FirmGuard

Financial Institution Uses FirmGuard SecureWipe to Prevent Data Breach After Executive Laptop is Stolen

Introduction

The Infrastructure and Operations department (I&O) of a regional financial services company recently adopted FirmGuard as part of their security stack. Recognizing BIOS security as a vulnerable layer in their endpoint protection strategy, they sought a solution that would ensure firmware integrity across the entire company. The decision was driven by SecureUpdate, which simplified the previously inconsistent and complex process of updating BIOS firmware. Before FirmGuard, BIOS updates were sporadic, often left undone due to the difficulty of managing the process at scale. With SecureUpdate, the I&O team could automate and streamline updates, improving both security and compliance.

> **Without SecureWipe I am not sure what we would have done; I don't want to think about it.**
>
> *- Director of I&O Department*

Additionally, the I&O team had started using SecureWipe internally, aiming to replace a costly and cumbersome legacy procedure which involved shipping endpoints and physical destruction of machines. SecureWipe greatly simplified the procedure and offered measurable cost savings. A key component of SecureWipe was the Certificate of Erasure (CoE), which provided the necessary audit trail for regulatory compliance when decommissioning sensitive systems. As the I&O team familiarized themselves with SecureWipe, they had not anticipated the novel use case that was about to unfold.

SUMMARY

A regional financial services company adopted FirmGuard for BIOS security. After an executive's laptop was stolen, the team used SecureWipe to remotely erase sensitive data, ensuring compliance and avoiding regulatory penalties. This incident proved FirmGuard's value, solidifying its role in their IT infrastructure.

KEY CHALLENGES

+ Remotely erasing the hard drive of an executive's stolen laptop
+ Improving corporate endpoint security posture to include BIOS security
+ Providing security reports, including Certificate of Erasure (CoE), to financial regulators

PRODUCT/FEATURE USED

+ SecureWipe
+ SecureUpdate
+ SecureCheck
+ SecureConfig
+ SecureSense
+ SecureBeat

A Stolen Laptop Sparks a Security Crisis

One morning, the I&O department received a frantic call—an Executive Vice President's laptop had been stolen in a "smash and grab" robbery. While he was at dinner with a client, a thief had broken into the trunk of his car and taken the device. The laptop contained sensitive financial data, prompting the Director of I&O to immediately inform the Chief Security and Compliance Officer (CSCO). Losing an asset with financial data—especially one belonging to a senior executive—triggered regulatory obligations that could lead to unwanted scrutiny, fines, and potential reputational damage.

FirmGuard

Certificate of Erasure

This document is provided to ACME Corporation to certify that the Phoenix® SecureWipe™ program executed the erasure method(s) on the material(s) listed on the form below.

Data Erasure Performed By: FirmGuard SecureWipe
Endpoint Computer Name: DELL-LAT-3520-2
Endpoint Model: Latitude 3520
Time Issued: 08/14/2024 | 20:30 UTC
Time Acknowledged: 08/14/2024 | 20:30 UTC
Performed By: John Smith (johnsmith)

Drive	Erase Method	Serial Number	Size
HITACHI HTS725050A7E630	Single Pass Zeros	TF1500Y9GX9BTB	536.99 GB

SAMPLE

Any Certificate of Erasure provided via the FirmGuard® platform is subject to the Terms and Conditions, and other policies, of the FirmGuard® platform and the SecureWipe FirmGuard® module found at www.firmguard.com or successor website as of the date listed above ("Policies"). Phoenix Technologies does not make any representation or warranty of any kind regarding the completeness of any erasure or destruction beyond those explicitly recited in the Policies.

SecureWipe™ is designed to assist organizations in meeting compliance requirements related to data sanitization and protection, including but not limited to: ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, NIST SP 800-88, NIST Cybersecurity Framework, GDPR, HIPAA Security Rule 45 CFR 164.310(d)(2), PCI DSS, DoD 5220.22-M, and FISMA. Users are responsible for ensuring full compliance with these standards.

phoenix technologies
2105 S. Bascom Avenue,
Suite 316 Campbell, CA 95008.3295

After each SecureWipe, a Certificate of Erasure (CoE) is produced and stored in the portal to document the details of the wipe. A CoE can be crucial for compliance with data protection regulations and standards like NIST, ISO, HIPAA, or CMMC, as it serves as proof that sensitive data has been handled appropriately and securely destroyed.

The Director of I&O understood the gravity of the situation and huddled with his team. They decided to try and erase the stolen laptop remotely using SecureWipe. The FirmGuard admin was instructed to issue a wipe command, even though the stolen laptop was offline. For several hours, the team monitored its status—until suddenly, it came online. Presumably, the thief had powered it up, and as expected, it automatically connected to FirmGuard. The wipe command was executed, erasing the laptop's entire contents within minutes. A Certificate of Erasure (CoE) was then generated, providing verifiable proof that the data had been securely removed.

> **I cannot overstate how important the SecureWipe CoE was for the financial regulators. It made all the difference for us.**
>
> *- Chief Security and Compliance Officer (CSCO)*

Regulatory Compliance and Avoiding Reputational Damage

Everyone breathed a sigh of relief that a crisis had been averted. The CSCO promptly reported the incident to financial regulators, submitting the CoE as verification that the data had been securely erased. After a thorough review, regulators determined that no fines would be issued due to the limited exposure of personally identifiable information (PII) and that no public disclosure was required, sparing the company from reputational harm. What could have been a major security crisis was neutralized—swift action, combined with FirmGuard's capabilities, ensured compliance and mitigated risk.

A Worthwhile Investment

This single use of SecureWipe paid for the price of FirmGuard many times over. The company hadn't considered remote disk erasure a critical part of their overall security strategy, but this incident convinced them that it is indispensable. FirmGuard had mitigated a potential data breach and ensured compliance, all with the click of a few buttons. FirmGuard is now firmly entrenched as a key part of the IT infrastructure and hopefully they never have an incident like this again, but if they do, they know exactly how to respond.

phoenix technologies
2105 S. Bascom Avenue, Suite 316
Campbell, CA 95008.3295
Toll Free: 1.800.677.7305
Tel: +1.408.570.1000
phoenix.com