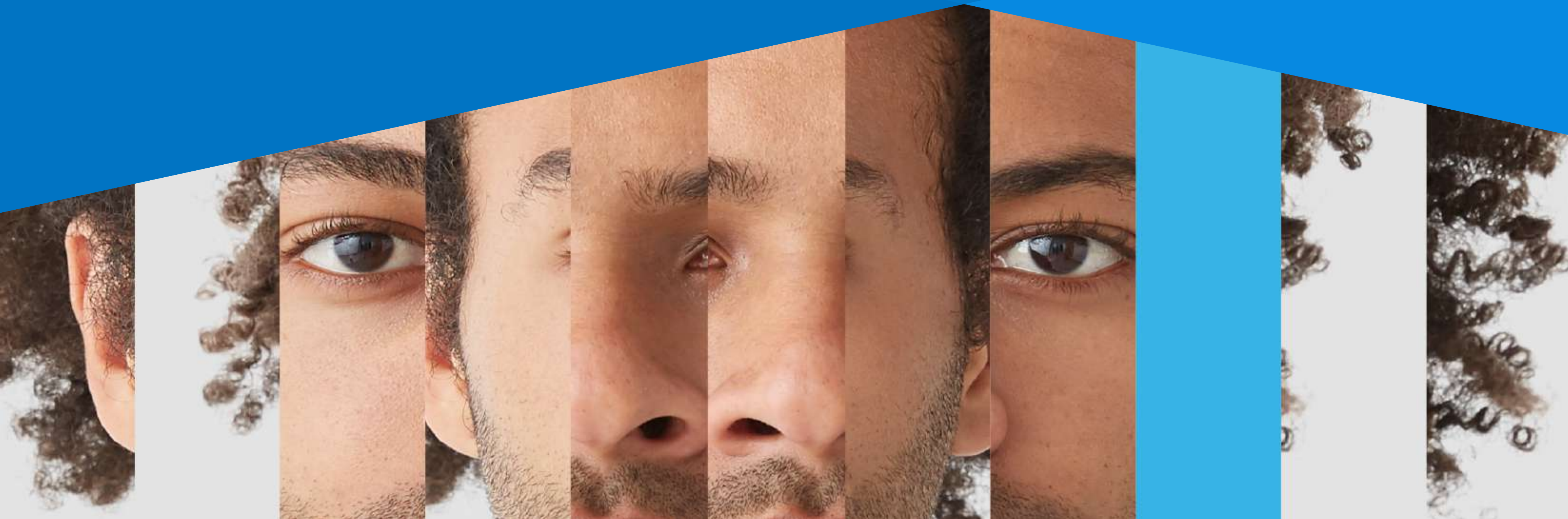
eBook

digicert®

10 WAYS TO PROTECT YOUR BRAND, CUSTOMERS AND REPUTATION



If encryption is security's backbone, then identity is its heart—the human value behind your organization's digital brand. Since eCommerce began in the 1990's, trust and face-value identity has enabled honest business to flow.

But now, malicious websites are often hiding behind encryption. This wide-spread anonymity is jeopardizing business identities, leaving customers to get caught up in scams and left to figure it out. Moreover, a lack of identity verification for users, applications and devices on your network can be an easy way in for hackers and can put your organization in the news—in a bad way.

With the tools in this eBook, you can validate your business identity to your customers, prove your website's legitimacy, secure network access and invest in building customer trust.

Because, by authenticating the identity of your business and protecting both yours and your customers' data, you can interact with confidence.

Reassure your customers it's you.

CONTENTS

REASSURE YOUR CUSTOMERS IT'S YOU

PROTECT AGAINST UNINTENDED ISSUANCES AND UNAUTHORIZED ACCESS

MAKE IT EASY TO MANAGE

> *Phishing was present in 78% of cyber espionage incidents in 2019*.*
>
> **Verizon Data Breach Investigations Report, 2019**

*https://www.nextgov.com/cybersecurity/2019/05/cyber-espionage-targeting-public-sector-rose-168-2018/156849/

REASSURE YOUR CUSTOMERS IT'S YOU

1. USE TLS/SSL CERTIFICATES THAT VALIDATE YOUR IDENTITY

1.1 DV v. OV v. EV

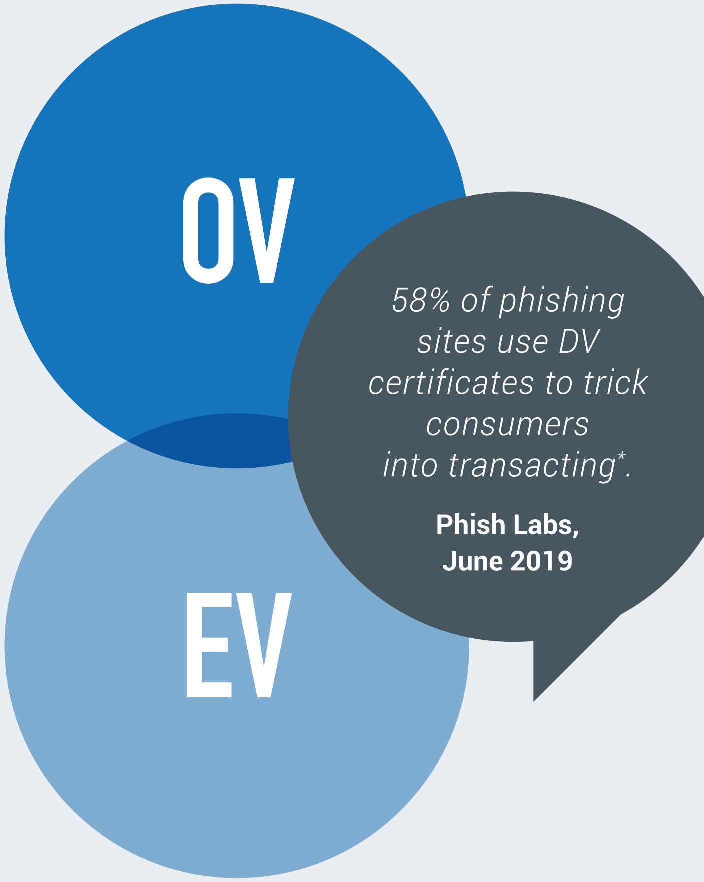
Domain Validation (DV) certificates provide encryption but fail to go the next step in validating the identity of the organization. In fact, many cybercriminals use DV certificates to impersonate official websites. Ultimately, it's the spoofed business's identities that are damaged. It's for this reason that organizations should protect their brand by using high assurance certificates that require the further checks.

By validating your identity with Organization Validation (OV) and Extended Validation (EV) TLS certificates, you prove your legitimacy in the eyes of your customer. These high-assurance TLS certificates put your business through stringent checks prior to being issued in order to provide additional guarantees—such as listing your organization's name and location—to assure consumers your website is authentic.

EV certificates offer the strongest identity assurance, brand protection and user protection by taking advantage of proven, highly trusted authentication methods beyond what OV and DV certificates offer. EV requirements ensure your certificates are only issued for your brand by authorized individuals as well as fully identifying the requestor and the entity making any requests—deterring fraud and allowing your customers to transact with confidence.

In many industries including finance and e-commerce, EV is a security best practice and recommended by industry leaders and regulators. Studies have shown that EV certificates have almost no incidents of phishing when compared to DV and OV certificates[1].

High-assurance certificates not only provide comprehensive website security and robust protection against identity-targeted attacks but prove to your customers you are exactly who you say you are.



58% of phishing sites use DV certificates to trick consumers into transacting.*

Phish Labs, June 2019

[1] Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites. (Vincent Drury and Ulrike Meyer, Department of Computer Science, RWTH Aachen University

*https://info.phishlabs.com/blog/more-than-half-of-phishing-sites-use-https

1. USE TLS/SSL CERTIFICATES THAT VALIDATE YOUR IDENTITY

1.2 ADDED IDENTITY PROTECTION AND TRUST FOR THE FINANCIAL SECTOR

Inconsistencies and differing levels of trust across the European Union's (EU) online financial market led to the introduction of eIDAS (electronic IDentification, Authentication and trust Services) for Payment Service Providers (PSPs).

eIDAS reduces red tape by standardizing and securing the market. Two of the qualified certificates are Qualified Web Authentication Certificates (QWAC) and Qualified eSeal Certificates (QsealC).

With a QWAC, you can validate your identity to your customers through your website while simultaneously encrypting and securing sensitive payment data. The authentication methods for QWACs are even more rigorous than for EV and require face-to-face validation of an authorized representative for the organization named in the certificate.

QsealC secures your applications and documents, 'sealing' your data, sensitive documents and other communications to ensure that they're tamper-proof and originate from a trustworthy source.

While PSP regulations vary depending on the region of the world in which you live, these certificates became mandatory in the EU for PSPs in September 2019 when the Payment Service Directive (PSD2) came into force.

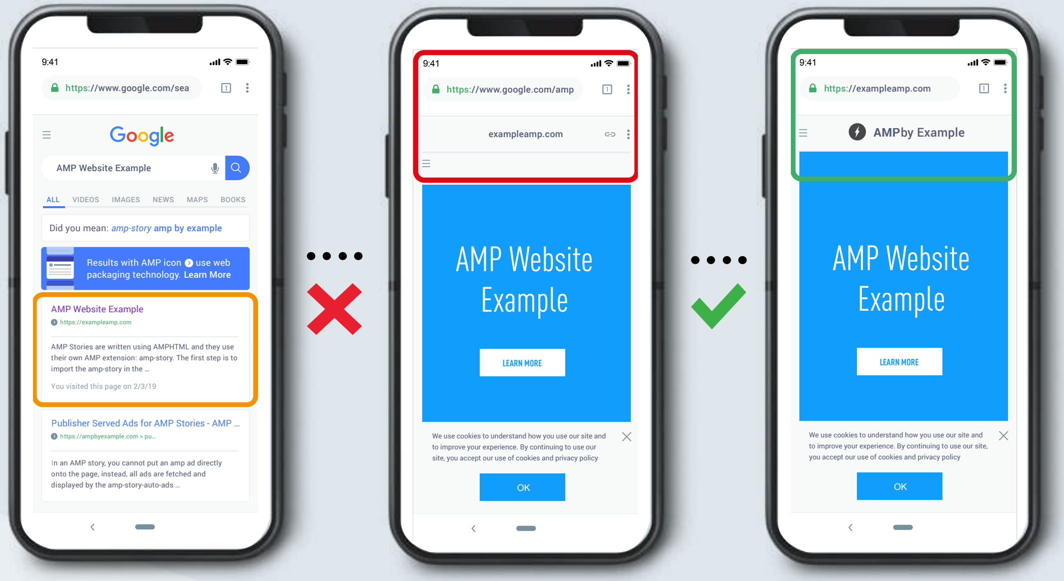
Securing this process through our high-assurance certificates and seals will communicate to your customers clearly and honestly that their information is safely making it only into your hands.

1. USE TLS/SSL CERTIFICATES THAT VALIDATE YOUR IDENTITY

1.3 SIGNED HTTP EXCHANGE (SXG) CERTIFICATES

If your business relies on high volumes of web content being viewed on mobile devices, you may be using Google AMP to enhance load times. But Google AMP makes your AMP-hosted web pages look as if they are owned by Google—often causing customer confusion and potentially a poor brand experience.

DigiCert® SXG certificates correct this impression so your company name appears correctly in the URL, while decreasing load times for cached content and maintaining the intended level of security for your webpage.


9:41
https://www.google.com/sea
Google
AMP Website Example
ALL
VIDEOS
IMAGES
NEWS
MAPS
BOOKS
Did you mean: amp-story amp by example
Results with AMP icon use web packaging technology. Learn More
AMP Website Example
https://exampleamp.com

AMP Stories are written using AMPHTML and they use their own AMP extension: amp-story. The first step is to import the amp-story in the ...

You visited this page on 2/3/19

Publisher Served Ads for AMP Stories - AMP ...
https://ampbyexample.com › pu...

In an AMP story, you cannot put an amp ad directly onto the page, instead, all ads are fetched and displayed by the amp-story-auto-ads ...

9:41
https://www.google.com/amp
exampleamp.com
AMP Website Example
LEARN MORE

We use cookies to understand how you use our site and to improve your experience. By continuing to use our site, you accept our use of cookies and privacy policy

We use cookies to understand how you use our site and to improve your experience. By continuing to use our site, you accept our use of cookies and privacy policy

Without a DigiCert SXG certificate, your brand and content looks like it belongs to Google.

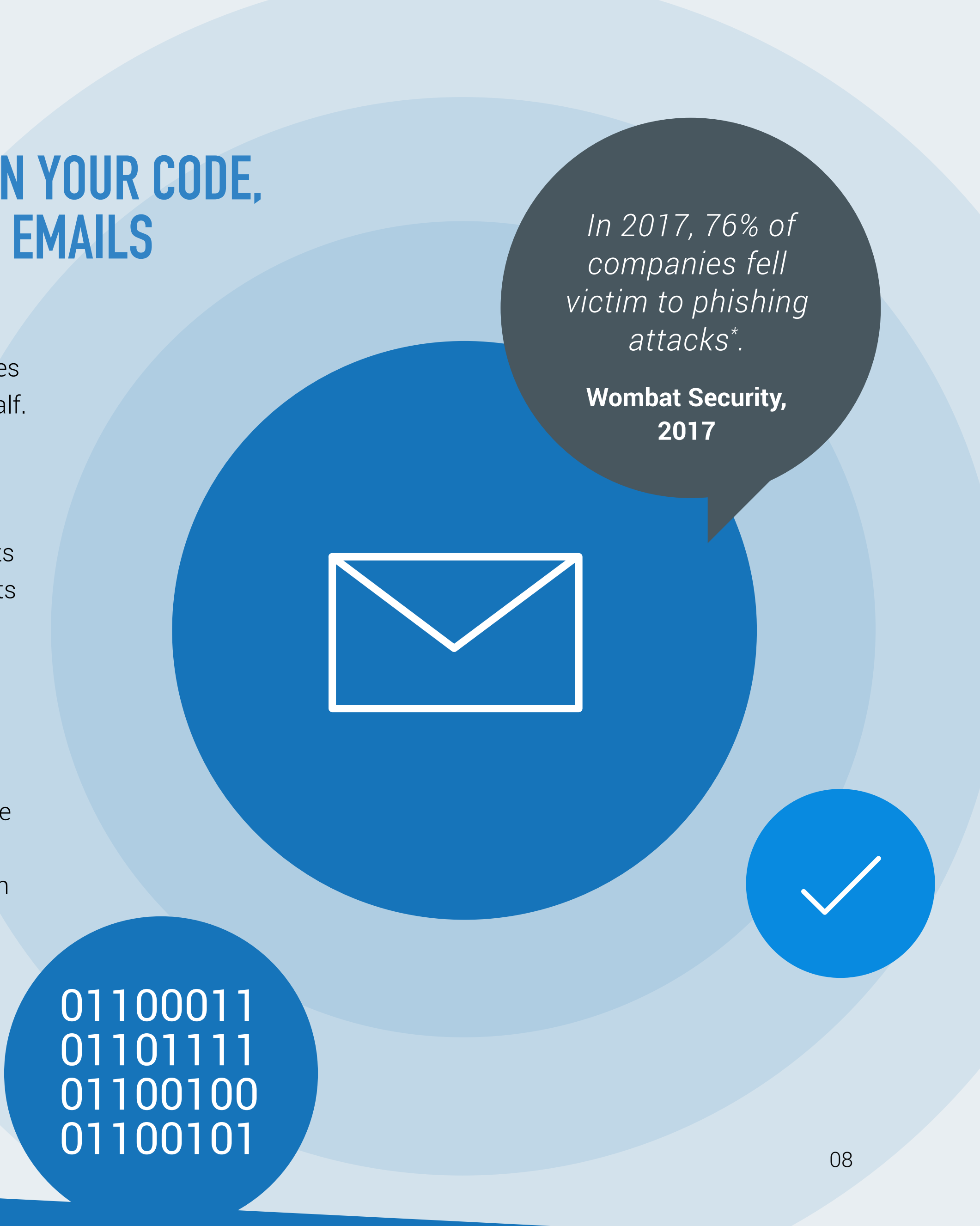
With a DigiCert SXG certificate, your domain and content is displayed with your URL and brand.

2. DEMONSTRATE IDENTITY EVERYWHERE: SIGN YOUR CODE, SIGN YOUR DOCUMENTS, AND SEND SECURED EMAILS

Your organization is identified by the emails, documents and applications that you send. Cybercriminals frequently intercept and embed malware in these types of assets and allow the recipients to unknowingly spread malware on their behalf. If your organization is targeted, it will be perceived as the source of the malware which could damage your reputation and lead to financial loss.

By implementing digital certificates for code and application signing, documents and emails, you can assure customers and partners of the integrity of the assets they receive. If your assets become compromised, your recipients are alerted and the assets are no longer associated with your company. This halts the exploitation of your identity to propagate malware.

DigiCert Enterprise PKI (Public Key Infrastructure) Manager™ simplifies security of both email communications and document signing. With flexible certificate profile configurations and enrollment methods, you're able to rapidly implement and enforce the security posture your business demands. And because it's based on the DigiCert ONE™ platform, you can manage your way—in the cloud, on-prem, hybrid and even in-country.



In 2017, 76% of companies fell victim to phishing attacks.*

Wombat Security, 2017

*https://www.wombatsecurity.com/news/76-organizations-report-being-victims-phishing-attacks

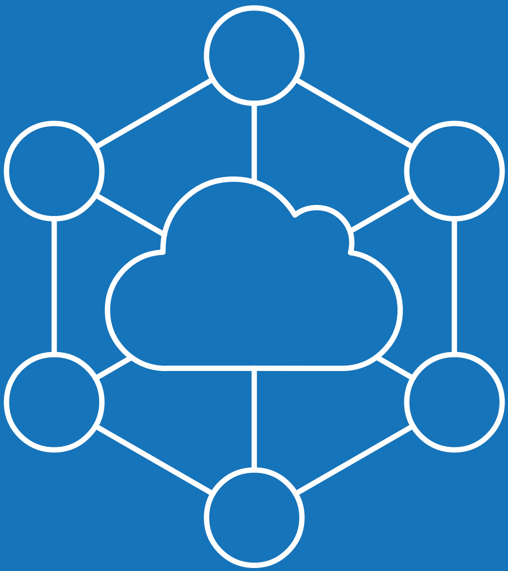
3. ESTABLISH IDENTITY FOR ALL YOUR IoT DEVICES

An estimated 75.44 billion connected devices are expected to be installed by 2025[3]. Security is one of the top concerns with IoT adoption by enterprises —in fact cybercriminals have already targeted IoT devices such as security cameras[4].

By deploying PKI and digital certificates, manufacturers can establish device identity for their IoT devices. This helps manufacturers to track their devices and provide system updates as necessary to maintain strong security. It also allows manufacturers to enable device-to-device interactions in certain industries, e.g. the auto industry. Unknown or unauthorized devices may be prevented or restricted, minimizing the risk of cyberattacks.

DigiCert IoT Device Manager™ gives you the power to bind certificate-based identity to your IoT devices centrally; to assign, define, and control the cryptographic based identity for every one of the devices in your network. By establishing your device's identity on the factory floor, you build another layer of security, reducing the risk for end-users.

> *The average cost of a data breech in 2020 will exceed $150 million*.*
>
> **Juniper Research, 2019**



[3] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[4] https://www.propertycasualty360.com/2019/12/19/protecting-iot-devices-from-cyberattacks/?slreturn=20191119173130

*https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

4. POST A TRUST SEAL ON YOUR WEBSITE

Concerns about payment security are always on your customers' minds. This is exacerbated by the growing prevalence of cybercrime; in fact, in 2017 almost 20% all shopping cart abandonment was due to payment security concerns. So, it is vital to visually define your identity to your customer at the point of sale.

Trust seals continue to be one of the top drivers of online trust and are a highly valuable feature of high-assurance TLS certificates. In fact, tests have shown an 18% reduction in bounce rates as well as a 19% increase in conversion after the introduction of trust seals to websites.

All DigiCert Secure Site™ TLS certificates come with the DigiCert Secured™ seal. All DigiCert Secure Site TLS certificates come with the DigiCert Secured™ seal or the Norton Powered by DigiCert seal. This gives customers quick and familiar assurance at the most critical moment of sale—and allows especially wary users to confirm the trustworthiness of your site with a single click.

digicert®
SECURED
TM

Norton
TM
powered by digicert®

DigiCert Trust Seals are ranked as the most trusted online.

Website Security Seal Study, 2018

[5] https://www.barilliance.com/10-reasons-shopping-cart-abandonment/

[6] https://www.digicert.com/site-seal-conversion-rate-benefits.htm

PROTECT AGAINST UNINTENDED ISSUANCES AND UNAUTHORIZED ACCESS

5. GUARD AGAINST UNINTENDED CERTIFICATE ISSUANCE

5.1 CREATE A CERTIFICATE AUTHORITY AUTHORIZATION (CAA) LISTING

To capitalize on an organization's trusted identity, malicious actors—both internal and external—will sometimes attempt to obtain a trusted certificate from a third party Certificate Authority (CA) on behalf of a legitimate domain. Because this "rogue certificate" is issued in the organization's real name by a known authority, end users have no reason to question its legitimacy, and attackers are free to essentially hide malicious content in plain sight. This is especially dangerous for larger organizations, where a single mis-issued certificate can easily slip through the cracks.

To protect domain owners from this type of attack, it became mandatory in 2017 for any CA to complete a check against a domain's CAA record before issuing a certificate.

CAA records are a "whitelist" of trusted CAs that is defined by the owner of a domain. By maintaining tight control of your CAA record—and permitting only CAs with strict authentication standards to issue certificates—you can prevent attackers from using mis-issued certificates to compromise your company's identity.

5. GUARD AGAINST UNINTENDED CERTIFICATE ISSUANCE

5.2 MONITOR CERTIFICATE TRANSPARENCY (CT) LOGS

A CT log is a curated list of certificates that allows businesses to quickly identify mistaken or fraudulently issued certificates.

Along with monitoring capabilities, certificate transparency makes all certificates issued to domain visible to the domain owner—making it easy to identify any unintentionally issued or fraudulent certificates and protect end users from them.

By proactively monitoring CT logs, you can detect unauthorized certificates that have been issued either without your express approval or outside your domain policy in a matter of minutes as opposed to days, weeks or months.

If you don't use CT logs monitoring you may have certificates that are outside your organization's security policies, issued from unapproved or fraudulent CAs, or incorrectly installed certificates that could leave your organization's most important domains vulnerable.

6. CHECK FOR BLACKLISTING

If you have a security issue with one of your domains you risk losing the trust of your customers as well as your domain being blacklisted. Having a certificate management solution that includes a blacklist checker not only simplifies your certificate administration, but also makes sure your domain doesn't become distrusted by browsers without your knowledge.

More than 1 million phishing websites pop up every month.*

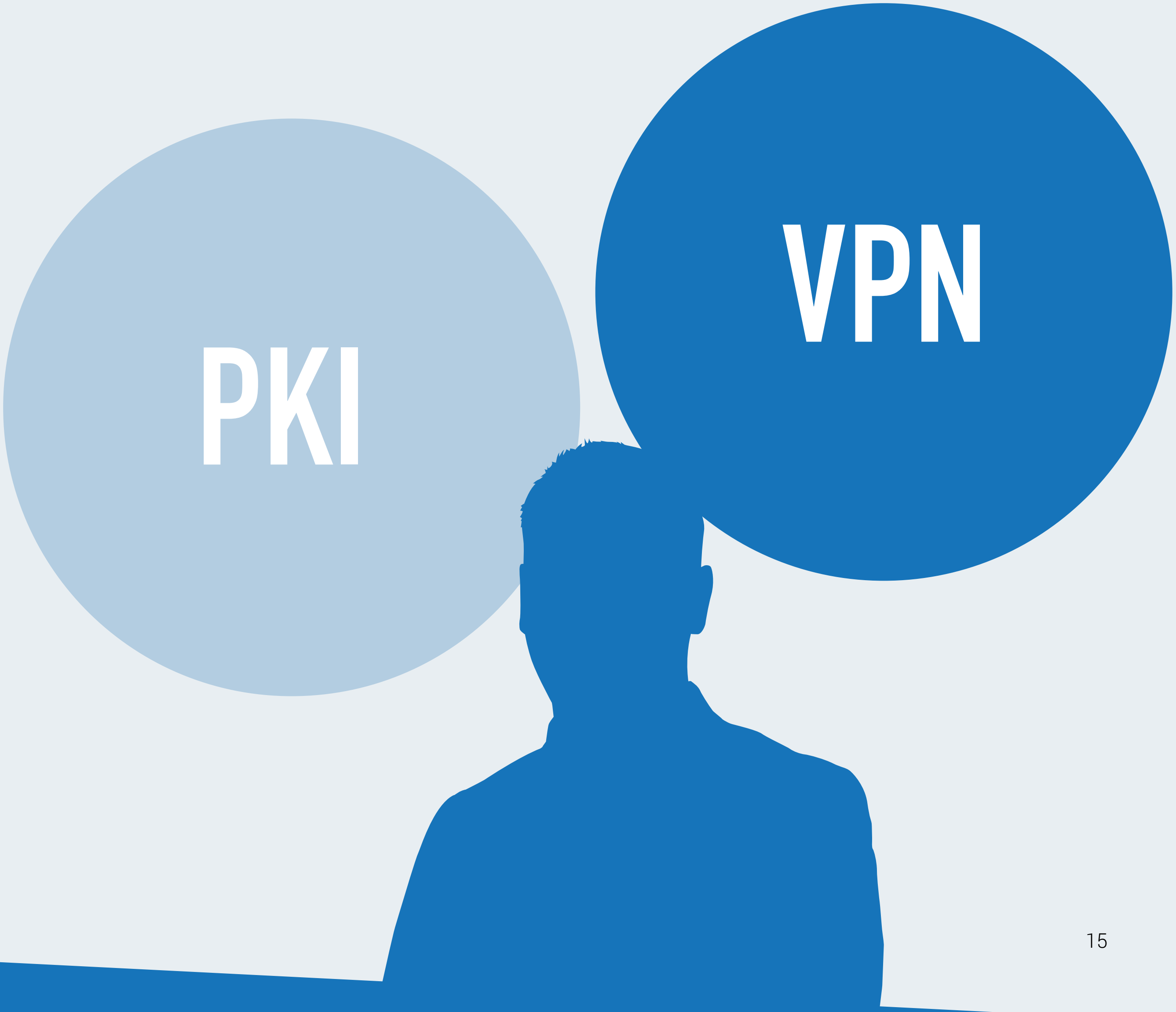
Webroot Quarterly Threat Trends, 2017

[3]https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf

7. VERIFY USER AND DEVICE IDENTITY

Within an enterprise, employees, contractors and partners use all types of devices to access sensitive information via corporate networks and applications. The lack of proper user or device authentication may result in a security breach that could lead to data and reputation loss.

By implementing Public Key Infrastructure (PKI) for mobile, VPN access and smartcard login, you can ensure trusted users and devices have access only to the information you authorize.



MAKE IT EASY TO MANAGE

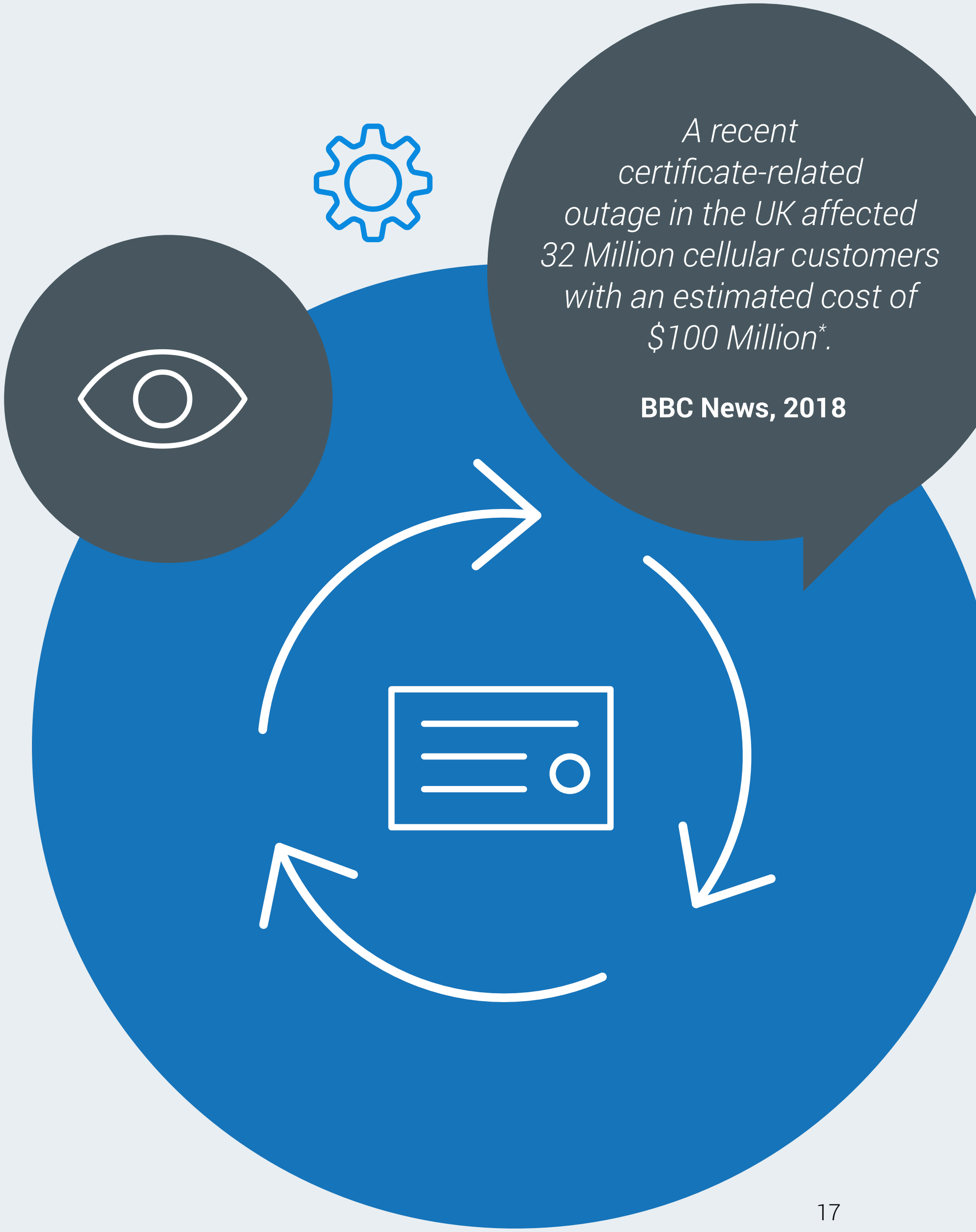
8. DISCOVER AND AUTOMATE

Lack of visibility is a top challenge many organizations face in managing their certificates. It's why many organizations operate without knowing if all their certificates are valid and is one of the largest contributors to the certificate-related outages that are damaging brands. The ability to streamline the management of the entire process is becoming a necessity.

DigiCert CertCentral® empowers your business with Discovery and Automation features—instantly detecting problems and vulnerabilities across your certificate portfolio and remediating issues based on recommended actions from the certificate analysis tool. You gain the visibility of your entire certificate inventory and instant control over problematic certificates.

With CertCentral, you may use the ACME protocol to automate deployment of OV and EV certificates—and even set custom validity periods—with every part of the cycle visible from a single screen.

CertCentral consolidates tasks for issuing, installing, inspecting, remediating, and renewing certificates. That means less time spent completing tedious manual workloads—or putting out fires—and more time focusing on brand-elevating tasks with the peace of mind that your certificates are sorted.



A recent certificate-related outage in the UK affected 32 Million cellular customers with an estimated cost of $100 Million.*

BBC News, 2018

*https://www.bbc.co.uk/news/business-46499366

9. SIMPLIFY DIGITAL CERTIFICATE ADMINISTRATION FOR ENTERPRISE IT

Many enterprises rely on highly complex certificate management environments. This uncertainty has pushed growing numbers of businesses to the proven security of PKI to safeguard their sensitive assets.

Public Key Infrastructure (PKI) is a suite of hardware, software, processes and policies that give a business the ability to create and manage all their digital certificates and public keys. But setting up PKI or even just deploying PKI can be a daunting and intricate task.

However, with ubiquitous and modern infrastructures, many enterprises are now beginning to take advantage of new agnostic integration techniques. PKI platforms simplify certificate lifecycle management and the end-user experience with secure communications. This is seamlessly integrated into your network and business applications, greatly enhancing your data access.

DigiCert Enterprise PKI Manager, part of DigiCert ONE, enables midsize and large enterprises to maintain strong authentication and encryption, secure email and digital signing with high performance, availability and scalability.

The DigiCert ONE platform delivers PKI solutions with minimal complexity and industry-leading flexibility via on-premises, cloud, or via hybrid deployment models to meet your business or in-country requirements.

*https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

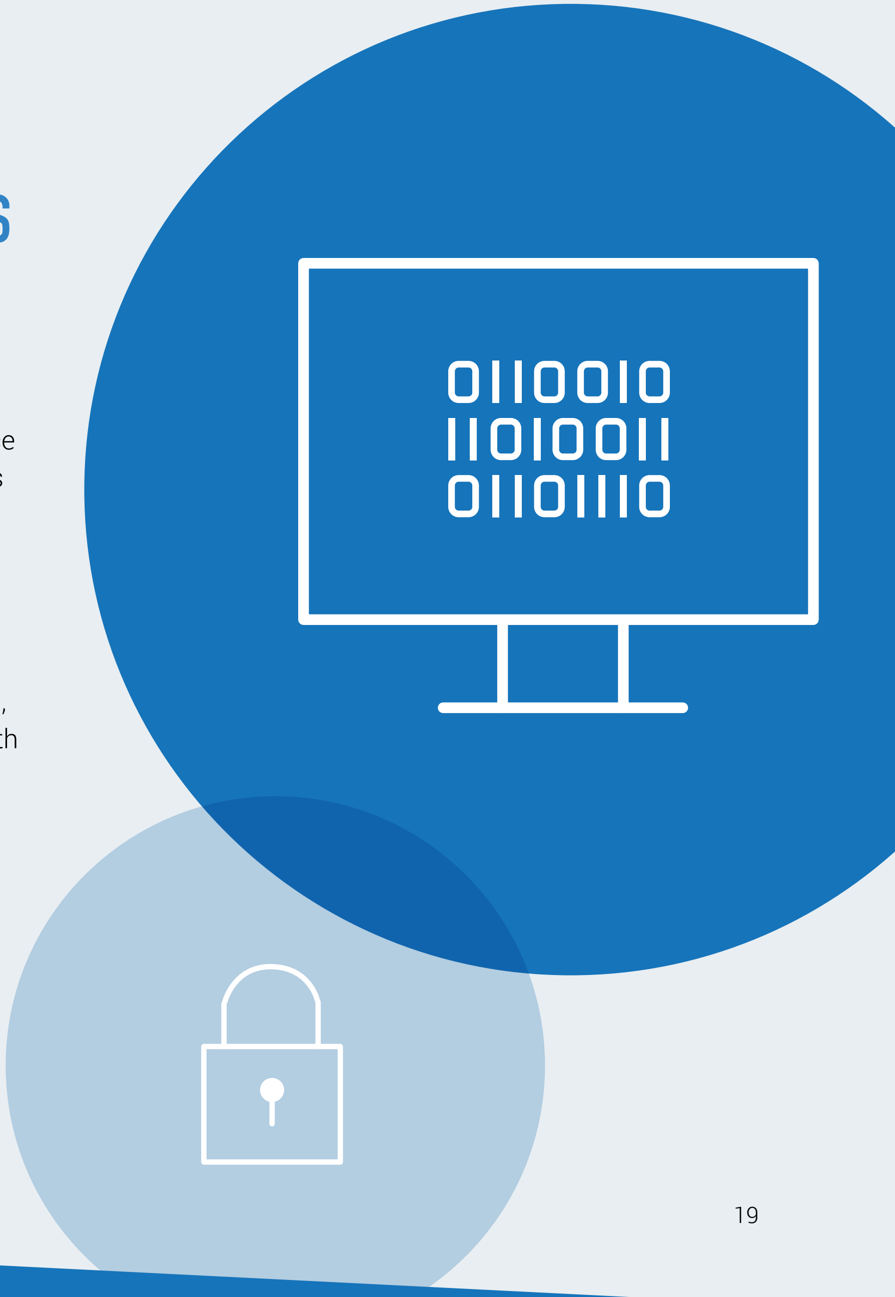
10. INTEGRATE SECURITY WITH DEVOPS AND BUSINESS COMMUNICATIONS SEAMLESSLY

The steps above prepare you for the most common causes of vulnerabilities that lead to compromised business identities. But many organizations striving to meet industry compliance standards and adopt best practices for a strong security profile find that some security practices can slow down product development and overall productivity.

By automating security and integrating it into the DevOps process, your code or app is continuously secured throughout its development with just the push of a button.

DigiCert Secure App Service™ (SAS) makes it easy for organizations to incorporate automated, secure and high-performing code signing within the DevOps process. Easy integration with both Continuous Integration/Continuous Delivery (CI/CD) platforms and DigiCert's Cryptographic Service Provider™ (CSP) enables automation and drives cost efficiency.

Key management options, role-based access control and audit logs increase security, control and accountability. While hash signing allows for rapid high volume and large file signings. All of this is powered by DigiCert's Secure App Service, enabling companies of all sizes to maintain secure and best practices in code signing.



CONTACT

For more information about how you can achieve the best practices for your TLS deployments, email our experts at:

contactus@digicert.com

To learn more about IoT and PKI management solutions that can transform your entire enterprise network, contact:

pki_info@digicert.com