# MINIMIZE SECURITY RISKS BY KNOWING WHAT IS PROTECTED

With the ever-growing number of internet-connected devices, enterprises must now secure communications between a multitude of devices and their end users. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates provide a layer of encryption between sites to prevent intruders from acquiring sensitive information such as user IDs, passwords, and credit card data.

While SSL/TLS certificates are key to managing security, they present a significant logistical challenge. Each certificate has its own activation, expiration, and renewal date, which forces enterprises to manage thousands, if not millions, of individual checkpoints to ensure every device and application is protected.

Unfortunately, many IT operations and security teams are still tracking their enterprise-wide list of security certificates using spreadsheets or other manual methods. In many cases, this results in losing track of each certificate's location and renewal date, which leads to unplanned expirations and increased security risks.

According to Tag Cyber's *2021 Security Annual*, "74 percent of IT and security experts believe their organization does not know how many keys and certificates they have, much less where to find them when they expire."

## So, how do you know what is being protected?

BMC Helix Discovery's software-as-a-service (SaaS)-based, agentless discovery and dependency modeling solution helps IT teams discover security certificates on all of their assets and applications. Within minutes, security professionals can obtain an up-to-date list of security certificates and their expiration dates across cloud-native or on-premises environments.

With an accurate assessment of the security landscape, IT teams can manage each certificate's lifecycle and help their organizations maintain a high level of security across the entire infrastructure. This single view of certificate information also makes it easy to proactively plan certificate refreshes and prevent service interruptions.

## How does it work?

While performing a deep scan within your operating system, BMC Helix Discovery identifies all of the software instances running on each secure socket. It then establishes a connection with each socket to obtain the details on every security certificate in use—across web and application server environments and applications running on-premises or on the cloud.

In the case of network devices, BMC Helix Discovery performs a Simple Network Management Protocol (SNMP) query to obtain the list of virtual servers that are using SSL profiles. It then makes API calls to collect the information about each respective TLS certificate. BMC Helix Discovery also integrates with native cloud services such as Amazon Certificate Manager (ACM) to obtain the list of certificates managed by the ACM service.

Once the certificate information is collected, BMC Helix Discovery automatically stores certificate information in its central datastore, which can be used for queries and post-processing. For organizations that consolidate and maintain their inventory information using BMC Helix Discovery's out-of-the-box CMDB sync, these certificate details are automatically updated into the CMDB.

Using BMC Helix Discovery's certificate dashboard and reporting features, IT professionals can observe the software and the node on which each certificate is installed. End users can also obtain detailed information about each certificate's lifecycle such as its location, organization, encryption type, validity dates, and IP host. Having easily accessible, up-to-date information gives organizations the ability to understand the potential impact of each certificate's status so they can plan and prioritize refreshes while maintaining high performance and availability.

## Increase your security landscape

By properly monitoring and managing their SSL/TLS certificates, IT organizations can :

- Minimize risk
- Avoid unplanned expirations
- Strengthen data security and encryption
- Protect customer data
- Increase productivity
- Offer secure, safe online experiences

BMC Helix Discovery's SaaS-based, agentless asset discovery and dependency modeling solution helps IT organizations easily track the latest certificate status across the infrastructure. This puts organizations in an ideal position to proactively plan certificate refreshes; prevent service downtime; build trust; and protect their business, brand, and customers.

Visit the BMC Helix Discovery webpage to learn more.