TLS AUTOMATION MATURITY ASSESSMENT RESULTS

An assessment of your organization's current automation maturity, risk level and opportunities for improvement.

digicert®

WHAT ISN'T AUTOMATED, WILL MAKE YOU VULNERABLE

Uncover modern, best practices to managing TLS certificates.

IT leaders today are looking for more efficient and agile ways to protect organizations' digital security, as they spend more time than ever before managing increasing numbers of TLS certificates and responding to risks. As a result, many IT professionals are turning to TLS automation solutions to better oversee their complex workloads.

The automation imperative

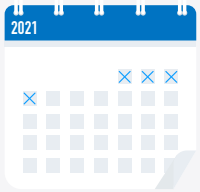
Digital security experts agree that TLS automation is the most proven way organizations can better prepare for future vulnerabilities. One major reason is because automation helps simplify convoluted certificate management tasks. With tools like the discovery feature in DigiCert CertCentral®, companies can automatically track and identify every certificate inside and outside their networks.

In addition, automating the entire lifecycle of TLS certificates allows organizations to preserve their security postures by avoiding outages from unexpected lapsed or expired certificates. Furthermore, companies with automated certificate lifecycle management are ready to adapt quickly to widespread industry, or Certificate Authority (CA), compliance events requiring quick certificate replacements and timely re-issuing of certificates, or even a post-quantum cryptography future. For these reasons and more, companies need agile and efficient processes in place to maintain their digital security.

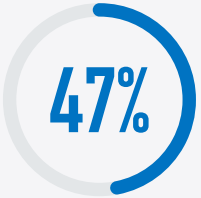
Where does your security rank?

The DigiCert TLS Automation Maturity Assessment was designed to help assess your organization's current use of TLS certificate discovery and automation tools and identify areas to improve your security posture. This assessment will help guide you on deciding which deployment model would best fit your organization. We've got solutions for large, mid-size and small businesses with a wide number and range of certificates. Because every organization is unique, we believe the best automation solution for your organization is the one that best serves your IT needs and resources.

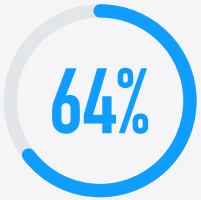
DIGITAL SECURITY BY THE NUMBERS



1-4 total days spent per month managing certificates



47% avg. amount of overall time IT professionals spend managing certificates

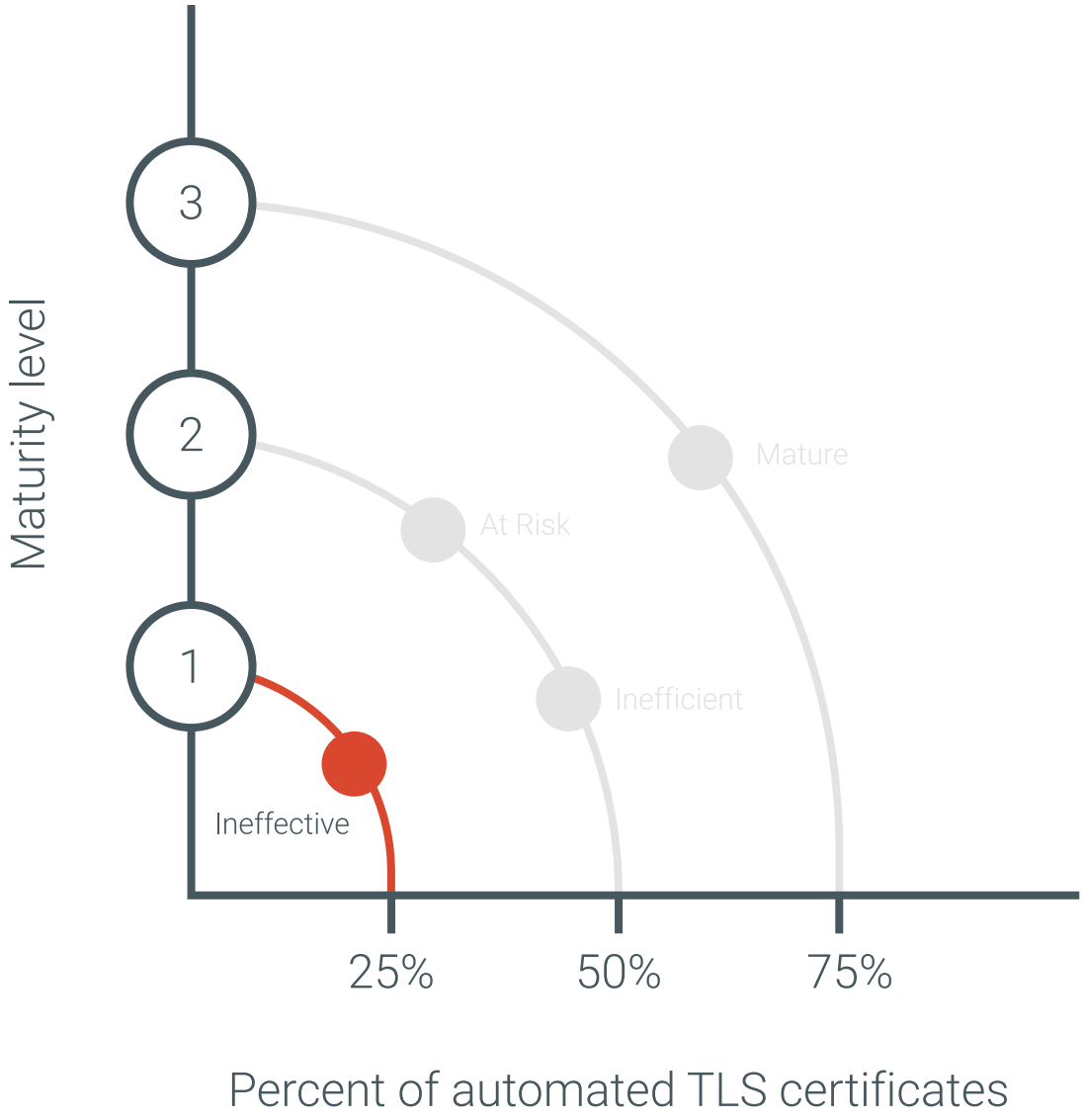


64% find an untracked certificate monthly

38% believe time needed managing certificates is a major concern

Source: TLS Certificate Automation Research YouGov Report, Feb. 2021

TLS AUTOMATION MATURITY MODEL



YOUR RESULTS

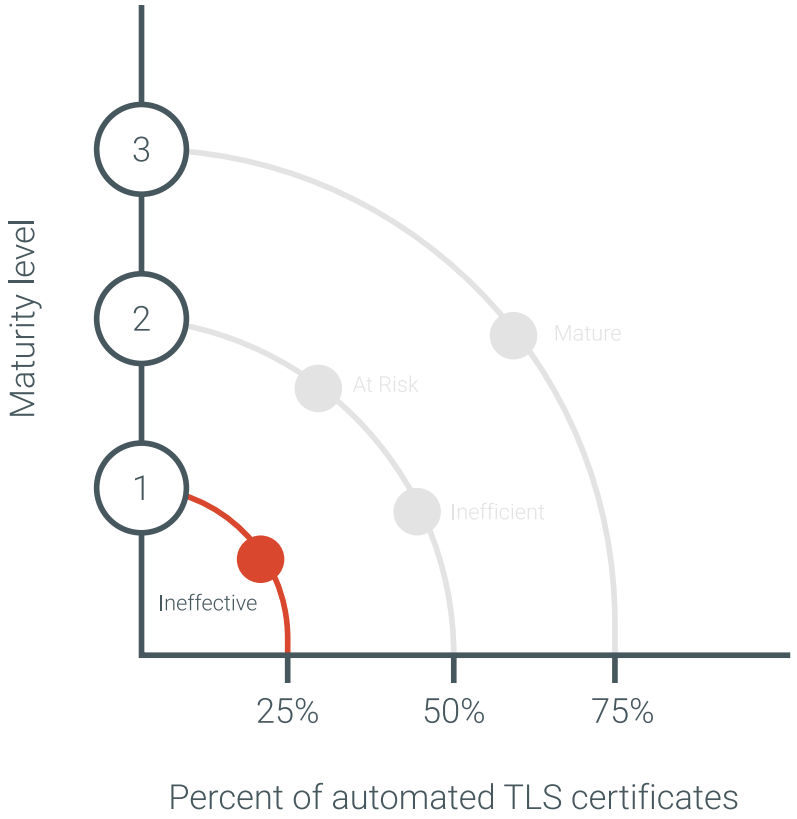
A guide to understanding your security posture.

Security Posture:
REACTIVE

YOUR OVERALL RISK IS: HIGH

Your current certificate management strategies are causing your organization to be reactive to unexpected certificate outages, vulnerabilities or CA events. One of the biggest threats to your security is your lack of awareness and incapacity to take action in a timely manner. Your company is exposed to all types of potential security events by using inefficient, manual processes.

For smaller organizations, you may have a record of your certificate inventory, but are potentially in the dark about certificate related issues that can easily go undetected like misconfigured certificates, weak keys, cipher suites or hashes. For larger organizations, it's difficult to track your complete certificate inventory. This leads to blind spots and potential entry points for malware attacks when rogue certificates are installed from various parts of your organization without your knowledge. Companies at this level are exposed and at a high-risk for costly outages.



THE PATH FORWARD

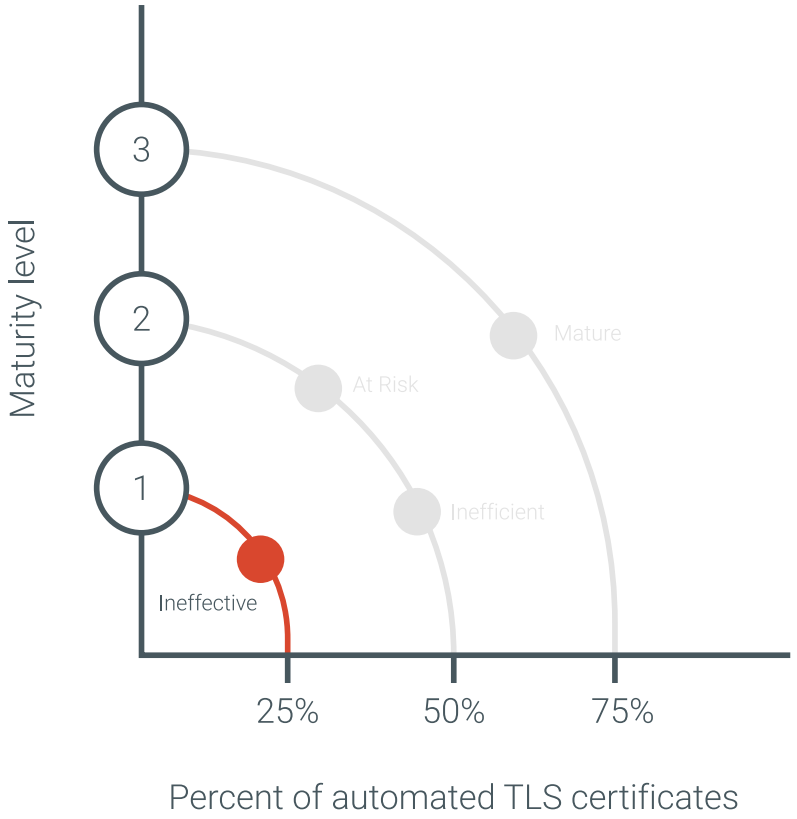
Next steps to improve your security posture.

Security Posture:

REACTIVE

We highly recommend taking the following actions **within the next 90 days:**

- Use a management tool to centrally manage certificates: DigiCert CertCentral® gives you tools to track, issue, revoke and replace all certificates from a single console
- Deploy a discovery scanning tool to view all your certificate inventory: Run targeted scans to help track any changes that occur in your environment and get valuable insights into potential certificate issues
- Focus on TLS management best practices: Educate and train employees to track your entire certificate inventory and protect your environment with standardized key storage, lifecycle components, decommissioning processes and monitoring via CT logs.
- Set up automation processes at scale: Use profiles, schedules, alerts and third-party integrations
- Use our Automation Wizard: DigiCert's industry-unique wizard will help you correctly and easily choose the right deployment model, setup, and installation
- Use APIs: REST API can integrate into any system or application of your choosing. DigiCert also has pre-existing third-party integrations available
- For small to mid-sized enterprises: Managed ACME provides a hosted, agent-based tool that uses ACME protocol and allows for easy management via CertCentral's UI



HOW YOUR TLS SECURITY STACKS UP

Compare your security posture in this overview of all three assessments.

Security Posture:
REACTIVE

YOUR OVERALL RISK IS: HIGH

Your current certificate management strategies are causing your organization to be reactive to unexpected certificate outages, vulnerabilities or CA events. One of the biggest threats to your security is your lack of awareness and incapacity to take action in a timely manner. Your company is exposed to all types of potential security events by using inefficient, manual processes.

For smaller organizations, you may have a record of your certificate inventory, but are potentially in the dark about certificate related issues that can easily go undetected like misconfigured certificates, weak keys, cipher suites or hashes. For larger organizations, it's difficult to track your complete certificate inventory. This leads to blind spots and potential entry points for malware attacks when rogue certificates are installed from various parts of your organization without your knowledge. Companies at this level are exposed and at a high-risk for costly outages.

Security Posture:
NEEDS IMPROVEMENT

YOUR OVERALL RISK IS: MEDIUM

Your organization is off to a solid start by using tools like a centralized TLS/SSL certificate manager. However, your team can still improve on being more agile in order to provide swift remediation to outages or other issues. Without automation tools, the time required to remediate potential issues, particularly within distributed or complex environments can become cumbersome, ineffective, and time consuming. Inefficiency can also be seen in your network when some actions need to be performed in bulk, like replacing vendor certificates (they are often self-signed or have weak keys) or controlling the deployment of correct certificate types.

Under an efficiency front, automating isn't one-size-fits-all, and different deployment types such as on-premises, cloud or hybrid solutions can be more suitable than others.

Security Posture:
PROACTIVE & MATURE

YOUR OVERALL RISK IS: LOW

You've got efficient and controlled automation processes in place and a complete view of all TLS/SSL certificates in your environment making your company proactive to compliance issues, future industry events and potential certificate outages. Mature companies are in control of their certificate entire inventory and have automated up to 75% of their certificates. They've also made automation a standard part of their organization's security policies.

Consider how you can automate up to 100% of your certificate inventory so you are totally prepared for the threats of tomorrow, including replacing certificates swiftly in the case of an outage or post-quantum cryptography future.

OUR RECOMMENDATIONS

Learn more about TLS automation solutions you should implement.

Security Posture:
REACTIVE

We highly recommend taking the following actions **within the next 90 days:**

- Use a management tool to centrally manage certificates: DigiCert CertCentral® gives you tools to track, issue, revoke and replace all certificates from a single console
- Deploy a discovery scanning tool to view all your certificate inventory: Run targeted scans to help track any changes that occur in your environment and get valuable insights into potential certificate issues
- Focus on TLS management best practices: Educate and train employees to track your entire certificate inventory and protect your environment with standardized key storage, lifecycle components, decommissioning processes and monitoring via CT logs.
- Set up automation processes at scale: Use profiles, schedules, alerts and third-party integrations

Security Posture:
NEEDS IMPROVEMENT

We highly recommend taking the following actions **within the next six months:**

- Deploy automation processes tailored for your business: From ACME URL to APIs, Managed ACME Agent, Sensor Automation and the all-new Automation Manager, we provide solutions that are customized to fit your security needs
- Schedule certificate discovery scans for all primary web domains, or fully qualified domain names (FQDNs), monthly
- Consider your TLS stack and look for systems or budget consolidation opportunities: Focus on innovation, process improvements and efficiencies
- Make automation a standard part of your organization's TLS/SSL certificate management policies and lifecycle management
- Use our Automation Wizard: DigiCert's industry-unique wizard will help you choose the right deployment model

Security Posture:
PROACTIVE & MATURE

We highly recommend taking the following actions **within the next year:**

- Continue to make automation your standard policy for certificate management
- Automate multiple deployments using various models (ie. hosted and/or on-premises deployment)
- Schedule certificate discovery scans for all primary web domains, or fully qualified domain names (FQDNs), monthly
- Consider using DigiCert Automation Manager: Our on-premises, containerized, sensor-based management tool that creates a single secured connection for all TLS certificates behind your firewall
- Maintain crypto-agility by continually using automation tools to adapt to future threats such as post quantum cryptography

GET THE INDUSTRY'S BEST ADVICE

Our automation solutions are not one-size-fits-all. Talk to your account manager or email contactus@digicert.com to learn about which automation solution would best meet your organization's security needs.

digicert®