Cybersecurity Solutions Guide
Transforming Their technology into Your solution
Better security for better business

Enabling business strategy with simplified, more connected IT security

We live in a connected world in which data is the lifeblood of business – in particular, data security is of utmost importance to our valued Federal customers. To protect its value, data must be secure wherever it resides, and wherever it needs to go.

At IMPRES, we increasingly hear from customers that many security solutions restrict the flow of data making it less useful to the organization, and even burdensome to the end user. This often creates risk when well-intentioned employees fail to comply with known security practices. Some solutions are simply not tailored to the unique needs of a specific company, or industry.

The IMPRES approach to security is based on simplicity, efficiency, and connectivity that combine to tie together the splintered aspects of IT security into one, integrated solution, capable of sharing insights across the organization. IMPRES experts add a critical layer of guidance which help businesses focus their security efforts. We deliver simplified security, making it easy for business users to manage their rules and policies, and for end users to comply with these rules, and policies.

Together, these enhancements can radically change the culture of compliance within an organization, and strengthen the overall security posture. This allows for easier adoption of disruptive technologies like cloud and mobility, so that an organization can focus on their core business, or mission.

The IMPRES cybersecurity solution approach makes us different. And while we know that every organization has security requirements that are entirely unique, we hope you will allow us to demonstrate our understanding, commitment, and capabilities in a mutually useful conversation.

Steve Ridgeway
Executive Vice President / Facilities Security Officer
IMPRES Technology Solutions, Inc.
The IMPRES difference

Delivering a context-aware security framework that is connected end-to-end to reduce complexity and mitigate risk

Governance
We assist organizations with the definition, integration, and administration of cybersecurity governance activities. Strengthening a security posture requires the seamless connection of people, processes, and technologies. IMPRES engineers collaborate with our customers to establish a conceptual framework and derive a practical operational methodology to support the proactive addressing of adversarial threats. We deliver robust ‘single’ and ‘suite’ solutions that ensure comprehensive compliance with NIST guidelines.

Cloud
As Federal agencies continue to migrate existing enterprise systems to the ‘cloud’, IMPRES stands at the forefront as an innovator and leading integrator in developing unique cyber solutions that address cloud-specific risks and fail points. Our engineers are fluent in the integration of Software Defined Networks with traditional network environments, offering increased security protection on-premises and within the cloud. We assist with the integration of access management tools, apply traffic and data analysis solutions, implement single sign-on control, and install disaster recovery technologies to improve the operational security and management of an organizations cloud.

Performance Analytics and Situation Mitigation
As active threats arise, agencies require the proactive management of threat intelligence and the automatic adjustment and provisioning of security postures – all while ensuring the seamless continuity of daily operations. Our cybersecurity solutions are uniquely developed and assembled to address these concerns, offering unparalleled scope and capability, including the capacity to analyze and evaluate internal user behavior and external threats to your technology ecosystem. We leverage pin-point threat vector analysis tools to identify outside risks, while applying industry-leading tools to synthesize and report behavioral trends from users, devices, and applications.

Collaboration
We understand the need to share sensitive, proprietary data in a fast, reliable, and secure manner. Our cybersecurity engineers work with your leadership from the on-set to understand your needs, developing a scaled solution that retains the capacity to deliver the level of security required for your existing user base, while offering the enhanced capability to evolve and defend your data against threats as your usage increased.

Endpoint Protection and Devices
With the increased use of mobile and tablet devices, it has never been easier to access your data on-the-go. However, it has also never been more crucial to establish a rigorous security approach that provides oversight, governance, and protection against vulnerabilities inherent in the use of these appliances. Simply relying on anti-virus software is not enough – organizations of all types require a more structured, disciplined, and proactive response to the over 200,000 new malware generated daily. IMPRES offers unique concepts, including the application of evolving software and security mechanisms that provide the level of endpoint protection your organization and data demands.
Innovation abounds as creative uses for connected devices, applications, and data continue to emerge. However, internet-connected intelligent devices that run and manage our world (often with little or no human intervention) no longer benefit from the ‘air gaps’ created by secure private networks.

As these and other Internet of Things (IoT) systems flood the internet, they must be protected from malware, hacking, spyware, and performance-corrupting activity.

IMPRES provides security solutions that draw on the extensive product development and expertise built by Intel across four decades of innovation. Intel embeds security at the ‘nano-scale’ – built-in at the silicon level to provide protection at a fundamental layer, below the OS – helping to assure that processing starts secure, runs secure, and stays secure.

The approach ensures protection against more threats, allows for faster detection of threats, and supports more immediate recovery of infrastructure and data.

Working in close partnership with our customers, OEM manufacturers, and distributors, IMPRES enables organizations to benefit from a security framework that addresses the expanded requirements for trust, solution integrity, accountability, and privacy that span every layer of the IoT: devices, connections, the cloud, and data centers.
The IMPRES difference

Unlike traditional Value Added Resellers, IMPRES abides by vendor-neutral principles, which strengthens our commitment to achieving maximized value and quality for your organization.

To ensure your organization possesses the level of protection it requires, IMPRES engineers collaborate with your leadership to derive a clear understanding of your existing infrastructure. Once a baseline is established, we conduct a detailed review of your risk points and offer recommendations for how to mitigate the occurrence of system threats.

IMPRES engineers possess the technical fluency to assemble products from multiple vendors, ensuring the seamless integration of various components that will blend into the background of your enterprise without disrupting daily activities.

Owing to our vendor-neutral approach, IMPRES’ focus is always on ensuring your business objectives are met. With this in mind, we design solutions that will not only maximize your operational desires, but will provide the needed immunity to existing and anticipated cyber threats.

The IMPRES approach is fundamentally unique – rather than aim to 'lock' your system to avoid outside threats, we provide tools, technologies and guidance that enables your organization to conduct business free from fear, while complying with the most stringent regulations.

We offer a combination of consulting security services and a deep technology portfolio covering network, identity and access management, data encryption, endpoint security, and security managed services.

Our capabilities within these areas ensures organizations receive solutions that work across the vast expanse of their enterprise, enabling protection against internal and external threats, while eliminating blind-spots within your architecture.

The result is a comprehensive, holistic and robust response to the most pressing of cybersecurity needs.

The need for a new approach

The cybersecurity space has never been more saturated with options, nor more complex to understand. As agencies and organizations worldwide invest resources toward protecting their enterprise, the threat of internal and external breaches is rising exponentially.

Today’s organizations require a disciplined, rigorous, and comprehensive methodology to not only combat existing threats, but to anticipate and predict the potential for future threats. This proactive approach is paramount to providing the level of protection required, ensuring your enterprise and its contents are sealed from disruption.

Simply applying an individual off-the-shelf solution or installing a hardware appliance is not enough. Concurrently, stacking solutions without a clear understanding of the interplay can increase your organization’s exposure to cyber threats.

Our cybersecurity engineers are leading experts with the knowledge, capabilities, and vision to design and implement the right solutions for your specific needs. As a leading provider in the cybersecurity space, we possess a deep understanding of the existing solutions available and the technical ability to blend and assemble the right solution for your enterprise.
**Governance**

**The challenge:**

Against a backdrop of five macro influences that are making robust governance, risk, and compliance difficult to achieve, the need is ever more pressing. To overcome this challenge, organizations need to ensure that the people, processes, and technology used to govern the organization are integrated and coordinated with the people managing enterprise IT, and that intelligence flows freely between the two.

- **Increasingly complex infrastructure** driven by cloud, virtualization, mobility/BYOD, plus the volume of unstructured data and proliferation of data, devices and architectures
- **Threats** growing in frequency and severity – exacerbated by the fact that corporate data is constantly on the move
- **Compliance and governance** with legislation and regulations always evolving and differing from country to country
- **Limited security budgets** and shortages of skilled resources
- **Siloed security architecture** across strategic IT pillars, including architecture mobility and the data center, leaving points of exposure

---

*Out-of-the-box reporting enables us to easily achieve and prove compliance with our own policies and with our customers’ requirements as well. There is no way we could have been able to meet our compliance objectives without these solutions.*

Security Practice Manager
Large US-based contracting firm

---

The growing challenge of addressing risk while achieving governance and compliance
Governance

The IMPRES solution:

IMPRES takes a unified approach to security, bridging the gap between the demands of an effective governance and compliance framework, and the practical requirements of managing risk and securing the enterprise IT.

We achieve this by helping customers to implement a seamless, connected security strategy that works across the organization, from the device, to the data center, to the cloud. In doing so, we remove avoidable gaps in security by taking a lifecycle approach:

Embed
Unlike many of our competitors, before infrastructure and solutions even reach customers, we work with the OEMs to ensure we can embed relevant security capabilities as a part of the manufacturing process, including Trusted Platform (TPM) chip, secured signed BIOS (may prevent hijacking), embedded authentication, and cloud security. Some of which are in use in cell phones today.

Detect and protect
IMPRES helps organizations to strengthen their security posture by proactively detecting cyber threats using insight and intelligence gained from integrated manufacturer tools around Threat Intelligence and Managed Security Services (billions of events per day).

This proactive detection is combined with the protection of information regardless of device and location, achieved by:

- Data (backup and recovery, data protection and encryption)
- The endpoint (deployment, patching, MDM and firewall VPNs)
- File detection and notification (log monitoring and management)

Respond
Increasingly, organizations are accepting that at some point they may be breached and it is critical that they have a pre-determined plan and capabilities in place that can know if someone modifies the system registry and can force a reload of the system, or detects a malware or intrusion in your desktop applications, even before patching or virus protection is available, and resets the workspace.

IMPRES’ next-generation firewall solutions can address Zero Day threats, malware, viruses and intrusions as they occur. IMPRES provides services from SecureWorks, IBM, Avnet, and others, for Incident Response and Digital Forensics practices, and can provide rapid containment and eradication of threats, minimizing both their duration and impact across your business.

Individually, each IMPRES provided security solution is strong in its own right, as acknowledged by industry analysts. When combined, they deliver connected security that gives organizations a governance and compliance framework, which enables them to address risk and align with NIST guidance, including:

- Setting a strategic direction for governance and compliance
- Making sure objectives are met with appropriate processes
- Ascertaining that risks are managed
- Ensuring resources are being used in a responsible way
Cloud

The challenge:

Managing a network has never been more challenging. The mass onset of more demanding applications, such as voice, video, and application mobility, makes traffic prioritization a mandate, not simply a check box for current data and voice in today’s architecture.

Traffic rerouting, brought on by the massive number of new devices on the network, and reach to the cloud, (a mandate in the Federal Government and a reality today) is only complicated by the number of new devices and increasing dependence by outside groups to access and share data real-time.

The groups continually attacking our Federal, commercial, and US infrastructure networks from outside and inside makes it difficult, if not impossible, to keep up with the threats. A security appliance (e.g. firewall, IDS, ...) reduces risks, however, does not eliminate them. They provide perimeter protection, but do not provide protection inside the perimeter.

These methods work well when you can control all equipment and replace all your infrastructure at the same time. But what about those devices, servers, mainframes, service devices in hospitals (gauges and meters in key systems) that do not lend themselves to replacement? Or in a cloud – you cannot control everything that is there. How do you prevent attacks, infection, hijacking, and malware from affecting these targets?

To combat this exposure, management teams need to ensure consistent, organization-wide cloud policies and procedures and give themselves the assurance that they know who is accessing data, on what device, from which location and, significantly, in what context.

100% of the network and security policies use IP addresses as identity. This is the root cause of complexity, network security vulnerabilities, poor segmentation, and lack of mobility.
The IMPRES solution:

As Federal agencies continue to migrate existing enterprise systems to the cloud, IMPRES stands at the forefront as an innovator and leading integrator in developing unique cyber solutions that address cloud-specific risks and fail points.

The IMPRES solution offers secure networking time reduced by 97%. Resource added with explicit trust segmentation, cloaked and encrypted communication. Deployed by NetOps and easily verified by InfoSec. By combining legacy and additional identity protocols you will reduce the attack surface up to 90%, improving time to mitigation, revocation, and quarantine up to 25%, and decreasing failover and disaster recovery times to as little as 1 second.

Our engineers are fluent in the integration of Software Defined Networks (SDN) with traditional network environments, offering increased security protection on-premises and within the cloud. We assist with the integration of access management tools, apply traffic and data analysis solutions, implement single sign-on (SSO) control, and install disaster recovery technologies to improve the operational security and management of an organization’s cloud.

IMPRES provides solutions that not only allow the traffic prioritization needed for today’s networks with SDN. Automating the rerouting of traffic is an inherent part of the architectures brought by these solutions.

The issue we have seen in every OEM’s offering is that each solution has a very individual way of looking at management and traffic flow. Not only is this unrealistic, but it is what has caused the greatest amount of complexity in technical environments, and as such, provides the greatest number of security problems in these systems.

Whether you are using bare metal servers, storage, networking, or using VMware, KVM, OpenStack, Hyper-V, Azure, or AWS, to provide your infrastructure the ability to move freely and manage environments from on-premises to the cloud is undoable, according to the manufacturers, unless you choose to ‘standardize’ your infrastructure to their hardware or software.

IMPRES provides standards based on open source to manage all your SDN networks, legacy networks, and even down to the hypervisor and physical hardware levels, from one management console.

To simplify the complex, we use identity-defined networking: a unified platform for secure networking. This allows us to lift the IP addresses off the network and to integrate this with our SDN solutions and offerings from companies traditionally used by each of the Federal agencies today in an adaptive security framework. This enables organizations to implement access controls that can satisfy the diverging demands of IT and business by combining security-focused software, services and hardware that incorporate embedded security.

The key is the simplicity of the network and the automation of response without the heavy lifting and complexity. From the management console that covers the SDN, legacy networks, physical, and virtual environments, as well as provisioning to and from the cloud, (leveraging the major cloud providers) and providing an ability to cloak and respond to attacks and threats – including responding to those probing for your network devices, while moving your network subnet, physical location – there are no others pulling together your environments as efficiently.
Performance Analytics & Situation Migration

The challenge:
As active threats arise, agencies require the proactive management of threat intelligence and the automatic adjustment and provisioning of security postures – all while ensuring the seamless continuity of daily operations.

IMPRES' cybersecurity solutions are uniquely developed and assembled to address these concerns, offering unparalleled scope and capability, including the capacity to analyze and evaluate internal user behavior and external threats to your technology ecosystem. We leverage pinpoint threat vector analysis tools to identify outside risks, while applying industry-leading tools to synthesize and report behavioral trends from users, devices, and applications.

Pretty much all cyber defense today is focused on what has already happened, inside, or at the perimeter of a company. Virus scanning, firewalls, and things like that. We realized that you can find a lot of signal for upcoming attacks in social media, chat rooms, and foreign open sources by applying our temporal analytics. So instead of waiting for attacks to happen, we can find early signals and try to prevent them in the first place.

Christopher Ahlberg
Founder, Recorded Future
Performance Analytics & Situation Migration

The IMPRES solution:

IMPRES offers a secured data feed that scours the web, and dark web, for any pertinent threats that might pertain to the customer’s environment. The solution is capable of looking for any instances – chatter, written, spoken, video – in over 12 languages for mention of any specific search criteria, i.e. DoD, Medical, Navy, located in California, or the MAC address or IP address from any of those environments, or usernames, hardware type, or software type. This data can provide a rich and quickly validated group of good data.

By combining this data collected from within the network – such as what websites, hardware, username, MAC addresses, IP addresses, or what kind of work might be occurring – and providing real-time multi-variate statistical correlation of events or resources, allows you a better view of where to spend your money.

The nirvana in the industry has always been if these threats could be realized in real-time and mitigation provided to respond to these threats in real-time as well. All the while, the applications in the sourced environments would evaluate the resource utilization and not simply suggest, but automatically reconfigure and redeploy the environments, to maintain the optimal utilization of all resources, while maintaining application performance. The optimal utilization of resources to assure application performance can only be obtained if the work is done real-time, and analytics become predictive rather than merely reactive. Any product can react to an ‘alert’... we are dynamically creating the alerts and looking for the solutions based on what we have available to mitigate, and then acting upon that.

By combining threat vector analysis and real-time predictive analytics into a singular solution to respond to the mission and technical requirements, we are able to not only determine the most likely threat vectors, but are able to make changes within the environment to ensure performance of all applications on a real-time basis. This differs in that it will be part of your software installed on a single hardware platform and integrated with your current in-house security and system products. By combining best of breed products and integrating their capabilities at the onset, we can provide the ability to not only move virtual equipment internally, but physical equipment as well.

We can proactively avoid outages due to ‘learned’ or ‘known’ threats and ensure application performance without degrading the performance of any workloads. The adaptive security framework from IMPRES enables organizations to implement access controls that can satisfy the diverging demands of IT and business by combining security-focused software, services, and hardware that incorporate embedded security.
Collaboration

The challenge:

In order to optimize business processes and improve productivity, organizations demand richer collaboration capabilities internally, externally, and across borders – making security a real challenge.

The fractured nature of the collaboration and mobility solutions market has forced many IT departments to rely on multiple vendors to support a variety of mobile endpoints, operating systems, applications, and users. Since these solutions frequently don’t talk to each other, they create complexity, additional cost, and ultimately, security challenges.

These challenges are fueled by organic growth and further exacerbated when organizations undergo mergers and acquisitions – often accumulating additional solutions in the process.

The complexity of data anywhere and users everywhere, as well as a patchwork of siloed security, is now so extreme it is creating risk and hampering innovation.

As technology changes accelerate across applications, infrastructure, cloud, and security, organizations must be agile enough to accommodate these changes and be able to evolve their security frameworks to keep pace with changes in business processes.

“The use of industry standard protocols and interoperability between the {firewalls} and {switches} means we aren’t faced with incompatibilities that add to the complexity and burden of IT management.”
Collaboration

The IMPRES solution:

From hardware encryption, smartcards, biometrics, identity and access reporting, data protection, recovery, to privileged access management, multifactor authentication, next-generation firewalls, unified threat management, VPNs, secured mobile devices, patching, fabric management, alerting… the IMPRES security framework delivers a single, comprehensive, end-to-end solution that closes gaps between siloed security solutions, reduces complexity, and mitigates risk – securing the organization from device, to data center, to cloud.

It allows employees to work together using their preferred mobile devices, laptops, and desktops – whether they are personally owned or corporate issued. Importantly, an intuitive drag and drop interface allows security workflows to be easily modified to align with new business processes, ensuring that the security implemented stands in the way of threats, not people and productivity.

The end-to-end security strategy from IMPRES is flexible, modular and based on SAML standards. It integrates with your existing security investments and is fast to deploy. What sets the solution apart is the ability to connect the selected security analytics engine, access control, and firewall, to deliver an adaptive security framework that is both content- and context-aware, as well as being policy-driven.

For example, in a situation in which someone outside the organization receives an email with an attachment classified as ‘internal only’, access to the attached document will be rejected before passing through the firewall.

Where most solution providers leave off, is once the documents or data leave your environment. With the IMPRES solution set for collaboration, data can be tagged and encrypted with a set of keys. Even if the data moves to a USB drive, CD, network drive or cloud entity, the keys follow. When ‘you’ decide the end user should no longer have access, you can revoke those rights.

Importantly, the framework embeds business policy and procedures into collaboration workflows to determine who gains access to which applications and data, removing the burden of having to make access decisions from IT. This also means that employees, partners and customers can easily be provisioned and de-provisioned as required by the business.
Endpoint protection & devices

The challenge:

For many organizations, the main challenge surrounding mobility is how to expand access to sensitive or ‘secured’ applications and data for authorized individuals, while simultaneously safeguarding against costly security breaches.

IT departments are asked to facilitate access through an increasingly broad array of computing device types (laptops, tablets, and smartphones), operating systems, (including Windows 10, Samsung® Android™ and Apple® iOS) as well as different mobility models, such as site issued, DoD or agency-owned, personally-enabled (COPE), choose your own device (CYOD), and bring your own device (BYOD).

Critical to meeting this challenge is understanding the different mobility requirements of users. If IT doesn’t enable the mission with an appropriate mobility strategy, it can be undermined by shadow IT – with employees finding workarounds that can be risky, and could lead to data leakage and cyber attacks.

Likewise, if employees feel that security policies impede productivity or could encroach on their personal data, they can be expected to circumvent those policies. This privacy concern is exactly the reason why mobile device management (MDM) alone cannot resolve all the issues presented by mobility.
Endpoint protection & devices

The IMPRES solution:

With the increased use of mobile and tablet devices, it has never been easier to access your data on the go. It has never been more crucial to establish a rigorous security approach that provides oversight, governance, and protection against vulnerabilities inherent in the use of these appliances.

Simply relying on anti-virus software is not enough – organizations of all types require a more structured, disciplined, and proactive response to the over 200,000 new malwares generated daily.

IMPRES offers unique concepts, including the application of evolving software and security mechanisms that provide the level of endpoint protection your organization and data demands.

Solutions from IMPRES can incorporate products with the mandates to keep your equipment patched, and help deploy images to desktops, endpoints, and push updates to mobile devices. It is extremely fast to deploy, easy to maintain, offers simple administration, and increases the performance and security of your current OS patching methods.

Further into the portfolio of endpoint protection, IMPRES provides comprehensive mobile enablement solutions that are flexible enough to support your choice of mobility strategy. This unified solution integrates multiple capabilities, including management of systems, mobile devices, applications, content, encryption, and policies; plus, secure access to corporate resources, user self-service, and real-time reporting and alerts. We go beyond mobile device management by integrating a containerization approach as part of our integrated offerings.

The capabilities of these solutions allow you to manage the entire endpoint, while containerization enables IT to manage a corporate workspace – including data and apps – over and above the endpoint. In doing so, anything that goes into the container can be owned/controlled by IT. Anything outside the container is kept personal. As a result, IT only sees/manages the corporate workspace, not the entire device, enabling organizations to overcome privacy concerns and related legal implications.

Specific to the DoD, IC, and civilian spaces, there is often the requirement for a more robust offering. This is where IMPRES provides a more complete overview.

We bring best of breed, with compliance and integration in mind. Use of solutions that provide far more than anti-virus, they can be used to complement or completely replace, but they are designed to provide protection for viruses and threats before they are even known by the rest of the world.
Take a closer look

In order to provide you with as much information as possible about IMPRES’ cybersecurity solutions, we have put together resources for you to take a closer look.

Discovery workshop
Spend half a day with an IMPRES Solutions Architect to brainstorm and blueprint your organization’s unique needs and requirements. See how they can be mapped with IMPRES’ cybersecurity solutions for your environment and your expanding boundaries. You’ll also learn from other organizations and the specific benefits that they have realized in working with us.

Collaboration
Ask your IMPRES Account Representative to help set up an Executive Briefing and see first-hand a demonstration of IMPRES-provided security solutions in action.

Collaboration and integration of your base assets to continue your flow of data between groups is a key point within the IMPRES cybersecurity solutions set, and are easily demonstrated via a Proof of Value (POV) at your site. Please ask your IMPRES Account Manager for details.

For more information visit:  www.imprestechnology.com/cyber
Or email: esg@imprestechnology.com