Enterprise Strategy Group by TechTarget

BRIEF

FEBRUARY 2025

Entrust Selling Certificate Business Underscores Need for Enterprise Crypto Agility

Todd Thiemann, Senior Analyst

Abstract: Entrust announced the sale of its certificate authority business to Sectigo in January 2025, an event that will cause many enterprises to reevaluate their certificate lifecycle management strategy. Recent research by Informa TechTarget's Enterprise Strategy Group into non-human identities (NHIs) revealed that digital certificates were of concern to enterprises,[1] and the Entrust-Sectigo transaction reinforces the need for enterprises to maintain crypto agility to adapt to and recover from changes in cryptographic infrastructure. Enterprises should focus on gaining visibility into their expanding digital certificate estate in preparation for upcoming changes posed by shortening certificate validity periods and impending changes needed to prepare for post-quantum cryptography (PQC).

Overview

To gain further insight into trends and issues surrounding the management of NHIs, Enterprise Strategy Group surveyed 367 IT, cybersecurity, DevOps, platform, and cybersecurity engineering professionals at organizations in North America (US and Canada) involved with or responsible for the technologies and processes that secure NHIs and machine workloads. As part of that research, these decision-makers were asked about their concerns around security and management of NHI assets, including digital certificates.

Analysis

NHIs, also referred to as machine identities or workload identities, are an essential but frequently underappreciated element of the enterprise attack surface. These identities include digital certificates, application credentials, API keys, and service accounts. The most common concern raised by enterprises for NHI management was the risk of operational disruption caused by an expiring digital certificate (see Figure 1).

Entrust was facing declining trust in its certificates and made a strategic decision to stop operating as a public certificate authority (CA) and divest its CA customers and contracts to Sectigo. This move enabled Entrust to focus on higher-growth security products while allowing Sectigo to grow its enterprise customer base.

Zooming out to understand the context, digital certificates verify the identity of websites, individuals, devices, or servers and enable secure communication across the internet. Certificates establish a trust chain, and revoking certificates causes digital havoc and requires applications, browsers, endpoints, and mobile devices to be revised to include a new and trusted certificate.

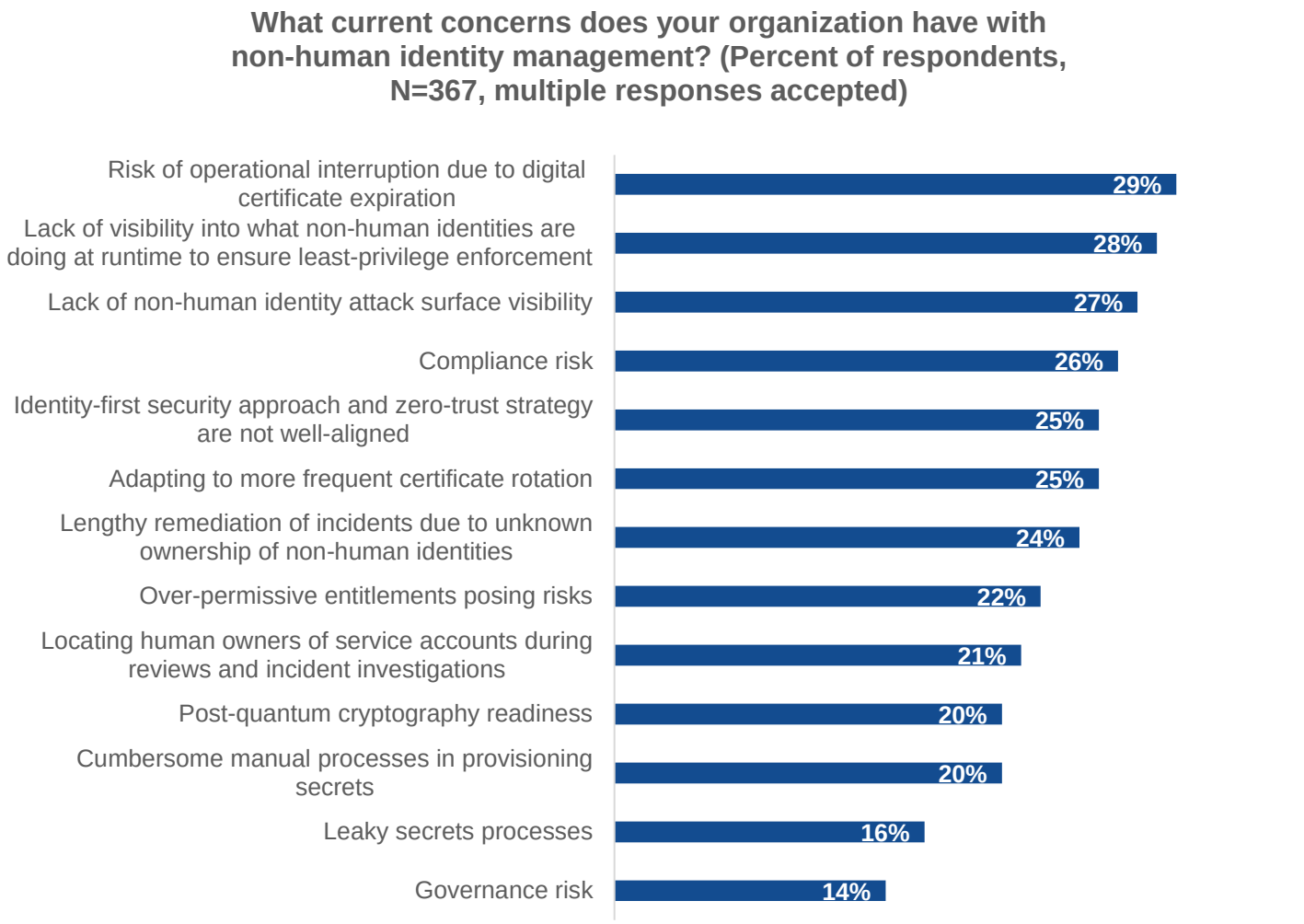
Enterprises have previously had to adapt to rapid change in their certificate estate, such as when Google, Mozilla, and Apple announced in 2018 that they would be distrusting Symantec CAs and urged anyone using a Symantec CA to replace their certificates using a trusted CA instead. That was a significant disruption that challenged

[1] Source: Enterprise Strategy Group Research Report, *Managing Non-human Identities for an Effective Cybersecurity Program*, December 2024. All research references and charts in this brief are from this report.

enterprise PKI and security teams to move to a new CA or risk critical application and service outages. Symantec would then later exit the CA business by selling its CA operations to DigiCert.

Another recent example of rapid change occurred in 2024 when DigiCert announced that it would be revoking TLS/SSL certificates that were incorrectly validated. Rapidly responding to these sorts of changes can be challenging without the right certificate lifecycle management infrastructure and processes.

Figure 1. Digital Certificate Expiration Leads Concerns Around NHI Management



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cryptographic agility refers to the ability of an enterprise to rapidly adapt cryptographic algorithms and practices without significantly disrupting the overall compute infrastructure. It enables organizations to switch between different algorithms and protocols, update cryptographic components, implement new security standards, and prepare for PQC challenges. Certificate lifecycle management (CLM) solutions provide a key building block for crypto agility.

While CLM solutions are frequently used, many enterprises still use spreadsheets and manual processes to manage certificates. Such manual processes are error-prone and can break down as certificate volumes grow. The danger here is that expiring certificates and misconfigurations put enterprises at risk of application outages and vulnerabilities.

The standards for CAs are set by the industry's Certification Authority Browser Forum (CA/Browser Forum), which includes the major security ecosystem participants that play a role in certificate infrastructure. Those standards include rules around certificate issuance, validation, and revocation and are intended to secure data transported via the internet. The CA/Browser Forum is considering proposals from Google and Apple to reduce the validity period of certificates to enhance security and promote automation. The current lifespan is 398 days, but that period is expected to dramatically shrink in response to a proposal from Google to reduce the maximum Transport Layer Security (TLS) server certificate validity to 90 days, while Apple is proposing to shorten SSL/TLS certificates to 47 days by 2028. That shorter certificate validity requires that enterprises increase their agile certificate management processes and consider automation to adapt to more frequent certificate rotation.

Enterprises also need to consider expected changes from traditional public-key cryptographic algorithms to standardized PQC. NIST recently released an Initial Public Draft (IPD) report detailing the NIST roadmap for the PQC adoption, which includes aggressive timelines for deprecating (2030) and disallowing (2035) a broad range of currently used algorithms. Enterprises will eventually need to consider deploying updated cryptographic algorithms to prepare for quantum threats targeting traditional encryption algorithms.

To understand migration timelines, consider the Secure Hash Algorithm (SHA). SHA-1 was deprecated in 2011. The SHA-1 to SHA-2 migration started around 2013-2014, and public systems largely transitioned by 2017, yet it took many enterprises an additional three to five years to fully migrate private and internal systems to SHA-2 due to the logistical challenges of the process. In other words, migrations can take time and preparation.

With change on the horizon, enterprise security teams need to prepare and up their crypto agility game. The first step to crypto agility is getting visibility to public and private trust certificates across an organizations' complex hybrid multi-cloud environments. A full discovery and the creation of a dynamic inventory of these certificates, including crypto algorithms, expiration dates, the CA, where the certificates are installed, and the internal owner of the certificates, provides a starting place. Understanding the human owner of the non-human certificate will speed action when changes need to happen. And manually cobbling together inventory information in a spreadsheet is a dangerous game that risks missing something significant.

Conclusion

The Entrust decision to sell its CA business to Sectigo provides a catalyst for enterprises to prepare themselves for change, which can come quickly through distrusted certificates or more gradually as certificate validity periods shorten or PQC algorithms need deployment. As organizations start to prepare for PQC readiness, it's time they implement crypto agility and use the recent certificate incidents and coming changes to improve their overall crypto hygiene. Improving crypto agility with necessary processes and solutions in place to evolve and future-proof their certificate infrastructure will enable enterprises to turn a potential catastrophe into a minor bump in the road.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com