Digital Energy
Baseline Security Center Cyber Security Solutions

INTEGRATED TOOLS THAT BOOST SECURITY AND EFFICIENCY IN OT ENVIRONMENTS

To guard against cyber attacks and ensure the continuous availability of critical operational technology (OT) infrastructure, power generators must implement and sustain a growing number of vital security controls. However, with limited budgets and staff, it gets increasingly difficult to contend with these escalating demands. Now there is a clear solution: Baseline Security Center from GE's Digital Energy.

CYBER THREATS IN OT

About half of all CEOs (49%) say that becoming a victim of a cyber attack is now a case of "when," and not "if."[1]

Once a day, the energy sector faces a cyber attack that hasn't been seen before.[2]

46% of all cyber attacks in the OT environment go undetected.[3]

ge.com/power/digitalenergy

CHALLENGES

Today's power generators must guard against continuously evolving, increasingly advanced cyber threats. For the security teams in these organizations, a range of security mechanisms need to be implemented, but that's only the beginning. Threats—and the mechanisms needed to guard against them—evolve rapidly. Therefore, systems need to be tuned, monitored, and managed on a continual basis—and many teams struggle to keep pace with all these ongoing demands.

Further, establishing these security mechanisms doesn't just take time, it takes expertise. The reality is that implementing general purpose security platforms in OT environments can break business-critical plant operations. As a result, even basic security tasks—including managing inventory and identities, collecting and reviewing logs, and updating passwords—don't happen fast enough or at all. Often, it's these fundamental tasks being missed that ultimately proves costly, leaving the business exposed to devastating cyber attacks.

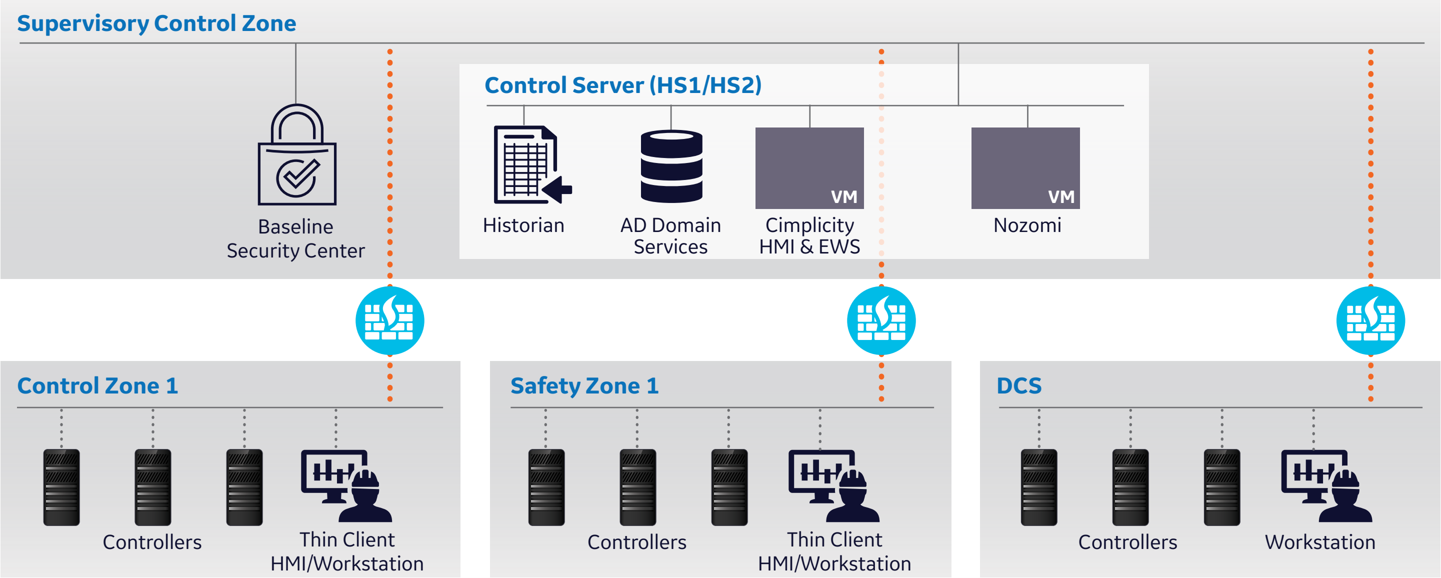
Quite simply, in many organizations, security demands are growing too fast, and time, staff expertise, and money are in too short supply. Given these realities, many decision makers have been faced with two highly unappealing scenarios:

- Make the massive investments of staff time and budgets that are required to build a comprehensive security program from scratch.
- Do nothing, or do the minimum, and hope their organizations aren't exposed by a cyber attack or hit by massive fines for non-compliance.

Now GE's Digital Energy offers a far more appealing alternative.

Baseline Security Center
Cyber Security Solutions

Integrated Tools that Boost Security and Efficiency in OT Environments



Baseline Security Center features a broad range of capabilities and offers efficient integration in OT environments.

Advantages

Baseline Security Center offers the following advantages:

Comprehensive coverage.

Supports integration with a range of operating systems, including various versions of Linux, Windows, and UNIX.

Optimized for plant control and operational technology environments.

Features close alignment with power generators' OT environments, including GE and third-party equipment.

Advanced automation.

Automates patch deployments, configuration policy enforcement, configuration file backup, and more.

Optimized integration.

Delivers applications, services, hardware, and configurations that are pre-integrated, tested, and tuned.

Enhanced flexibility.

Helps customers address near- and long-term needs, featuring a modular approach that enables teams to start small and expand over time. Offers capabilities for feeding information into an enterprise security operations center, so teams can efficiently manage an entire fleet. Supports flexible integration of new technologies.

Solution

Today, GE's Digital Energy offers Baseline Security Center. This solution delivers comprehensive security capabilities in a single, pre-integrated platform, enabling your organization to establish robust, defense-in-depth controls in plant environments.

The solution provides security controls and OT maintenance tools for both GE and non-GE control networks. With Baseline Security Center, you can leverage a full suite of security capabilities—without all the time, cost, and effort of procuring, testing, integrating, and deploying these disparate solutions independently.

Baseline Security Center collects, correlates, and forwards security logs and events, and it presents this information to plant personnel in a highly usable format. The solution offers identity and password management capabilities for control-system environments. In addition, the solution can be customized so it aligns with your existing environment, including your security incident and event management (SIEM) platform, backup mechanisms, anti-virus technologies, log management platforms, and more.

Baseline Security Center represents a complete solution, delivering an integrated platform that offers all these features:

- Hardware appliance and operations console
- Hardened server and thin-client console
- Optional, hardened firewall
- Secure-by-design configuration
- Global regulatory certifications and hardware support

In addition, the solution features applications and services that deliver comprehensive security capabilities, supporting access control, patch management, log aggregation, and much more. The solution offers intelligence reporting for Baseline Security Center servers, and, for assets managed by the solution, it reports on patch availability and vulnerabilities. The solution is backed by complete services and support, including assistance with setup, installation, and integration of workstations and network assets.

Baseline Security Center
Cyber Security Solutions

Integrated Tools that Boost Security and Efficiency in OT Environments

Benefits

By putting Baseline Security Center to work in your organization, you can capitalize on the following benefits:

Maximize cost and staff efficiency.

Baseline Security Center packages and pre-integrates dozens of security technologies—so your teams don't have to. The solution eliminates all the efforts that would be required to procure, integrate, deploy, and maintain these solutions individually. The solution centralizes the management of patches, anti-malware, backup and recovery, and user identities. Further, the solution delivers automation and advanced technology that streamlines ongoing management and maintenance.

Mitigate risk.

With Baseline Security Center, you can gain actionable insights into your OT environment and security posture. You can quickly establish comprehensive security mechanisms that mitigate the risk of cyber attacks and failed compliance audits. The solution can help your team address a broad range of cyber security regulations, standards, and guidelines, including NEI 08-09, NERC CIP, and IEC-62443 (ISA 99).

Optimize availability.

Baseline Security Center helps your team ensure that the security controls implemented are aligned with your operational goals. The solution supports the implementation of maintenance and governance processes that help protect your most critical assets.

Key Capabilities

Identity Management and Access Control

With Baseline Security Center, your organization can establish least-privileged access controls for administrators, which is a central tenet to complying with security best practices and many regulatory mandates. The solution enables your team to establish central management of user identities and role assignments.

Baseline Security Center helps your team create password complexity rules and enforce policies around secure passwords. For example, it enables you to prohibit the use of vendors' default passwords. The solution augments these capabilities by offering certificate services and encryption that secure communications between GE's HMIs and controllers.

Malware Protections

Baseline Security Center features anti-virus capabilities that detect and disrupt malicious code discovered on the network. The solution also offers application whitelist capabilities that help ensure only authorized software runs in the environment.

System Hardening

Baseline Security Center employs a number of hardware and software configurations that make assets more difficult to attack. Baseline Security Center features a hardened appliance with secure-by-design configurations. Based on either an HPE ProLiant DL360 or Dell PowerEdge R430 server, the solution includes mounting hardware, security bezel, and blockers for unused USB and network ports.

Baseline Security Center establishes secure configuration of privileges and implements a least-privileged approach for administrative access. The solution offers a number of configuration management capabilities. The solution collects baseline configurations for managed assets, it creates alarms when configurations are changed, and it automatically corrects unauthorized changes. The configuration management software's agentless deployment streamlines implementation and ongoing administration.

Supporting Windows and Linux operating systems, the solution's host intrusion detection system delivers capabilities for file integrity monitoring, log monitoring, rootkit detection, and active response to alerts.

System Backup and Recovery

Baseline Security Center is fully customizable, so you can effectively adapt it to meet the specific needs of your environment. With the solution, you can leverage your existing technologies and the feature sets integrated within a range of operating system environments. The solution's lightweight deployment requires minimal configuration. The solution automates backup of critical configuration files to support fast, efficient system recovery in the event of system corruption, misconfiguration, or compromise.

Log Aggregation and Security Incident and Event Management (SIEM)

Baseline Security Center includes a SIEM that offers asset and software discovery capabilities and that enables you to do event correlation and logging. The SIEM is configured to monitor your control networks and your Baseline Security Center environment. The solution features customizable dashboards and pre-packaged dashboard views, offering visibility into network traffic, system state, security alarms, and recent events.

Baseline Security Center also offers advanced log aggregation capabilities, providing a centralized system that can aggregate device logs from a range of sources, including event logs in Microsoft Windows-based systems, syslog data and other log formats from Linux-based systems, logs from network devices and embedded systems, and application-level log files. The solution offers customizable dashboards and it enables you to do centralized review, management, reporting, and searching on alerts. In addition, logs can be forwarded to the Baseline Security Center SIEM and third-party SIEMs for event correlation and automated log analysis.

Network Infrastructure Management

Baseline Security Center offers a number of capabilities that support efficient, automated management and maintenance of network equipment, including switches, routers, and firewalls. The solution does automated backup of configuration files, which enables more rapid and efficient recovery from issues and outages.

Patch Validation Program

This optional program offers comprehensive patch management services, covering all the GE assets in the environment that are managed by Baseline Security Center. This program offers testing and validation of anti-virus and host intrusion detection signature updates as well as operating system patches.

Through this program, we deliver patches via a convenient, secure web portal. These patches are delivered in complete, scripted packages that are easy to deploy. Featuring cumulative updates, these packages also help you ensure you're current with the latest releases. Plus, using the Baseline Security Center appliance, you can establish automated, centrally managed deployment of patches.

Intelligence Reporting

On an ongoing basis, GE delivers reports on patch availability and vulnerabilities affecting equipment in scope. Through this reporting, you can gain timely, intuitive insights into your organization's cyber-security posture and its areas of exposure.

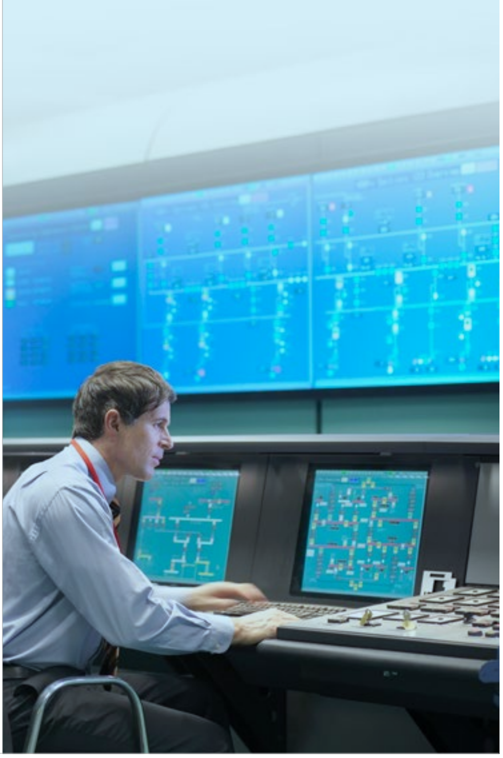
Backed by Extensive Support and a Commitment to Quality

Baseline Security Center is backed by extensive services and support. Our experts will set up the Baseline Security Center system in your environment, performing installation, commissioning, and start up of the included applications and services. We offer your team two days of onsite, hands-on training. We also offer documentation, optional factory acceptance testing, and optional ongoing maintenance.

GE is committed to quality services and support. We employ Six Sigma tools and we empower team members to make customer-focused quality the highest priority. Further, our team participates in a number of external quality certification programs, including ISO-9001:2015 and ISO-27001:2013.

How to Get Started

To learn more and sign up, please contact your local GE's Digital Energy or GE's Power Services Account Executive or call 770-722-2552.



Sources

[1] KPMG International, "Growing Pains: 2018 Global CEO Outlook," May 2018, https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/05/growing-pains.pdf

[2] S&P Global, "Feature: Energy industry faces unprecedented cyber threats almost daily," July 19, 2018, www.spglobal.com/platts/en/market-insights/latest-news/electric-power/071918-feature-energy-industry-faces-unprecedented-cyber-threats-almost-daily

[3] Ponemon Institute LLC, "The State of Cybersecurity in the Oil & Gas Industry: United States," February 2017, www.crc-ics.net/documents/CRC-ICS-2017_Pokemon%20Report-Cyber_Readiness_US_Oil__Gas_2017.pdf

Contact Us
www.gepower.com/contact