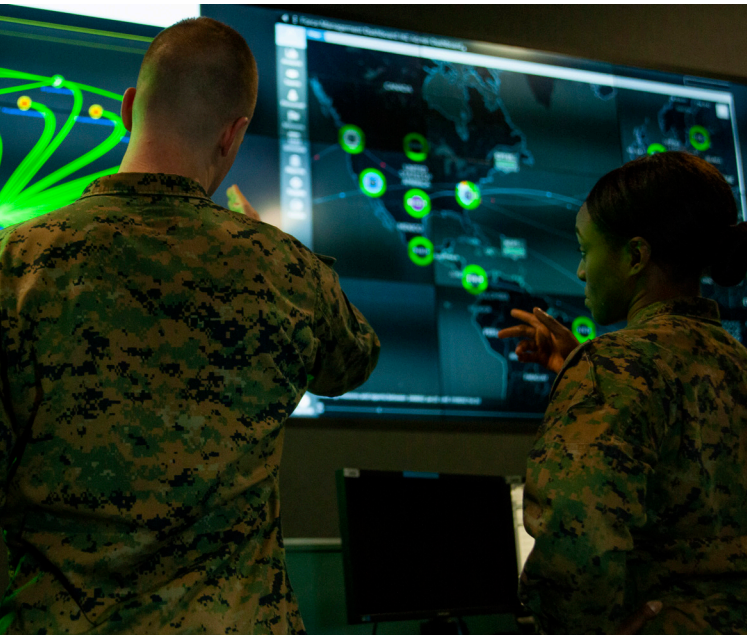
Ivanti for the Department of Defense

Preserve National Security with Ivanti



Persistent and Emerging Concerns for DoD

We have always been at war with threat actors who use strategies like phishing, malware, password and credential attacks, and others. But the war is getting more sophisticated. Threat actors are shifting command line and remote shell exploits over malware. 64% of attacks use this method to be exact.

The threat actors themselves are changing too. Increasing cyber threats from Iran, China, Russia, and North Korea are becoming more eminent. There is also a rise in threats from cyber mercenaries and access brokers.

These changes are being driven in part by the evolving way we utilize technology. We have an increasing reliance on mobility and modern endpoints to enable the mission. And with all of this comes a need to look at our own approach to cybersecurity.

The President of the United States has already signed various executive orders around cybersecurity in an effort to increase the security of the nation. The question is, can we meet them? And will they be enough?

Vulnerabilities: Causes & Effects

Government consistently ranks 3rd amongst the most targeted industries for cybersecurity threats. But changing threat actors and evolving methods aren't the only things contributing to this.

31% of government security incidents are due to improper usage. 80% of compromises are based on stolen identity or credentials. Government personnel are hugely implicated in security breaches.

Not to mention, it can take as long as 231 days – over 7.5 months – to identify a breach in the public sector. And each breach is costly, averaging about $1.6 Million each.

This has led to situations like the 2022 Russian cyberattack for which CISA issued a "shields up" warning. The 2021 hacking of Microsoft by China. And the 2020 phishing attacks by hackers posing as the CDC and WHO.

64%

of attacks are shifting command line and remote shell exploits over malware

31%

of government security incidents are due to improper usage

80%

of compromises are based on stolen identity or credentials

The Solution

In light of these challenges, many agencies are adopting a multi-pronged strategy to secure their environments and ensure the mission.

1. Adopt Zero Trust Architecture (ZTA)
   - ZTA assumes threats are already in your environment so there is no inherited trust and compliance enforcement is ongoing.
2. Utilize User Endpoint Management & Mobility Management
   - Discovery, secure, and manage devices, and secure users.
3. Implement Risk-Based Patch Management
   - Targeted vulnerability remediation that incorporates active threats that lets you stay ahead.
4. Control with Change Management
   - Complete end-to-end life cycle change management processes that provides real-time visibility and transparency.

Ensuring the Mission & Securing the Nation

The Ivanti platform can help support government agencies looking to implement such a strategy to help them ensure the mission and secure the nation. Let's dive deeper into the following components of the Ivanti suite:

1. Ivanti Neurons for Zero Trust Access (ZTA)
2. Ivanti Neurons for Unified Endpoint Management (UEM)
3. Ivanti Neurons for Patch Intelligence
4. Ivanti Neurons for Service Management

Ivanti Neurons for ZTA

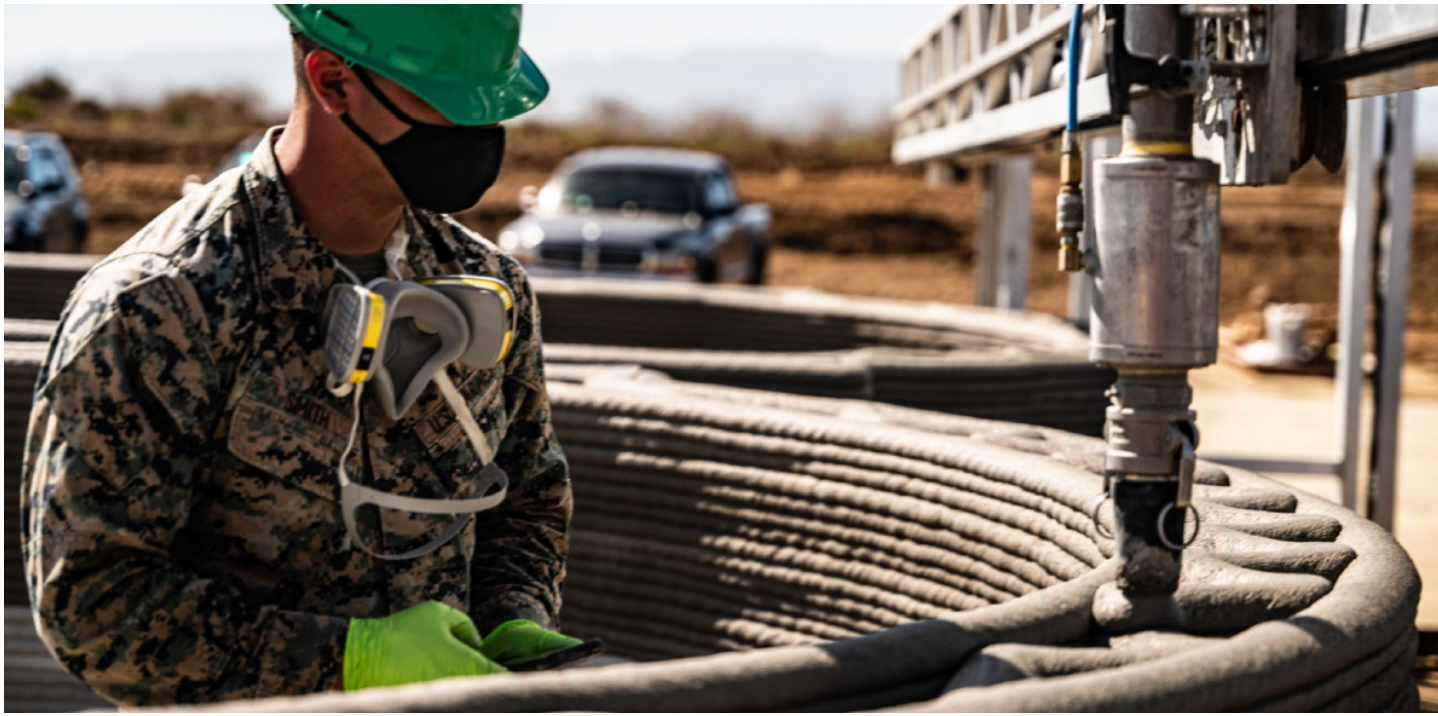
- Create secure connections between devices to applications
- Eliminate bandwidth and data charges
- Constantly verify users, their devices, and applications

Ivanti Neurons for Zero Trust Access uses the web to create a secure connection from the device to an application, eliminating bandwidth and data charges through gateways while constantly verifying the user, their device, and applications based on granular constraints.

Ivanti Neurons for Endpoint Manager

- Accurate and actionable device insights
- Efficient device management
- Automated healing actions

With Ivanti Neurons for Unified Endpoint Management (UEM), you now have more visibility into your entire asset estate, bringing in the mobile devices and combining them with your traditionally managed devices–putting your IT team on a path to hyper-automation to enable you to self-heal, self-secure your devices and provide a personalized, contextual experience.



Ivanti Neurons for Patch Intelligence

- Remediate vulnerabilities faster
- Identify non-compliant systems
- Deliver actionable intelligence automatically

Ivanti Neurons for Patch Intelligence delivers automated insight into your risk exposure by providing remediation prioritization based on adversarial risk. Quickly understand which remediation actions to take first with Vulnerability Risk Rating (VRR). Threat-context for vulnerabilities via supervised and unsupervised machine learning provides real-time intelligence on vulnerability exploits that are actively trending in the wild, and those that have ties to ransomware. Act faster against risk exposure prioritizing where to patch with Ivanti Neurons for Patch Intelligence.

Ivanti Neurons for Service Management

- Automate workflows
- Eliminate costly manual processes
- Increase efficiency, compliance, and security

Ivanti Neurons for ITSM is the most flexible and complete cloud-optimized ITSM solution available. Automate workflows, eliminating costly manual processes while making your business more efficient, compliant, and secure. Whether you're looking for an IT help desk / support ticket solution or need to perform more advanced ITIL service management processes, Ivanti Neurons for ITSM can easily scale and adapt to meet your specific business needs.

Benefits

- Stay one step ahead of threat actors
- Proactive security
- Increased transparency
- Centralized visibility
- Insights about users, devices, applications, and gateways
- Automated responsiveness
- Flexible consumption
- Effortless scalability
- Rapid deployment of applications
- Up to date security patches
- No siloes
- More productivity
- Collaboration without compromising security

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com