there has been an increase in so-called non-person entities — for example, robotic process automation, or bots. Some adversaries will try to compromise a digital, rather than a human, user. When humans aren't involved in a process, agencies still need to make sure that applications are controlled and authenticated at the same security level before they access sensitive data. So, for example, instead of a human user inserting a smartcard into a computer, an agency using bots could meet the same public-key authentication requirements with a network-hosted PKI credential.

Complying with government mandates

Industry consortiums and government leaders have issued many guidelines and policies to help agencies strengthen their ability to secure complex IT environments. For example, Federal Information

Shutterstock/FCW Staff

> New technology tools enable agencies to gain a deeper understanding of users' online behavior so **they can make more informed decisions about authentication.**

Processing Standard (FIPS) 140 defines a secure, proven method for developing cryptographic modules such as those used for authenticating a digital or a human user.

Furthermore, the recent executive order on cybersecurity mandates encryption for data in transit and at rest, multifactor authentication, zero trust architecture and supply chain security. To help with compliance, the National Institute of Standards and Technology (NIST) has developed well-defined frameworks for zero trust and other cybersecurity standards. In addition, the Defense Department's Cybersecurity Maturity Model Certification (CMMC) dovetails with some of NIST's data protection strategies.

Companies are working with agencies to develop tools and techniques for continuously monitoring data protection under government policies. The cybersecurity controls embedded in models like CMMC are also uncovering shadow IT — those applications and devices that are typically hidden from IT administrators — and making sure security protocols are applied to everything that touches the network.

Complying with government mandates and policies is essential for helping agencies discover the resources they need to protect, protecting the data itself and also controlling access to the data. ■

Bill Becker is vice president of product management at Thales TCT.