Real Talk With | Global Defense Company

Manufacturing

"When it comes to the business of defense, information security is always a top priority. Together with Xerox, we're able to be more proactive and deliberate about the protection of customer data and intellectual property."

—*Director of Information Technology,*
Global Defense Company

Our Challenge

"As a global defense manufacturer, compliance, consistency, IT security and risk mitigation management are major priorities. Network printing devices are an integral part of our company's IT infrastructure. Through recent audits, noncompliant multifunction devices (MFDs) were discovered. We wanted a customized solution that would help mitigate risks on our devices that house customer data across our multiple businesses over several geographies."

Our Solution

"Since network security compliance is paramount, we needed a solution that would not only bring our fleets up to compliance, but also continue to deliver consistent results and prevent any future security risks. Xerox provided a solution that seamlessly integrates with our existing system … and their Print Security Audit Service was added to increase security management and provide ongoing monitoring and protection."

Our Results

In the first year, we've already seen several important benefits:

- Proactive management of print devices and network security
- Reduced risk of human-factor security breaches
- Consistent, automated reporting on compliance of devices to provide feedback on compliance gaps
- Support for security governance and regulatory compliance
- Plus the ability to securely print when and where employees want, all while improving control over device usage and print costs

"Our strong partnership with Xerox makes it possible for us to be a secure, trusted partner to our customers worldwide. We make military and commercial aircraft engines as well as many other aircraft components. So there's no room for a breach."

—Director of Information Technology,
Global Defense Company

Inside a Very Secretive Place

As you can imagine, a global defense manufacturer with annual revenues of over $60 billion has extensive data and information to protect. They provide a broad range of high-tech products and services to the aerospace and building systems industries around the world.

Security is a priority, but it can also get in the way of productivity.

With highly sensitive information residing on the company's devices, including customer data and intellectual property, the potential for a breach was real.

In fact, a standard security audit revealed that it was possible to breach a device using public information.

The company wanted to maintain the security of information throughout its document infrastructure, yet foster communication and productivity among its workforce.

To make matters worse, whenever a networked device went down, it lost its security settings. And there was no automated way to become aware of these situations, so the risk was very real.

Once the company called for an end-to-end infrastructure audit, including printers and devices on the network, noncompliant MFDs were discovered globally across all three printer suppliers.

Defending the Data

With a Managed Print Services (MPS) approach from Xerox, this defense manufacturer was able to start protecting its own data better. By optimizing the company's printing environments, they made sure everything connected in a secure and compliant way.

The next generation of Xerox® MPS is designed to deliver continuous innovation.

There are immediate security and cost-saving benefits. And additional safeguards can happen over time, as improvements are added layer by layer. Some of those layers include:

- Xerox® Print Security Audit Service. It can easily be integrated with many others MPS components to create a tight environment.
- Xerox® Secure Access. Using a proximity card and secure PIN code, employees are now required to authenticate 100 percent of print jobs for release at available printers. And it's quick and easy.
- Controlled Access to Devices. Not all devices are available to all users. Password assignments differentiate access levels for heavily protected areas and devices.
- Scheduled Image Overwrite. Many print devices keep images of all documents on a hard drive, which is accessible even after the device has been disposed of. With scheduled image overwrite, that data is wiped on a regular basis to ensure it's not breached at a later date.

Closing the Gaps

The Xerox strategy for managing print services provides a proactive approach to potential security breaches. Ongoing management of print devices and firmware updates supports the company's established and evolving security standards.

Initially, service was deployed on the company's networked devices. This ensures consistent behavior of devices, aids in troubleshooting and is part of the company's overall security policy. Now automated audits take place, and they can be scheduled.

With any gaps detected, there is now a standardized plan for remediation. Immediately following communication and approval from the client, the remediation process begins to address and prevent risks.

"We now have the systems and controls to prevent data breaches today, and to respond quickly to new threats in the years ahead," says the IT decision maker.

To learn more about securing your network, visit xerox.com/security today.

Ready For Real Business xerox®