Comprehensive Server Restoration with Hewlett Packard Enterprise

HPE delivers industry-leading security and recovery capabilities in its ProLiant Gen10 portfolio

Summary

The proliferation of cyberattacks alarms every enterprise and government worldwide. Nation states attack government IT infrastructure to disable systems and paralyze national security efforts. Sophisticated hackers attack corporate entities to steal intellectual property (IP), steal customer data or hold information for ransom.

Distributed denial of service (DDoS) and other traditional attack vectors are quickly giving way to more insidious means. More than 91 percent of ransomware attacks come via email attachments.[1] Organizations of all sizes seem to recognize this, since more than $10 billion annually will be spent on security training for employees.[2] Yet despite all this focus, ransomware attacks have gone up 15 times in just two years and by next year, a company will be infected with ransomware every 14 seconds.[3] More broadly, the total cost of cyber security to the global economy will balloon to $6 trillion by 2021 and $8 trillion by 2022.[4]

The question isn't "if" your datacenter is going to be attacked, but "when." While a penetration into IT infrastructure may be inevitable, suffering from a breach is completely avoidable. The question businesses of all sizes should be asking themselves is, "How quickly can my IT organization detect, isolate and remove malware; restore infrastructure to a known good state; and re-install operating systems, applications and data?" According to a study by Accenture, the average ransomware attack time to recovery is 23 days. The average cost? $2.4 million. When a large shipping company recently fell victim to the NotPetya cyber-attack, it had to restore over 4,000 servers and 45,000 PCs in 10 days.[5] This effort included wiping each server and PC clean. It then required reinstalling operating systems and over 2,500 applications, with all the associated data.[5] While the company didn't publicly attribute a cost to recovery efforts, the total damage estimate was approximately $300 million.[6]

1-4: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
5: https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/
6: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

Cybersecurity is a multidimensional challenge that requires a multidimensional response. Moor Insights & Strategy believes IT organizations would be well-served to consider comprehensive security as a bare minimum requirement when investing in server infrastructure. Silicon rooted security, complemented by tools that enable fast time to recovery, should be a must for any server that gets installed and connected in any datacenter. Tools like Hewlett Packard Enterprise's Server System Restore should be considered to drive fast time to recovery. In fact, MI&S has not seen a more comprehensive server recovery tool in the market.

ANATOMY OF AN ATTACK

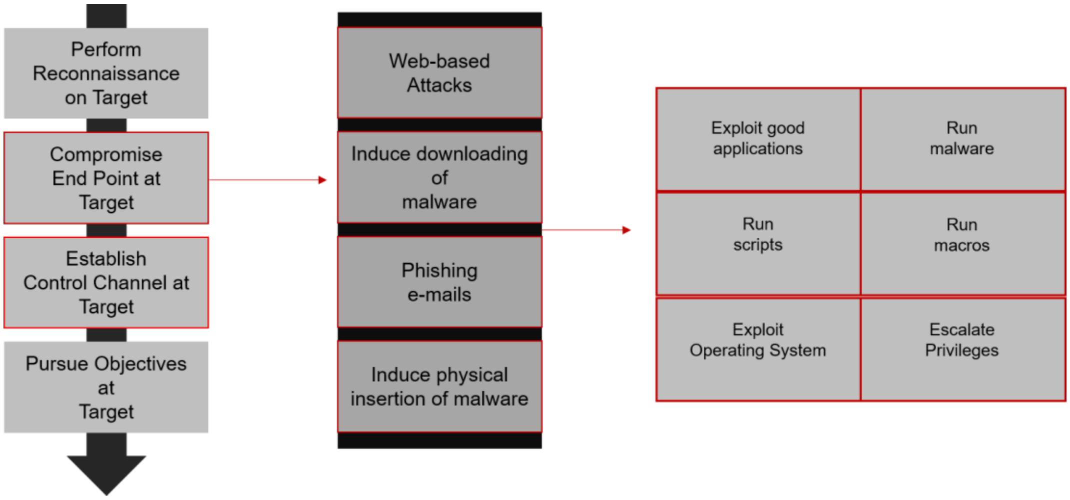
Cyber-attacks against datacenters have evolved considerably. Bad actors have figured out that there is no need to breach the perimeter as long as there's a human on the other end of an email chain. The largest breaches recorded are the result of people being people. A USB stick left on the ground of a parking lot outside a building on a US military base in Afghanistan led to the largest compromise of US military computers in history and took 14 months to recover.[7] A password handwritten and left for anybody to see led to the infamous breach of Target in 2013.[8] And passwords stored in the clear on GitHub led to the breach of Uber in 2016.[9]

The process of attacking an organization can be broken into four distinct phases:

- *Perform reconnaissance* – Identify the target. Look for obvious weaknesses to exploit. Plan the attack (DDoS, phishing email, etc.).
- *Breach* – Send the phishing email. Insert the malware via USB or other means. Execute DDoS attack.
- *Gain a control plane/channel* – Inject malware into the environment through a number of means.
- *Execute plan* – Download. Encrypt. Erase. Distort.

7-9: Statements by James Morrison, a Computer Scientist with the Federal Bureau of Investigations, June, 2017

FIGURE 1: THE PHASES OF A CYBER ATTACK


Perform Reconnaissance on Target
Compromise End Point at Target
Establish Control Channel at Target
Pursue Objectives at Target
Web-based Attacks
Induce downloading of malware
Phishing e-mails
Induce physical insertion of malware
Exploit good applications
Run malware
Run scripts
Run macros
Exploit Operating System
Escalate Privileges

Source: Moor Insights & Strategy

If this all sounds a little militaristic, it's because it is. Attacks against government and corporate entities are anything but random. Nation states are the originators of many of the hacking tools in existence. And, in fact, those nations are often the perpetrators. Also consider the amount of money at stake. As mentioned previously, cyberattacks will cost the global economy about $6 trillion in 2021, which is one-third the GDP of the United States and larger than the entire global illegal drug trade.

Bootkit and *firmware* attacks are perhaps the most insidious. These attacks allow for bad actors to gain access to a server below the OS layer. This level of access allows for malware to remain present, yet virtually undetectable to even modern security technologies deployed in the datacenter. Firmware attacks are also the most difficult to combat, and the most likely to remain undetected −averaging 99 days before being discovered.

As difficult as it is to maintain control over server firmware in the enterprise, IT organizations are ill prepared. In a study by the Information Systems Audit and Control Association (ISACA), only 8 percent of enterprises had adequate measures in place to control and manage the firmware in their environment.

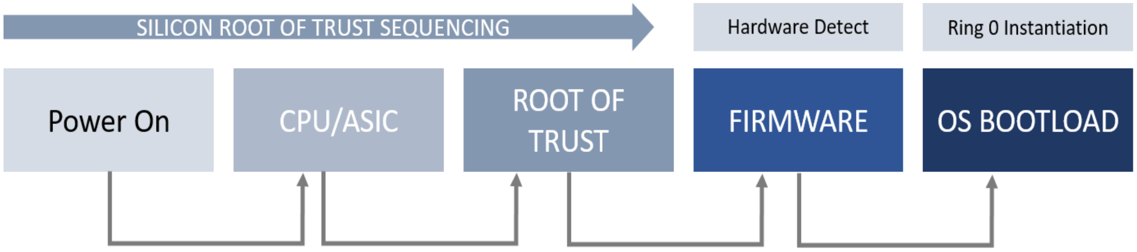
PROTECTING AGAINST ATTACKS

While there is no "silver bullet" for protecting your datacenter, MI&S has found some server platforms employing security mechanisms that offer high levels of protection. One of these is the Gen10 ProLiant server portfolio from Hewlett Packard Enterprise.

HPE's silicon root of trust provides protection as soon as the server is powered on and the Integrated Lights Out (iLO) firmware comes alive. As the server initializes, its firmware is compared against an immutable fingerprint stored in iLO 5 to verify that all the firmware code is valid and uncompromised.

If any malware or compromised code has been inserted in the iLO 5 firmware UEFI System ROM, the silicon will detect it as the infected firmware code would be altered and, therefore, would not match-up (with the hash burned into the silicon). UEFI then validates the connection to the operating system through secure boot, thus completing a complete root, or chain, that is anchored in the silicon. Other server essential firmware is also validated, to include the CPLD, M.E., I.E. and Option ROM, thus completing the verification of almost 4 million lines of firmware code.

FIGURE 2: HEWLETT PACKARD ENTERPRISE SILICON ROOT OF TRUST



Source: Moor Insights & Strategy

Put more simply, HPE's silicon root of trust creates an immutable fingerprint that is used to validate firmware. Changes to firmware are quickly identified, enabling IT organizations to more quickly respond to firmware attacks.

RECOVERING FROM ATTACKS

Recovery time objective (RTO), work recovery time (WRT), maximum tolerable downtime (MTD) are terms with which most IT professionals are familiar. These terms help define an organization's tolerance for downtime in disaster recovery scenarios. Most disaster recovery (DR) plans were created prior to the real threat of cyberattacks and — as a result — are incomplete. Recoveries from cyberattacks have traditionally been messy. In essence, servers must be rebuilt from firmware to operating systems to applications and to data. In an enterprise environment, this task can seem impossible, even with the configuration management tools available from most server vendors. These tools tend to lack the integration and secure handshakes to ensure a complete and timely recovery that will not reintroduce malware into an environment from which it was just removed.

Moor Insights & Strategy believes there are three things IT organizations should require from the recovery tools employed.

- ***Security -*** Scouring 5,000 servers of malware only to reintroduce that malware when reinstalling an operating system is a real problem experienced by enterprise IT organizations. A secure "handshake" from firmware recovery to the repository that holds ISO images, applications and data is an absolute must.
- ***Scalability -*** Look for recovery tools that can restore the datacenter at scale. The shipping company took 10 days to restore 4,000 servers, which is impressive, but the downtime cost approximately $200 million. The ability to restore those 4,000 servers in parallel would greatly reduce the financial impact.
- ***Simplicity –*** As the role between IT and business continues to blur, the tools used in the restoration of servers must provide near single click restoration capability. A comprehensive tool that that lacks usability is a comprehensive tool that will lack use.

IT organizations would ideally deploy a tightly integrated cybersecurity platform. Or, at the very least, they should deploy tools that share DNA. Meaning, the tools used to protect an environment reside in the same technology portfolio of those tools used to recover from cyberattacks. This ensures the tightest levels of integration and should lead to the most complete solution.

HPE SERVER SYSTEM RESTORE

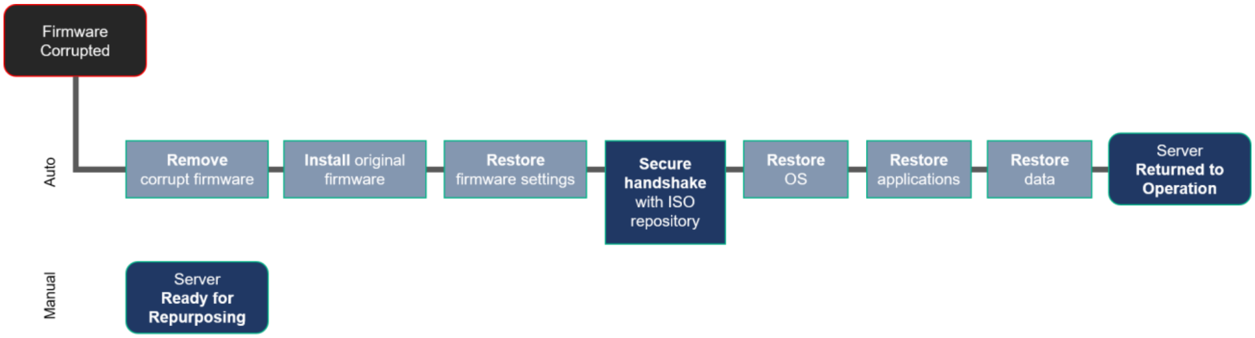
Server System Restore is a feature in Hewlett Packard Enterprise's iLO Amplifier Pack. It securely delivers automatic server restoration to up to 10,000 servers with a single click.[10] What makes this feature uniquely powerful is its ability to manage cyber incidents so completely for HPE Gen10 servers that have the iLO Advanced Premium Security Edition installed. When a server is detected with corrupt firmware, IT administrators can enable one of three responses:

- ***Auto Restore***:
  - Corrupt firmware is removed.
  - Verified uncompromised server essential firmware is reinstalled

[10] HPE Internal Testing - February 2017

  - Firmware settings are recovered and installed, saving time to manually recreate settings.
  - Secure handshake is established with the ISO repository which prevents corrupt image installation.
  - Facilitation of an OS restoration from an ISO site is completed.
  - Facilitated restoration of applications is accomplished.
  - Recovery of the data from a protected secondary back-up repository.
  - Server is returned to operation.
- ***Manual Restore:***
  - Corrupt firmware is removed
  - Verified uncompromised server firmware is reinstalled.
  - The target server is left in a cleaned state, waiting for the IT professional to take action (e.g. repurpose server)

Figure 3: Server System Restore Options


Firmware Corrupted
Auto
Manual
Remove corrupt firmware
Install original firmware
Restore firmware settings
Secure handshake with ISO repository
Restore OS
Restore applications
Restore data
Server Returned to Operation
Server Ready for Repurposing

Source: Moor Insights & Strategy

At the time of this report, Hewlett Packard Enterprise appears to have the most comprehensive security offering from a major server manufacturer in its Gen 10 lineup. Silicon root of trust-based security can reduce the time it takes to detect firmware attacks dramatically. And Server System Restore delivers on what Moor Insights & Strategy views as critical factors in a restoration process; security, scalability and simplicity. These solutions make up what may be the most secure chain of trust in the server industry.

Call to Action

The world is changing. Deploying three-tiered web applications with a DMZ and firewall is no longer enough to protect the datacenter. The acquisition and use of malware to attack organizations is simpler and more frequent than ever. And affected organizations seem more willing than ever to pay the ransom to a bad actor in exchange for the return of customer data.

Moor Insights & Strategy sees small to mid-size enterprise IT organizations as the richest target for hackers. This is due to the amount of data stored combined with less comprehensive security measures. However, whether you manage a datacenter, a server room or a closet – your data is at risk.

As companies spend tens of billions of dollars on security software, or deploy software defined networking for policy-based management, the lowest levels of hardware are left vulnerable to root kit attacks that can wreak havoc for months before detection.

Moor Insights & Strategy believes companies of all sizes should look to expedite infrastructure modernization projects to better leverage the security features that can offer protection from the silicon up. These new server platforms also provide the hooks for more comprehensive recovery capabilities in response to a cyberattack.

Hewlett Packard Enterprise is the only major server vendor that delivers Silicon Root of Trust and comprehensive recovery through Server System Restore. Because of this, organizations of all sizes should consider deploying HPE iLO 5 Amplifier Pack and iLO Advanced Premium Security Edition.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Matt Kimball, Senior Analyst at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

DISCLOSURES

This paper was commissioned by Hewlett Packard Enterprise (HPE). Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.