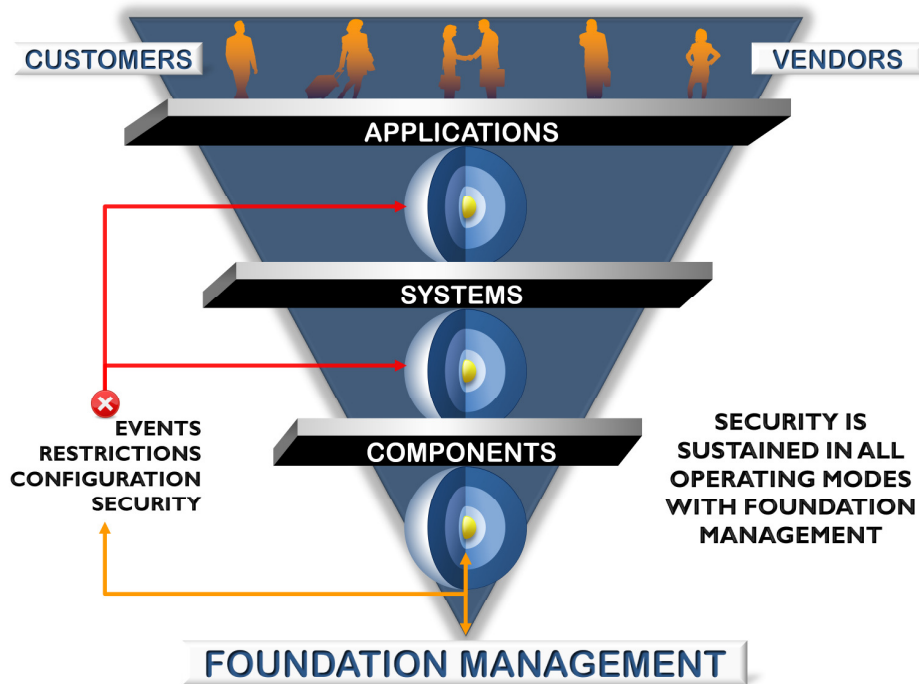




What is Foundation Management Security?

Foundation Management addresses security at all levels of IT infrastructure in a bottom-up approach that encompasses all possible modes of operation.

This is a distinct departure from traditional security practices that are built from a top-down perspective with the assumption that security only applies to the IT infrastructure when that infrastructure is available on the normal network.



Foundation Management builds from the Bottom-up of IT architecture, starting with the high authority, privileged interfaces in the Component layer of IT.

Yet the nature of IT infrastructure presents a challenge to the top-down security model. For example, a security breach at the systems layer automatically compromises the applications layer—and a security breach at the component layer automatically compromises **both** the systems and applications layers.

Foundation Management addresses this security dependency in the IT infrastructure, and its inverted pyramid relationship, thereby addressing a number of security considerations that have been left out of enterprise security models and strategy to date.

FOUNDATION MANAGEMENT FOR SECURITY

What Problems does it Solve?

Security must protect the organization from damage by preventing outsider intrusion and limiting access to sensitive data by insiders. Foundation Management is a key element in this strategy: used to prevent insiders (including outsiders if they get past perimeter defenses) from:

- Gaining access to, altering or destroying sensitive data
- Disruption from improper configuration of components or systems
- Wreaking havoc through insertion of destructive code or programs

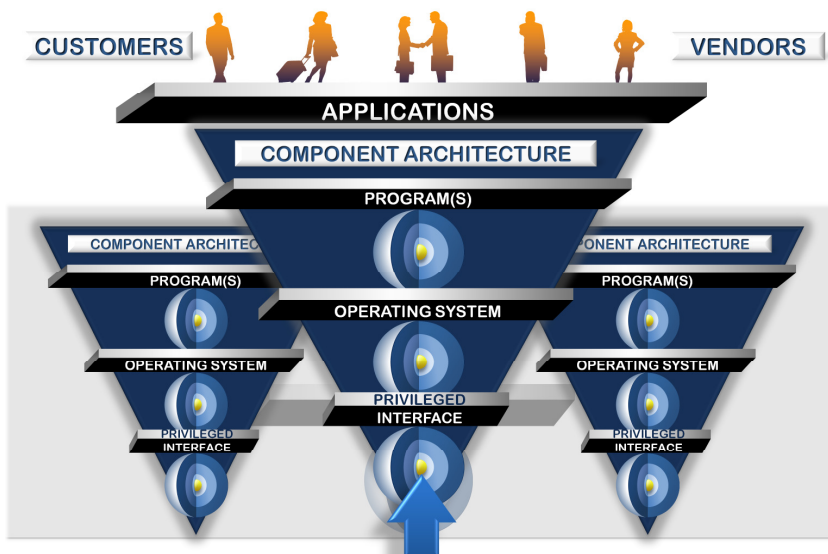
The component layer of IT architecture is the most unsecured and vulnerable part of IT infrastructure. Privileged insiders routinely access the

component layer to configure, repair, and maintain the component and systems layer of the architecture.

These privileged insiders are “trusted” IT experts (internal IT staff, contractors and vendor service technicians) who have access to IT infrastructure at its very foundation through privileged component interfaces that include physical interfaces (baseboard management controllers, privileged serial ports) and software (consoles) to operating systems, virtual machines, etc.

Foundation Management addresses the security gap at the component layer where privileged interfaces are at best managed through manual controls and are, at worst, “secured” by “trusting” the IT experts (internal IT staff, contractors and vendor service technicians) who use them. Foundation Management starts here—where IT infrastructure is most vulnerable to theft, revenge, innocent error and even terrorism. This is the **Insider Threat**.

Foundation Management also augments existing security practices by capturing both device health and security-related events from “gate keeper” security devices including firewalls, intrusion-detection and authentication systems. By monitoring and managing these security “gate keepers,” Foundation Management increases the ability of the organization to detect threats, prevent undesirable actions, and capture security-related records.



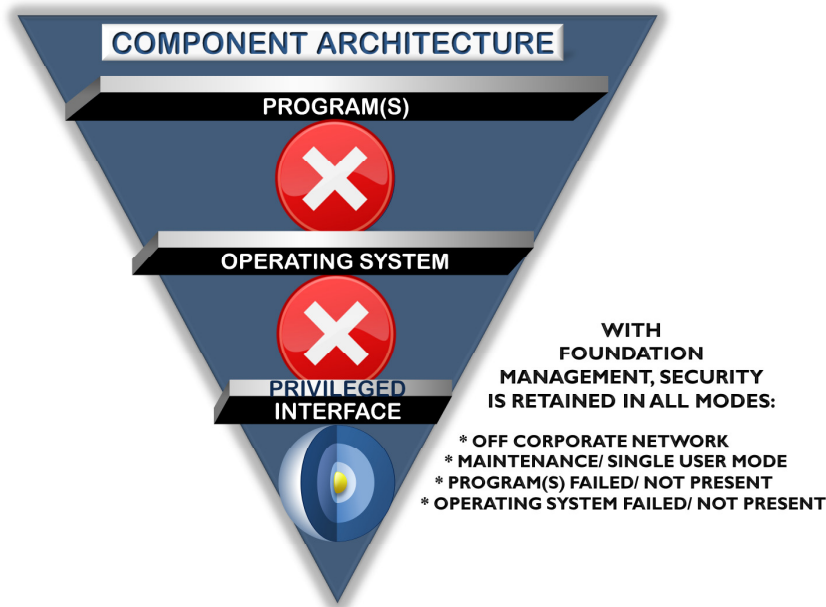
PRIVILEGED INTERFACES (BMC, SERIAL PORT, CONSOLE) IN THE COMPONENT LAYER HAVE THE HIGHEST AUTHORITY, GREATEST VULNERABILITY AND MOST RISK

FOUNDATION MANAGEMENT FOR SECURITY

How is it Different?

By starting with the component layer of IT infrastructure, Foundation Management secures IT infrastructure at the very foundation of the infrastructure by establishing connection and control over privileged component interfaces that are used to configure, repair, and maintain the systems layer of the architecture regardless of the operation mode of the component.

This means that even while systems and components are “off the corporate network” the security model is still in place.



The Security Model remains in place in all “operating modes,” even when programs, the operating system, and corporate network access is not available.

This security approach manages Insiders that are supposed to be there (staff, contractors, service techs) and Insiders who CAME FROM the outside by breaking through security.

This approach also includes “friendly outsiders” who work with our partners: people who can “ride in” on a designed network connection and gain access to privileged interfaces.

Unsecured privileged interfaces are the most vulnerable security point in our organizations today, but with Foundation Management that vulnerability is finally secured.

How do I Act on This?

The Defense Foundation from TDi Technologies® delivers Foundation Management Security, directly addressing the challenge of the Insider Threat.

The Defense Foundation secures privileged interfaces – placing them under secure, role-based systems management and authentication and provides forensic recording of every action taken over a privileged interface, recording this information down to the keystroke for each action.

The next step is to talk with us, so that we can get to know your situation and help you determine the best steps to take in order to leverage the capabilities of the Defense Foundation for your organization.

CONTACT:

Contact form: www.TDiTechnologies.com/contact

Toll Free: **800.695.1258**

International: **972.881.1553**

Email: sales@TDiTechnologies.com

You can also read more on Foundation Management and TDi Technologies® on the web at www.TDiTechnologies.com and review additional information on the Defense Foundation on the web at www.TDiTechnologies.com/defense-foundation.

TDi Technologies®
Defense Foundation
TDi Foundation Product Series

Your Business is Built on IT