EBOOK

Security at the Speed of DevOps

HOW SECURITY & DEVOPS CAN COLLABORATE TO MITIGATE RISK

KEYFACTOR

Table of Contents

© 2020 Keyfactor | All Rights Reserved | www.keyfactor.com

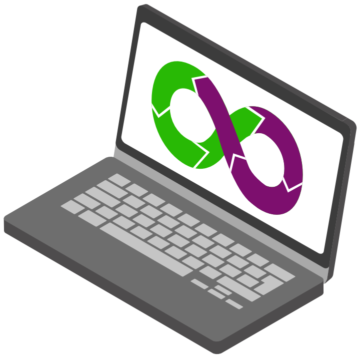
Introduction

Today, speed and security rule the world of enterprise technology. Unfortunately, the two are often at odds. But in a world where no organization can afford to sacrifice either one, we must find a solution to satisfy both.

THE NEED FOR SPEED IN HIGHLY COMPETITIVE, INNOVATIVE MARKETS

From finance and healthcare to retail and manufacturing, the level of competition is higher than ever. And this competition is fueled in large part by innovations in technology that create better business processes and customer experiences.

Those who cannot keep up with the pace of innovation are likely not to succeed. As a result, most enterprise engineering teams have embraced new technologies, such as cloud and containers, and new development methodologies, such as DevOps, Agile and Continuous Integration/Continuous Delivery (CI/CD), to help them deliver more, faster.



HEIGHTENING SECURITY TO MAINTAIN TRUST IN A CONNECTED DIGITAL-FIRST WORLD

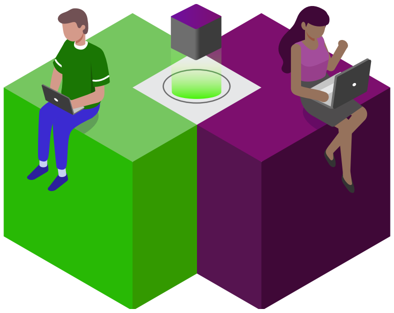
The high levels of innovation — and the speed at which those advancements now come to market — have created a highly connected, digital-first world. While these advancements have allowed us to do more, faster and created better experiences, they also increase security vulnerabilities.

Each digital connection poses a security risk that enterprises must protect. Failure to do so can result in a loss of trust, which leads to lost customers and can prove nearly impossible for businesses to recover from. This situation puts enormous pressure on enterprise security teams to exercise tight controls.

DELIVERING ON SPEED AND SECURITY SIMULTANEOUSLY

As engineering and development teams continue to move faster to deliver innovative new products to market and stay ahead of the competition, it becomes extremely difficult for security teams to keep up. And in many cases, security teams have already fallen behind — whether or not they know it yet.

This situation is not sustainable though, and the time to find a solution is now. This eBook will explore exactly how we got here, the gaps between DevOps and security that exist today, how to bridge those gaps and the benefits that come from doing so.



© 2020 Keyfactor | All Rights Reserved | www.keyfactor.com

HOW WE GOT HERE:

Speed and Security in the Digital Enterprise

Over the past decade, we've heard a lot about digital transformation in the enterprise. Now, we're seeing the results of those transformations, with the realization of a digital-first world.

As with any change, the move to digital has brought with it a new set of challenges, and one of the biggest that enterprises face today is maintaining the necessary level of security alongside the ever-increasing speed and diversity of development processes.

Today's Development Teams Deliver Fast

In terms of speed, many enterprises now have highly experienced development teams that are responsible for delivering new (and updated) applications to market. These teams face pressure to build, package and deliver applications quickly. For example, whereas enterprises once delivered the latest version of their software with big changes in each version every 1-2 years, organizations now release updates with smaller changes every several weeks.

MODERN DEVELOPMENT TEAMS HAVE EMBRACED:

CLOUD AND CONTAINERS

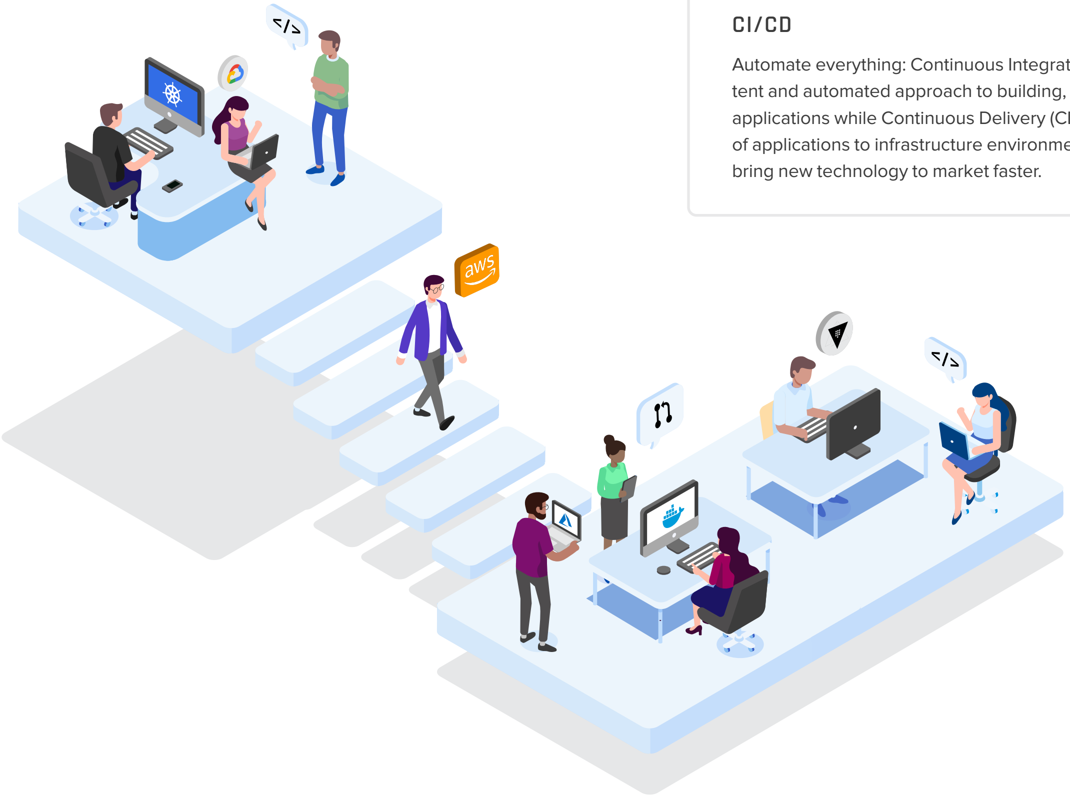
Ensure technology can run anywhere: Solutions like AWS, Microsoft Azure, Kubernetes and service mesh tools provide the access, flexibility and redundancy to ensure applications can run anywhere and reduce downtime.

DEVOPS AND AGILE

Stay nimble and deliver fast: Development methodologies like DevOps and Agile change the way engineering teams work by creating a continuous feedback loop that allows them to respond to changing requirements faster and deliver new features more quickly, rather than all at once.

CI/CD

Automate everything: Continuous Integration (CI) calls for a consistent and automated approach to building, packaging and testing applications while Continuous Delivery (CD) automates the delivery of applications to infrastructure environments, both of which help bring new technology to market faster.



Today's Security Teams Must Keep Up

Security has always been and will continue to be of utmost importance. Afterall, no one will use a technology that compromises important information or is prone to hacking. But how do you embed security into highly connected and dispersed platforms that are built and deployed in a fast-moving environment?

That's exactly the challenge facing modern security teams. New points of connection across infrastructure mean more vulnerabilities that require security controls, as does the use of more open-source and cloud-native toolsets within the development process. This growth alone would be challenging, but when you pair it with the fast pace at which development teams move, securing every single point becomes nearly impossible with the tools security teams have at their disposal.

Secrets management tools like HashiCorp Vault allow developers to securely store and access passwords, tokens, API keys and other credentials required for their day-to-day operations. In some cases, they can also act like a certificate authority (CA) to give developers quick access to digital certificates used in provisioning and signing processes. However, the problem is that security teams often lack visibility and control over these built-in CAs used outside of their owned and operated enterprise public key infrastructure (PKI). An increasing gap exists between the tools and policies used by developers and security teams.

PKI Enables Trust, But Volume and Velocity Explode in the Cloud

Public key infrastructure governs the issuance of digital certificates to protect sensitive data, authenticate users, devices and applications and secure end-to-end communications. It started out with a few limited use cases, such as issuing digital certificates to secure websites and allow devices to connect to VPN or Wifi networks. These limited use cases made it easy for security teams to manage PKI against set policies, including issuing, tracking and monitoring certificates. Today's highly connected, digital world has changed this.

In the past decade, we've moved from a static, perimeter-centric view of security to a dynamic, identity-based approach, and this shift has disrupted the way we use PKI. Cloud-native applications built around microservices have replaced static, monolithic applications and increased the volume and velocity of digital certificates required by enterprise PKI. Specifically, we not only have more devices and applications now, but the makeup of each one is more complex, which has increased the need for secure machine-to-machine communications. Meanwhile, the fast pace at which DevOps teams build new solutions and update applications has also increased the velocity at which these certificates need to be issued.

Along the way, many security teams have lost control over all of the certificates in play. This has happened as DevOps teams gain the ability to issue their own certificates through open-source tools or built-in CAs like Let's Encrypt, AWS, Microsoft Azure, Kubernetes and HashiCorp Vault. And when DevOps teams issue their own certificates, many of which security teams don't even know about, it becomes nearly impossible for security leaders to manage those certificates throughout their lifecycle and enforce policies consistently.

WHERE WE STAND NOW:

Understanding the Gaps Between DevOps and Security Teams

The speed of today's DevOps teams and the complexity of the solutions they build has led to rapid growth in the velocity and volume of digital certificates required. And as the use of digital certificates has exploded in most organizations, it's added a lot of complexity to how we think about enterprise PKI. But for the most part, security teams are still operating under older models of PKI where manual ticketing and request processes stand in the way of developer productivity.

DevOps teams need to move fast, and many aren't all that concerned about where certificates are issued from and what policies they comply with, so long as developers have what they need to keep moving forward at speed. Faced with this primary concern, many DevOps teams have started to issue their own digital certificates, creating numerous blind spots for their security counterparts and leaving their solutions open to risk. Consider the following:

DEVOPS TEAMS...

- Want to avoid time-consuming, manual certificate request processes
- So they issue their own certificates through unauthorized or "DIY" Certificate Authorities that are often built into DevOps and cloud tools
- Which leads to many non-compliant (and sometimes self-signed) certificates as well as a failure to properly track certificates and their expirations

THIS LEADS TO SECURITY TEAMS...

- Having limited visibility into the certificates that get issued
- Losing control over the PKI and struggling to enforce consistent enterprise policies
- Constantly chasing down non-compliant certificates
- Not having accountability when something goes wrong, such as an expired certificate that breaks functionality within an application

As a result of situations like this, serious gaps exist between DevOps and security teams. In particular, this creates four major areas for concern:

01 | SPEED

Traditional PKI involves manual and slow-moving request processes for digital certificates and overall lifecycle management. However, DevOps teams need to avoid this time-consuming process so as not to slow down delivery timelines.

DevOps teams use workarounds to issue their own digital certificates, largely through cloud-native and open-source tools. This approach gives DevOps the speed they need, but often circumvents the security team and enterprise PKI policies.

02 | VISIBILITY

Security teams require visibility into all certificates to run a best practice PKI program. This visibility allows them to ensure all certificates are consistent and issued only from a trusted and authorized PKI. Additionally, it allows the security team to manage certificates throughout their lifecycle by tracking things like Certificate Revocation Lists and expiration dates.

In the current environment, security has lost significant visibility into certificates. In some cases, security teams don't even know DevOps are issuing their own certificates, which curbs visibility entirely. But even in cases where security teams are aware that DevOps teams are doing this, many don't have full visibility into all of the certificates being issued.

© 2020 Keyfactor | All Rights Reserved | www.keyfactor.com

03 | POLICY ENFORCEMENT

Security teams set policies for digital certificates to meet certain security standards consistently across the enterprise. Enforcing these policies — such as algorithms, key lengths and issuing CAs — is essential to delivering on security commitments to employees and customers.

When DevOps teams issue certificates out-of-band, many fail to comply with security policies. And the fact that security teams have little-to-no visibility into these certificates makes it impossible for them to enforce those policies. One of the biggest issues that has cropped up around policy enforcement is the rise of self-signed certificates.

Digital certificates come from a Certificate Authority (CA), which should be trusted by the organization. Think of certificates and CAs like the driver's licenses and DMVs of the digital world. We trust identities on a driver's license because we know the strict requirements DMVs put into place to issue those IDs. A self-signed certificate is akin to a fake driver's license, as there is no trusted third party to verify the information, so the information can be anything the recipient (who is also the issuer) wants it to be — even if it's not true.

04 | ACCOUNTABILITY

When something goes wrong, someone needs to be held accountable. However, the current shadow environment in which DevOps teams circumvent security teams to issue their own certificates leaves no one accountable. DevOps teams can't be held accountable because they're not responsible for security; but security teams can't be held accountable because the certificates were issued without them knowing and without them having visibility to enforce policies.

A prime example of where this creates major challenges today is certificate expirations. When certificates expire they are no longer valid. This means that if an application requires certain technologies to communicate and a certificate is necessary for that communication to happen under enterprise security policies, if the certificate expires, the communication will fail and the application will stop working. When there is no accountability for the certificate, no one is looking out for expirations and this scenario is more likely to happen.

THE WAY FORWARD:

How to Bridge the Divide Between DevOps and Security

The situation of DevOps circumventing security and issuing their own certificates has created enormous problems. In fact, most security teams don't fully know how many certificates have been issued, let alone where they live and when they expire. For example, one organization had 100 self-signed certificates with a lifespan of 10 years — both of which went against the enterprise policy — unbeknownst to the security team. Fortunately, security teams are now realizing what's happened and starting to grasp the extent of this challenge.

So how do we bridge the gaps that exist between the DevOps teams who want to move fast and the security teams who need more visibility and control? Satisfying both speed and security simultaneously requires five key capabilities:

01 | VISIBILITY FOR SECURITY TEAMS

Security teams need a solution that can provide complete visibility into all certificates within the organization. Critically, security teams need more than a network scan that captures certificates at a point in time. Rather, this visibility should provide a real-time view of certificate inventories including details about where certificates live, who issued them and when they expire. That requires end-to-end visibility and direct integrations to both the CAs that issue the certificates and the end-devices and applications that consume them.

This visibility is essential for security teams to be able to consistently enforce policies to maintain security standards. It also gives security teams the insight they need to proactively avoid issues with compromised or expired certificates, which helps create accountability.

02 | SELF-SERVICE OPTIONS FOR DEVELOPERS

The process of getting new certificates must be easy and accessible for developers, otherwise they're likely not to follow it and continue issuing their own certificates outside of the security team's protocols. The best way to meet this need is to establish a self-service model for certificates that fits into the diverse toolsets that developers use today.

Specifically, introducing a PKI solution that provides easy-to-use APIs and interfaces for quick, easy certificate enrollment and can plug into the back-end of solutions that developers already use, like HashiCorp Vault, Kubernetes and AWS, satisfies both sides. For developers, everything appears to be business as usual as they continue to use the same tools and issue their own certificates in moments of need. But for security teams, it's a big change. Although the front-end experience might appear the same for developers, the back-end is governed by the security team's PKI solution, meaning the certificates developers issue are compliant with the organization's policies and the security team has full visibility and control over issuance processes.

03 | AUTOMATION TO STREAMLINE CERTIFICATE MANAGEMENT

End-to-end automation of all certificate-related tasks, from request intake to issuance, provisioning, installation and renewal, provides enormous benefits to DevOps and security teams alike.

For DevOps teams, this automation ensures that anything certificate-related requires minimal to no effort and won't slow them down as they work against tight timelines to deliver features and applications to market. For security teams, this automation not only ensures that they can help developers at the necessary speed (which protects against DevOps teams creating shadow processes), but it also streamlines processes across the organization to make best practice certificate lifecycle management across hundreds of thousands of certificates far easier and more efficient.

04 | POLICY CONTROL FOR SECURITY TEAMS

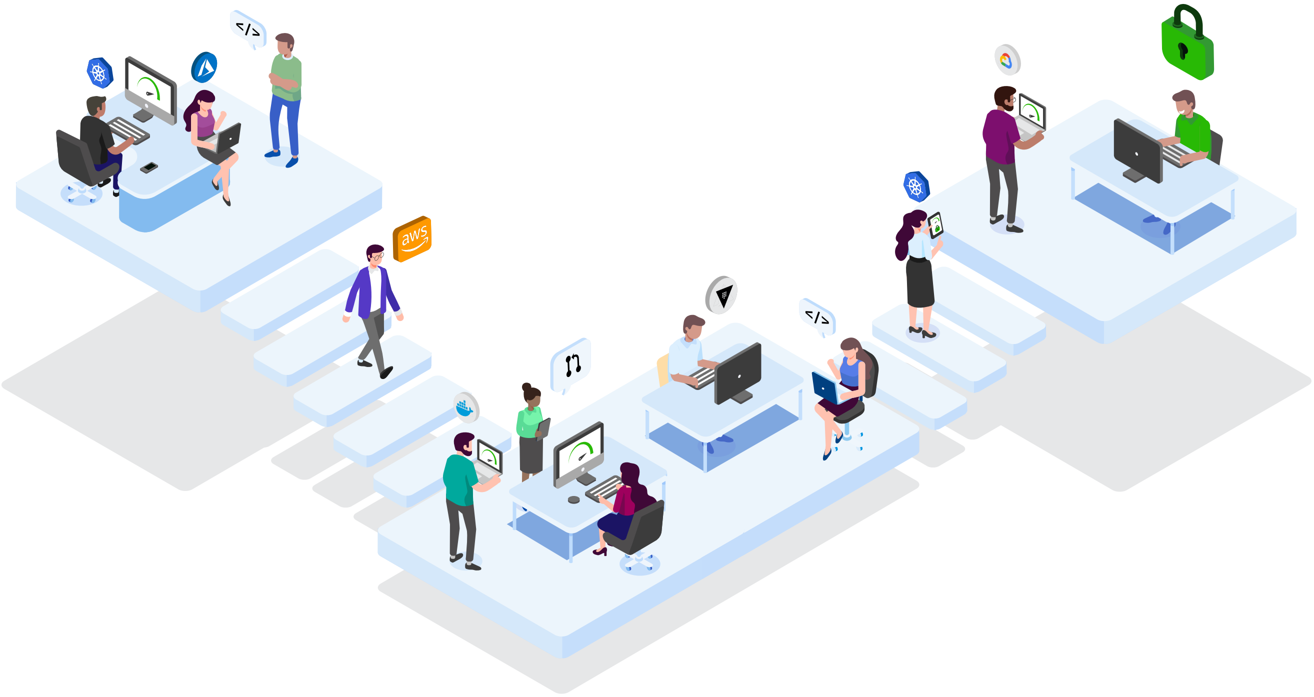
Once security teams have visibility into all certificates and DevOps teams are using certificates issued through the appropriate channels, it paves the way for the necessary policy control. Security teams can then enforce consistent policy and governance across all CAs and tools throughout the organization and effectively monitor and report on certificates to manage, revoke and reissue as needed. Of course automating certificate management makes all of this even more scalable for security teams.

This type of policy control is essential for security teams to meet the standards they set forth for the organization to protect sensitive data. It also ensures that accountability sits with the security team, which is important for driving proactive protection and understanding responsibilities.

05 | SCALABILITY TO MOVE AT THE NECESSARY SPEED

Finally, all certificate-related processes must be scalable to move at the speed of DevOps. Today, this can mean moving as fast as issuing and renewing thousands of certificates per second. This speed is critical, as it's the only way to ensure DevOps teams consistently follow procedure and issue compliant certificates every time rather than using shadow processes.

Two of the most important capabilities for meeting this scalability imperative are automating end-to-end certificate management, which helps increase speed (with accuracy), and introducing self-service options for developers by plugging in PKI systems to the back-end of their DevOps tools, which maintains the status quo for DevOps teams and guarantees they have access to certificates when they need them.



© 2020 Keyfactor | All Rights Reserved | www.keyfactor.com

SUCCESS IS POSSIBLE:

How One Organization's DevOps and Security Teams Collaborate

Despite the challenges that exist today, bridging the gaps between DevOps and security teams is possible. Success starts with ensuring visibility, introducing self-service options, automating certificate management, establishing policy guardrails and guaranteeing scalability. That's exactly how one large financial organization made it happen.

THE CHALLENGE: MITIGATING RISK BY ADHERING TO SECURITY POLICIES WITHOUT SACRIFICING SPEED

The organization's security team recently discovered that the DevOps team was not only circumventing processes in order to issue their own certificates, but also not adhering to policies by issuing self-signed certificates. At first, the security team gave the DevOps team an exception to proceed. However, this exception created significant risk, so they began searching for a solution that would satisfy the needs of the DevOps team without sacrificing the necessary level of protection.

THE SOLUTION: AUTOMATING CERTIFICATE LIFECYCLE MANAGEMENT TO MARRY SPEED AND SECURITY

To find a solution, the security team sat down with the DevOps team so that each side could understand the other's needs as they worked to develop a policy that would satisfy everyone. The DevOps team understood the importance of security controls, but also needed to maintain the ability to issue new certificates at the same speed and through the same programs so as not to break their existing architecture. Meanwhile, the security team needed a way to ensure new certificates would get issued from the correct root CA and to maintain visibility into all certificates.

Ultimately, the two teams landed on a solution that created a perfect marriage between speed and security: The ability to keep the front-end experience the same for the DevOps team while having the back-end certificate issuance and management controlled by the security team through Keyfactor.

Altogether, this solution has satisfied the DevOps team, because it maintains their ability to issue certificates used in production environments, while also satisfying the security team by ensuring that those certificates get issued from a trusted environment, introducing a standardized approach to certificate lifecycle management and providing the necessary level of visibility.

THE RESULT: SECURITY DELIVERED AT SPEED

The visibility, policy enforcement, orchestration and extensibility made possible by Keyfactor have helped the financial organization's DevOps and security teams introduce a approach that satisfies both their needs. Specifically, Keyfactor's cloud-hosted PKI service takes an API-first approach, which makes it highly available and extensible. This availability and extensibility makes it easy to plug into the DevOps team's existing architecture so that they can use the same tools and processes without interruption.

Despite this feeling of "business as usual" on the front-end for developers, quite a lot changed on the back-end for the security team. Keyfactor provided visibility and control while delivering on the need for speed. It did so through:

- Certificate Lifecycle Automation, which enables fast and secure delivery of certificates to any point in the DevOps environment and allows security teams to quickly discover, manage and automate the lifecycle of keys and certificates to ensure end-to-end policy.
- Secure Code Signing, which allows developers to sign any unit of code, at any stage in the CI/CD pipeline, from wherever they are while keeping keys protected in a secure vault or HSM. It also enables security teams to track and monitor every code-signing action and control access to keys to ensure that only the right developer signs the right code.
- PKI as-a-Service, which allows security teams to focus less time and effort on backend PKI maintenance, and more on enabling new use cases. Using a dedicated, cloud-hosted PKI provides a self-service backend for the security team, while they can deliver a self-service front-end to developers. It's a win-win.

KEYFACTOR

Conclusion

Right now, significant gaps exist between DevOps and security teams as they struggle to move quickly while maintaining security. Despite the difficulties of satisfying both speed and security simultaneously, it is possible to achieve both without making any sacrifices.

The key to bridging this divide without sacrificing speed or security is to introduce back-end controls for certificates that get issued through DevOps tools. This approach allows DevOps teams to move as quickly as they need to without changing their existing architecture, since they can continue to issue and use certificates in the same way they have been. But on the back-end, it gives security teams visibility into every certificate that gets issued to enforce policies and ensure accountability. And with automated certificate lifecycle management, the security team can automatically renew certificates as they expire to help ensure nothing breaks and to manage certificates with the necessary speed.

Security teams should take the lead on partnering with DevOps to introduce this type of solution, emphasizing that all of these security controls can sit alongside existing workflows. When that happens and the two teams align, DevOps can go as fast as they need to without taking actions that put the organization at risk.

Using HashiCorp Vault?

Learn about how Keyfactor Command and HashiCorp Vault together deliver a seamless, scalable and compliant PKI as-a-Service to secure your multi-cloud operations. DevOps teams move fast, while Security stays in control.

View Now ▶

KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the impact that breaches, outages and failed audits from mismanaged digital certificates and keys have on brand loyalty and the bottom line. Powered by an award-winning PKI as-a-service platform for certificate lifecycle automation and IoT device security, IT and InfoSec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale. Exceptional products and a white-glove customer experience for its 500+ global customers have earned Keyfactor a 98.5% retention rate and a 99% support satisfaction rate.

Learn more at **keyfactor.com**

CONTACT US

- www.keyfactor.com
- +1.216.785.2990