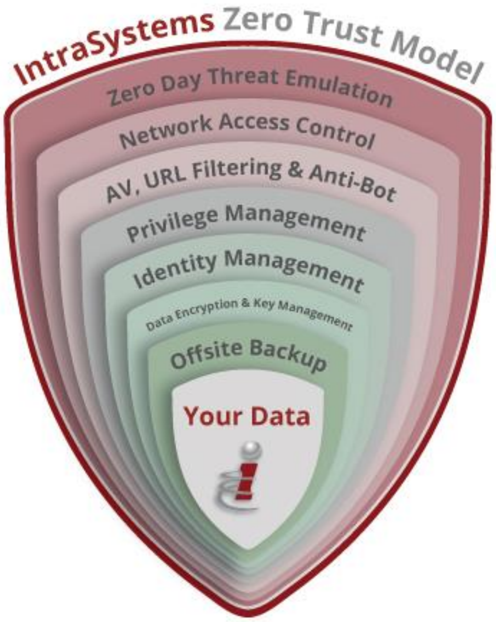
ZERO TRUST NETWORK

DEFEND YOUR DATA FROM CYBER THREATS WITH A ZERO TRUST NETWORK

At IntraSystems, we don't "trust" any packets, network traffic, and data……we reduce the temptation for insiders to abuse or misuse your network and we improve your chances of discovering cybercrime before it can succeed.

Some industry experts refer to this as "Zero Trust." Zero Trust eliminates the assumption of a "trusted" internal network where data is safe and an "untrusted" external network where data is unsafe. Zero Trust demands a network in a data-centric manner, investment in threat intelligence and detection, and development of robust vulnerability management, incident management, and forensic capabilities.

At IntraSystems, we've always equated security to an onion……a layered approach that requires many layers of trust. Unfortunately, trust is the fundamental problem in information security today.


IntraSystems Zero Trust Model
Zero Day Threat Emulation
Network Access Control
AV, URL Filtering & Anti-Bot
Privilege Management
Identity Management
Data Encryption & Key Management
Offsite Backup
Your Data

TRUE PROTECTION IS A MULTI-TIERED STRATEGY

The good news is that by changing your current trust model, we can create a network that is more efficient, compliant, and more cost-effective.

Moving to a Zero Trust model is a change in approach and requires a well-planned transition.

- All resources are accessed securely - regardless of location
- A "least privilege" strategy is implemented
- Access control is strictly enforced
- All network traffic is logged and inspected

ZERO DAY THREAT EMULATION

Hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. Zero-day protection provides a deeper level of inspection so you can prevent more malware and zero-day attacks, while ensuring quick delivery of safe content to your users. Our solution can catch the most sophisticated zero-day attacks utilizing unique CPU-level 100% evasion resistant technology. Delivers safe content that allows users to not only detect malware, but to rather prevent it; end-to-end protection on the network and a non-intrusive agent on endpoints; forensics tools for immediate analysis and remediation in case of a breach, and provides a single, consistent view into events and alerts.

NETWORK ACCESS CONTROL

Many (if not most) organizations have users with too much access to the network and data. Anything that lives within an organization's network needs protection. Our mission is to secure the network and data to reduce attack surfaces beyond what inadequate, traditional tools can do. We do this by wrapping network permissions around each unique user. Security is dynamic – it needs to change based on context such as user, role, location and device.

AV, URL FILTERING, ANTI-BOT UPDATES

Defense requires applying the best protection at the most vulnerable location – the endpoint. IntraSystems antivirus (AV), URL Filtering, and Anti-Bot solutions detect and prevent malware from executing your endpoints in real time - the most accurate, efficient and effective solution for preventing advanced persistent threats and malware from executing on your organization's endpoints. We identify unknown malware by analyzing suspicious files in a secured environment as well as detect and quarantine malware in both open and isolated networks without the need for continual signature updates.

PRIVILEGE MANAGEMENT

Having a privilege management capability allows you to remove admin rights from all users to stop attackers from exploiting privileges and gaining access to your data. Working in tandem with application control, this powerful combination makes whitelisting simple - allowing you to assign privileges directly to applications, tasks, and scripts to protect the endpoint against attacks that hit the operating system. We take a policy-based approach so that rules are assigned to different groups of users - depending on the specific needs of your business departments.

IDENTITY MANAGEMENT

IntraSystems verifies that your users are who they say they are and provides them with the right level of access. Users have convenient, secure access—from any device, anywhere—to the applications they need - whether in the cloud or on-premises. IntraSystems utilizes an enterprise-grade multi-factor authentication and access management solution that lets organizations consistently and centrally enforce dynamic risk-driven access policies aimed at providing continuous, seamless authentication. It protects all resources with a wide range of authentication methods, including push notification, biometrics, OTP, SMS, and traditional hardware and software tokens.

DATA ENCRYPTION & KEY MANAGEMENT

To reduce the risk posed by hackers, insider threats, and other malicious attacks, your organization must utilize encryption to protect sensitive data wherever it is found across your on-premises, virtual, public cloud, and hybrid environments. This includes data-at-rest in application and web servers, file servers, databases, and network attached storage, as well as data-in-motion across your network. Encryption applies security and access controls directly to your sensitive structured and unstructured data - wherever it resides. IntraSystems can deploy a comprehensive portfolio of data-at-rest and data-in-motion encryption solutions to secure all types of sensitive data across today's distributed enterprise.

OFFSITE BACKUP WITH MULTI-TIERED BACKUP

The days when you only had to protect data in your on-premises servers are gone. IntraSystems can protect your data in today's complex infrastructures—combining on-premises, virtual, cloud-hosted, and SaaS environments—with a backup solution that is designed from the ground up for the cloud-integrated systems you depend on today. It gives you the flexibility to easily backup data wherever it resides—on premise or in the cloud—and to replicate the data to a public or a private location of your choice.