Killing Two Regulatory Birds with One Stone

Regional US Insurance Company

Regulations and compliance requirements can be driven by a number of sources, including the Federal Government, industry associations, customers, or internal standards. In the Insurance industry, the driver is almost always State government. The Network Administrator at a regional insurance company in the Northeast knows this all too well. As he explains, "We have operations in Massachusetts and Connecticut, so we have two sets of compliance requirements to fulfill."

Fortunately for this and other STEALTHbits customers, InfoSec compliance requirements are fairly similar across states and regulatory bodies. Added the Insurance Company's Administrator, "Proving that we know who has access to data - especially sensitive data - and that we proactively monitor that access is critical to all the regulators. I'm not sure how we did it before we deployed STEALTHbits."

The Company uses the StealthAUDIT Management Platform to generate reports required by auditors that detail who has access to what data, and demonstrate that access has been revoked when employees leave the company or change roles. In one case, data required by auditors was not available in an out-of-the-box StealthAUDIT report, and the Administrator was especially impressed with STEALTHbits' corporate flexibility and open architecture: "STEALTHbits really stepped up to the plate and found a way for us to engineer a report that we could easily generate to satisfy auditors."

Additionally, StealthAUDIT's value extends beyond compliance reports. In a recent example, a senior-level Administrator left the Company, and his account credentials were used in a number of production SQL query applications. Understandably, the Company's IT administrators were concerned about deprovisioning his credentials without disabling critical production processes. Using StealthAUDIT, the Company was able to identify where the former Administrator was granted and using access, substantially reducing the operational risk of deprovisioning his account.

In Brief:

- Regional Insurance Company

- Subject to Massachusetts and Connecticut Insurance Regulations

- Using StealthAUDIT for compliance reporting and StealthINTERCEPT to monitor Active Directory changes

Quotes:

- "One of the easiest ways to know if you've been hacked is to look for the creation of an Admin Account that gives itself access to everything. That can't happen without our knowledge thanks to StealthINTERCEPT."

- "Proving that we know who has access to data - especially sensitive data - and that we proactively monitor that access is critical to all the regulators. I'm not sure how we did it..."

STEALTHbits
T E C H N O L O G I E S

In addition to StealthAUDIT, they've also deployed STEALTHbits' real-time threat detection product to monitor Active Directory changes to enhance overall security and network health. The Company has StealthINTERCEPT configured to generate an alert every time a significant change is made in Active Directory. Explains the Network Administrator, "One of the easiest ways to know if you've been hacked is to look for the creation of an Admin Account that gives itself access to everything. That can't happen without our knowledge thanks to StealthINTERCEPT."

About STEALTHbits Technologies

STEALTHbits Technologies is a data security software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.

Identify threats. Secure data. Reduce risk.

Quotes (continued):

...before we deployed STEALTHbits."

- "STEALTHbits really stepped up to the plate and found a way for us to engineer a report that we could easily generate to satisfy auditors."

Identify Threats. Secure data. Reduce risk.

STEALTHbits
T E C H N O L O G I E S